☑ ET MALWARE [PTsecurity] Remcos RAT Checkin 69
☑ ET MALWARE [PTsecurity] Remcos RAT Checkin 70
☑ ET MALWARE [PTsecurity] Remcos RAT Checkin 71
☑ ET MALWARE [PTsecurity] Remcos RAT Checkin 72
☑ ET MALWARE [PTsecurity] Remcos RAT Checkin 73
☑ ET MALWARE Malicious XLS DDE rar Drop Attempt (.live)
☑ ET MALWARE Locky CnC Checkin
☑ ET MALWARE ELF/Chacha.DDoS/Xor.DDoS Stage 2 CnC Checkin
☑ ET MALWARE Win32/BlackCarat Response from CnC
☑ ET MALWARE Win32/BlackCarat XORed (0x77) CnC Checkin
☑ ET MALWARE Zebrocy Backdoor CnC Activity
☑ ET MALWARE ArrobarLoader CnC Checkin M1
☑ ET MALWARE Possible APT29 CozyBear/SeaDaddy SSL/TLS Certificate Observed
☑ ET MALWARE Possible APT28 DOC Uploader SSL/TLS Certificate Observed
☑ ET MALWARE Possible DarkTequila SSL/TLS Certificate Observed
☑ ET MALWARE Octopus Malware Initial Connectivity Check
☑ ET MALWARE Octopus Malware CnC Server Request
☑ ET MALWARE Octopus Malware CnC Server Connectivity Check
☑ ET MALWARE Octopus Malware CnC Activity
☑ ET MALWARE Sidewinder Stage 2 VBS Downloader Reporting Successful Infection
☑ ET MALWARE MICROPSIA CnC Domain Observed in SNI (samwinchester .club)
☑ ET MALWARE MICROPSIA HTTP Failover CnC Checkin
☑ ET MALWARE MICROPSIA HTTP Failover Response M1
☑ ET MALWARE MICROPSIA HTTP Failover Response M2
☑ ET MALWARE MICROPSIA Sending JPG Screenshot to CnC with .his Extension
☑ ET MALWARE MICROPSIA HTTP Failover Reporting Infected System Information and RAT Version
☑ ET MALWARE Sharik/Smoke CnC Beacon 12
☑ ET MALWARE Sharik/Smoke Fake 404 Response with Payload Location
☑ ET MALWARE DNS Query for DNSpionage CnC Domain
☑ ET MALWARE TrueBot/Silence.Downloader CnC Checkin
☑ ET MALWARE TrueBot/Silence.Downloader Keep-Alive
☑ ET MALWARE MSIL/KeyRedirEx Banker Requesting Redirect/Inject List
☑ ET MALWARE MSIL/KeyRedirEx Banker Receiving Redirect/Inject List
☑ ET MALWARE MSIL/KeyRedirEx Banker Receiving Exit Instruction
☑ ET MALWARE BlackTech/PLEAD TSCookie CnC Checkin M1
☑ ET MALWARE BlackTech/PLEAD TSCookie CnC Checkin M2
☑ ET MALWARE MSIL/Lordix Stealer Exfiltrating Data
☑ ET MALWARE MSIL.BackNet Checkin
☑ ET MALWARE APT33/CharmingKitten DDNS Overlap Domain in DNS Lookup M1
☑ ET MALWARE APT33/CharmingKitten DDNS Overlap Domain in DNS Lookup M2
☑ ET MALWARE APT33/CharmingKitten JS/HTA Stage 1 CnC Checkin
☑ ET MALWARE APT33/CharmingKitten Shellcode Communicating with CnC
☑ ET MALWARE APT33/CharmingKitten Retrieving New Payload (flowbit set)
☑ ET MALWARE APT33/CharmingKitten Encrypted Payload Inbound
☑ ET MALWARE Perl/Shellbot.SM IRC CnC Checkin
☑ ET MALWARE JavaRAT CnC Init Activity
☐ ET MALWARE JavaRAT CnC Checkin
☑ ET MALWARE JavaRAT Keep-Alive (inbound)
☑ ET MALWARE JavaRAT Keep-Alive (outbound)
☐ ET MALWARE JavaRAT Sending Screen Size
☑ ET MALWARE JavaRAT Sending Screenshot
☑ ET MALWARE JavaRAT Requesting Screen Size
☐ ET MALWARE JavaRAT Requesting Screenshot
☑ ET MALWARE MSIL.Kraken.v2 HTTP Pattern
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 1/2 CnC)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 1/2 Staging Domain)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 3 Staging Domain)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 3 Staging Domain)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 Staging Domain)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 Staging Domain)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 Staging Domain)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 Staging Domain)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 Staging Domain)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 Staging Domain)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 Staging Domain)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 Staging Domain)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 Staging Domain)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 Staging Domain)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 5 Staging Domain)
☑ ET MALWARE ELF/Muhstik Bot Reporting Vulnerable Server to CnC
☑ ET MALWARE JunkMiner Downloader Communicating with CnC
☑ ET MALWARE Operation Baby Coin syschk CnC Communication
☑ ET MALWARE ELF/Muhstik Scanner Module Activity
☑ ET MALWARE TEMP.Periscope APT Domain in DNS Lookup
☑ ET MALWARE TEMP.Periscope APT Domain in DNS Lookup
☑ ET MALWARE Mylobot Receiving XOR Encrypted Config (0xde)
☑ ET MALWARE Operation Mystery Baby syschk CnC Communication
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif Inject Domain)
☑ ET MALWARE Observed Malicious SSL Cert (ServHelper CnC)
☑ ET MALWARE APT29 Domain in DNS Lookup (pandorasong .com)
☑ ET MALWARE Observed Malicious SSL Cert (APT29)
☑ ET MALWARE Hades APT Downloader Attempting to Retrieve Stage 2 Payload
☑ ET MALWARE Hades APT Domain in DNS Lookup (findupdatems .com)
☑ ET MALWARE JS.InfectedMikrotik Injects Domain Observed in DNS Lookup
☑ ET MALWARE JS.InfectedMikrotik Injects Domain Observed in DNS Lookup
☑ ET MALWARE JS.InfectedMikrotik Injects Domain Observed in DNS Lookup
☑ ET MALWARE JS.InfectedMikrotik Injects Domain Observed in DNS Lookup
☑ ET MALWARE JS.InfectedMikrotik Injects Domain Observed in DNS Lookup
☑ ET MALWARE JS.InfectedMikrotik Injects Domain Observed in DNS Lookup
☑ ET MALWARE JS.InfectedMikrotik Injects Domain Observed in TLS SNI

- [x] ET MALWARE JS.InfectedMikrotik Injects Domain Observed in DNS Lookup
- [x] ET MALWARE DarkGate CnC Requesting Data Exfiltration from Bot
- [x] ET MALWARE DarkGate Domain in DNS Lookup (hardwarenet .cc)
- [x] ET MALWARE DarkGate Domain in DNS Lookup (battlenet .la)
- [x] ET MALWARE ArtraDownloader/TeleRAT Checkin
- [ ] ET MALWARE Observed Malicious SSL Cert (BrushaLoader Domain)
- [x] ET MALWARE OceanLotus Stage 2 Domain in DNS Lookup (bootstraplink .com)
- [x] ET MALWARE OceanLotus Stage 2 Domain in DNS Lookup (widgets-wp .com)
- [x] ET MALWARE Observed Malicious SSL Cert (StrongPity Domain)
- [x] ET MALWARE Observed Malicious SSL Cert (StrongPity Domain)
- [x] ET MALWARE L0rdix Stealer CnC Sending Screenshot
- [x] ET MALWARE DNSpionage Commands Embedded in Webpage Inbound
- [x] ET MALWARE Inbound PowerShell Saving Base64 Decoded Payload to Temp M1 2018-11-29
- [x] ET MALWARE Inbound PowerShell Executing Base64 Decoded VBE from Temp 2018-11-29
- [x] ET MALWARE Observed Malicious SSL Cert (POWERSTATS Proxy CnC)
- [x] ET MALWARE DNSpionage Requesting Config
- [x] ET MALWARE Observed DNS Query for MageCart Data Exfil Domain
- [ ] ET MALWARE [PTsecurity] WeChat (Ransomware/Stealer) Config
- [x] ET MALWARE STOLENPENCIL CnC Domain in DNS Lookup
- [x] ET MALWARE STOLENPENCIL CnC Domain in DNS Lookup
- [x] ET MALWARE STOLENPENCIL CnC Domain in DNS Lookup
- [x] ET MALWARE STOLENPENCIL CnC Domain in DNS Lookup
- [x] ET MALWARE STOLENPENCIL CnC Domain in DNS Lookup
- [x] ET MALWARE STOLENPENCIL CnC Domain in DNS Lookup
- [x] ET MALWARE STOLENPENCIL CnC Domain in DNS Lookup
- [x] ET MALWARE Observed Malicious SSL Cert (Cobalt Group/More_Eggs CnC)
- [ ] ET MALWARE Cobalt Group/More_Eggs CnC Domain in DNS Lookup
- [ ] ET MALWARE Cobalt Group/More_Eggs CnC Domain in DNS Lookup
- [ ] ET MALWARE Cobalt Group/More_Eggs CnC Domain in DNS Lookup
- [ ] ET MALWARE Cobalt Group/More_Eggs CnC Domain in DNS Lookup
- [ ] ET MALWARE Cobalt Group/More_Eggs CnC Domain in DNS Lookup
- [ ] ET MALWARE Cobalt Group/More_Eggs CnC Domain in DNS Lookup
- [x] ET MALWARE ELF/Samba CnC Checkin
- [x] ET MALWARE Win32/DanaBot Harvesting Email Addresses 1
- [x] ET MALWARE RedControle Probing Infected System
- [x] ET MALWARE ELF/Win32 Lucky Ransomware CnC Checkin
- [ ] ET MALWARE Lucky Ransomware Reporting Successful File Encryption
- [x] ET MALWARE Donot (APT-C-35) Stage 1 Requesting Main Payload
- [x] ET MALWARE Shamoon v3 32bit Propagating Internally via SMB
- [x] ET MALWARE AveMaria Initial CnC Checkin
- [x] ET MALWARE [PTsecurity] Trickbot Data Exfiltration
- [x] ET MALWARE MSIL.Orion Stealer Exfil via FTP
- [x] ET MALWARE Observed DNS Query to known Windshift APT Related Domain 2
- [x] ET MALWARE APT28/Sofacy Zebrocy Go Variant CnC Activity
- [x] ET MALWARE APT28/Sofacy Zebrocy Secondary Payload CnC Checkin
- [x] ET MALWARE Ursa Loader CnC Checkin
- [ ] ET MALWARE TitanFox Loader CnC Checkin
- [x] ET MALWARE APT28 Zebrocy/Zekapab Reporting to CnC M3
- [x] ET MALWARE Operation Cobra Venom WSF Stage 1 - CnC Checkin
- [x] ET MALWARE DarkGate CNC Checkin
- [x] ET MALWARE DarkGate Domain in DNS Lookup (akamai .la)
- [x] ET MALWARE DarkGate Domain in DNS Lookup (awsamazon.cc)
- [x] ET MALWARE Kraken C2 Domain Observed (kraken656kn6wyyx in DNS Lookup)
- [x] ET MALWARE HackTool.Linux.SSHBRUTE.A Haiduc Initial Compromise C2 POST
- [x] ET MALWARE OceanLotus Stage 2 Domain in DNS Lookup (cdn-ampproject .com)
- [x] ET MALWARE OceanLotus Stage 2 Domain in DNS Lookup (sskimresources .com)
- [ ] ET MALWARE Observed Malicious SSL Cert (BrushaLoader Domain)
- [x] ET MALWARE Observed Malicious SSL Cert (StrongPity Domain)
- [x] ET MALWARE Observed Malicious SSL Cert (StrongPity Domain)
- [x] ET MALWARE L0rdix Stealer CnC Data Exfil
- [x] ET MALWARE IcedID WebSocket Request
- [x] ET MALWARE Inbound PowerShell Saving Base64 Decoded Payload to Temp M2 2018-11-29
- [x] ET MALWARE Observed Malicious SSL Cert (POWERSTATS Proxy CnC)
- [ ] ET MALWARE DNS Query for DNSpionage CnC Domain
- [x] ET MALWARE MSIL APT28 Zebrocy/Zekapab Reporting to CnC
- [x] ET MALWARE Observed DNS Query for MageCart Data Exfil Domain
- [x] ET MALWARE [PTsecurity] WeChat (Ransomware/Stealer) HttpHeader
- [x] ET MALWARE STOLENPENCIL CnC Domain in DNS Lookup
- [x] ET MALWARE STOLENPENCIL CnC Domain in DNS Lookup
- [x] ET MALWARE STOLENPENCIL CnC Domain in DNS Lookup
- [x] ET MALWARE STOLENPENCIL CnC Domain in DNS Lookup
- [x] ET MALWARE STOLENPENCIL CnC Domain in DNS Lookup
- [x] ET MALWARE STOLENPENCIL CnC Domain in DNS Lookup
- [x] ET MALWARE STOLENPENCIL CnC Domain in DNS Lookup
- [ ] ET MALWARE Cobalt Group/More_Eggs CnC Domain in DNS Lookup
- [ ] ET MALWARE Cobalt Group/More_Eggs CnC Domain in DNS Lookup
- [ ] ET MALWARE Cobalt Group/More_Eggs CnC Domain in DNS Lookup
- [ ] ET MALWARE Cobalt Group/More_Eggs CnC Domain in DNS Lookup
- [ ] ET MALWARE Cobalt Group/More_Eggs CnC Domain in DNS Lookup
- [ ] ET MALWARE Cobalt Group/More_Eggs CnC Domain in DNS Lookup
- [ ] ET MALWARE Cobalt Group/More_Eggs CnC Domain in DNS Lookup
- [x] ET MALWARE Win32/DanaBot Harvesting Email Addresses 2
- [x] ET MALWARE Observed MongoLock Variant CnC Domain (s .rapid7 .xyz in TLS SNI)
- [x] ET MALWARE RedControle Communicating with CnC
- [ ] ET MALWARE ELF/Win32 Lucky Ransomware Encryption Process Started
- [x] ET MALWARE Donot (APT-C-35) Stage 1 Requesting Persistence Setup File
- [x] ET MALWARE Shamoon V3 CnC Checkin
- [x] ET MALWARE Shamoon v3 64bit Propagating Internally via SMB
- [x] ET MALWARE Observed GandCrab Domain (gandcrab .bit)
- [x] ET MALWARE Win32/ArtraDownloader Checkin
- [x] ET MALWARE Observed DNS Query to known Windshift APT Related Domain 1
- [x] ET MALWARE MSIL APT28 Zebrocy/Zekapab Reporting to CnC M2
- [x] ET MALWARE APT28/Sofacy Zebrocy Go Variant Downloader Error POST
- [x] ET MALWARE APT28/Sofacy Zebrocy Go Variant Checkin
- [x] ET MALWARE Observed Malicious SSL Cert (SedUploader)
- [x] ET MALWARE JS/Unk Downloader 0 Byte POST CnC Checkin
- [x] ET MALWARE Operation Cobra Venom Stage 1 DNS Lookup
- [x] ET MALWARE Operation Cobra Venom WSF Stage 1 - File Decode Completed

- [x] ET MALWARE Operation Cobra Venom WSF Stage 2 - CnC Checkin
- [x] ET MALWARE ServHelper RAT CnC Domain Observed in SNI
- [x] ET MALWARE Observed Malicious SSL Cert (ServHelper CnC)
- [x] ET MALWARE ServHelper CnC Inital Checkin
- [x] ET MALWARE APT DarkHydrus DNS Lookup 1
- [x] ET MALWARE APT DarkHydrus DNS Lookup 3
- [x] ET MALWARE APT DarkHydrus DNS Lookup 5
- [x] ET MALWARE APT DarkHydrus DNS Lookup 7
- [x] ET MALWARE APT DarkHydrus DNS Lookup 9
- [x] ET MALWARE APT DarkHydrus DNS Lookup 11
- [x] ET MALWARE APT DarkHydrus DNS Lookup 13
- [x] ET MALWARE APT DarkHydrus DNS Lookup 15
- [x] ET MALWARE APT DarkHydrus DNS Lookup 17
- [x] ET MALWARE APT DarkHydrus DNS Lookup 19
- [x] ET MALWARE APT DarkHydrus DNS Lookup 21
- [x] ET MALWARE APT DarkHydrus DNS Lookup 23
- [x] ET MALWARE Observed Awad Bot CnC Domain (hawad .000webhostapp .com in TLS SNI)
- [x] ET MALWARE Observed Malicious SSL Cert (ColdRiver APT DNSpionage MITM)
- [x] ET MALWARE Observed Malicious SSL Cert (ColdRiver APT DNSpionage MITM)
- [x] ET MALWARE Possible Sharik/Smoke Loader 7zip Connectivity Check
- [x] ET MALWARE Observed TrumpHead Ransomware CnC Domain (6bbsjnrzv2uvp7bp .onion .pet in TLS SNI)
- [x] ET MALWARE APT DarkHydrus DNS Lookup 26
- [x] ET MALWARE APT DarkHydrus DNS Lookup 28
- [x] ET MALWARE Observed Malicious SSL Cert (POWERRATANKBA CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (MageCart CnC)
- [x] ET MALWARE MageCart CnC Domain in SNI
- [x] ET MALWARE OSX/LamePyre Screenshot Upload
- [x] ET MALWARE Atom Logger exfil via SMTP
- [x] ET MALWARE Observed Malicious SSL Cert (DonotGroup/Patchwork CnC)
- [x] ET MALWARE [PTsecurity] Remcos RAT Checkin 85
- [x] ET MALWARE [PTsecurity] Possible Backdoor.Win32.TeamBot / RTM C2 Response
- [x] ET MALWARE W32.Razy Inject Domain in DNS Lookup
- [x] ET MALWARE W32.Razy Inject Domain in DNS Lookup
- [x] ET MALWARE Observed Malicious SSL Cert (BrushaLoader CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (Zepakab CnC)
- [x] ET MALWARE CoreDn CnC Checkin M2
- [x] ET MALWARE Observed Malicious SSL Cert (APT32 CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (APT32 CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (APT32 CnC)
- [x] ET MALWARE Cayosin Botnet User-Agent Observed M1
- [x] ET MALWARE Peppy/KeeOIL Google Connectivity Check
- [ ] ET MALWARE Observed Malicious SSL Cert (BrushaLoader CnC)
- [x] ET MALWARE Win32/Remcos RAT Checkin 84
- [x] ET MALWARE OSX/Shlayer CnC Activity M1
- [x] ET MALWARE OSX/Shlayer CnC Activity M3
- [x] ET MALWARE Cayosin/Mirai CnC Domain in DNS Lookup
- [x] ET MALWARE Possible SharpShooter Framework Generated Script
- [x] ET MALWARE Observed Malicious SSL Cert (LazarusGroup CnC)
- [ ] ET MALWARE GanDownloader CnC Checkin
- [x] ET MALWARE TickGroup Datper CnC Checkin M2
- [x] ET MALWARE FBot Downloader Generic GET for ARM Payload
- [x] ET MALWARE BrushaLoader CnC DNS Lookup
- [x] ET MALWARE BrushaLoader CnC DNS Lookup
- [x] ET MALWARE BrushaLoader CnC DNS Lookup
- [x] ET MALWARE BrushaLoader CnC DNS Lookup
- [x] ET MALWARE BrushaLoader CnC DNS Lookup
- [x] ET MALWARE BrushaLoader CnC DNS Lookup
- [x] ET MALWARE BrushaLoader CnC DNS Lookup
- [x] ET MALWARE Observed Malicious SSL Cert (ServHelper RAT CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (ServHelper CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (ServHelper CnC)
- [x] ET MALWARE FlawedGrace CnC Activity
- [x] ET MALWARE APT DarkHydrus DNS Lookup 2
- [x] ET MALWARE APT DarkHydrus DNS Lookup 4
- [x] ET MALWARE APT DarkHydrus DNS Lookup 6
- [x] ET MALWARE APT DarkHydrus DNS Lookup 8
- [x] ET MALWARE APT DarkHydrus DNS Lookup 10
- [x] ET MALWARE APT DarkHydrus DNS Lookup 12
- [x] ET MALWARE APT DarkHydrus DNS Lookup 14
- [x] ET MALWARE APT DarkHydrus DNS Lookup 16
- [x] ET MALWARE APT DarkHydrus DNS Lookup 18
- [x] ET MALWARE APT DarkHydrus DNS Lookup 20
- [x] ET MALWARE APT DarkHydrus DNS Lookup 22
- [x] ET MALWARE APT DarkHydrus DNS Lookup 24
- [x] ET MALWARE Observed Malicious SSL Cert (ColdRiver APT DNSpionage MITM)
- [x] ET MALWARE Observed Malicious SSL Cert (ColdRiver APT DNSpionage MITM)
- [x] ET MALWARE Observed Malicious SSL Cert (ColdRiver APT DNSpionage MITM)
- [x] ET MALWARE Observed Cryptor Ransomware CnC Domain (e3kok4ekzalzapsf .onion .ws in TLS SNI)
- [x] ET MALWARE APT DarkHydrus DNS Lookup 25
- [x] ET MALWARE APT DarkHydrus DNS Lookup 27
- [x] ET MALWARE PS/PowerRatankba CnC DNS Lookup
- [x] ET MALWARE PS/PowerRatankba CnC DNS Lookup
- [x] ET MALWARE Observed Malicious SSL Cert (MageCart CnC)
- [x] ET MALWARE MageCart CnC Domain in SNI
- [x] ET MALWARE AtomLogger Exfil via FTP
- [x] ET MALWARE [PTsecurity] Bitter RAT C2 Response
- [x] ET MALWARE TeamBot CnC Activity
- [x] ET MALWARE [PTsecurity] Remcos RAT Checkin 86
- [x] ET MALWARE W32.Razy Inject Domain in DNS Lookup
- [x] ET MALWARE W32.Razy Inject Domain in DNS Lookup
- [x] ET MALWARE Observed Malicious SSL Cert (Donot Group/APT-C-35 CnC)
- [x] ET MALWARE [PTsecurity] Remcos RAT Checkin 87
- [x] ET MALWARE CoreDn CnC Checkin M1
- [x] ET MALWARE Observed Malicious SSL Cert (APT32 CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (APT32 CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (APT32 CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (APT32 CnC)
- [x] ET MALWARE Cayosin Botnet User-Agent Observed M2
- [x] ET MALWARE Observed CDC Ransomware User-Agent
- [x] ET MALWARE BrushaLoader CnC Domain in SNI
- [x] ET MALWARE Possible Astaroth User-Agent Observed
- [x] ET MALWARE OSX/Shlayer CnC Landing M2
- [x] ET MALWARE OSX/Shlayer CnC Activity M4
- [x] ET MALWARE DirectsX CnC Checkin
- [x] ET MALWARE Possible SharpShooter Framework Generated VBS Script
- [x] ET MALWARE Punto Loader Checkin
- [x] ET MALWARE TickGroup Datper CnC Checkin M1
- [x] ET MALWARE TickGroup Datper CnC Checkin M3
- [x] ET MALWARE BrushaLoader CnC DNS Lookup
- [x] ET MALWARE BrushaLoader CnC DNS Lookup
- [x] ET MALWARE BrushaLoader CnC DNS Lookup
- [x] ET MALWARE BrushaLoader CnC DNS Lookup
- [x] ET MALWARE BrushaLoader CnC DNS Lookup
- [x] ET MALWARE BrushaLoader CnC DNS Lookup
- [x] ET MALWARE BrushaLoader CnC DNS Lookup

☑ ET MALWARE BrushaLoader CnC DNS Lookup	☑ ET MALWARE BrushaLoader CnC DNS Lookup
☑ ET MALWARE BrushaLoader CnC DNS Lookup	☑ ET MALWARE BrushaLoader CnC DNS Lookup
☑ ET MALWARE BrushaLoader CnC DNS Lookup	☑ ET MALWARE BrushaLoader CnC DNS Lookup
☑ ET MALWARE BrushaLoader CnC DNS Lookup	☑ ET MALWARE BrushaLoader CnC DNS Lookup
☑ ET MALWARE BrushaLoader CnC DNS Lookup	☑ ET MALWARE BrushaLoader CnC DNS Lookup
☑ ET MALWARE BrushaLoader CnC DNS Lookup	☑ ET MALWARE BrushaLoader CnC DNS Lookup
☑ ET MALWARE BrushaLoader CnC DNS Lookup	☑ ET MALWARE BrushaLoader CnC DNS Lookup
☑ ET MALWARE BrushaLoader CnC DNS Lookup	☑ ET MALWARE BrushaLoader CnC DNS Lookup
☑ ET MALWARE BabyShark CnC Domain in SNI	☑ ET MALWARE DonotGroup/Patchwork CnC DNS Lookup
☑ ET MALWARE DonotGroup/Patchwork CnC DNS Lookup	☑ ET MALWARE ArtraDownloader CnC Checkin
☑ ET MALWARE OSX/Shlayer Malicious Download Request	☐ ET MALWARE JS/Agent.NZH CnC Response
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 11 CnC)	☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 11 CnC)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)	☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)	☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)	☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)	☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)	☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)	☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)	☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)	☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)	☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)	☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)	☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 4 CnC)	☐ ET MALWARE Win32/Kribat-A Downloader Activity
☑ ET MALWARE [PTsecurity] Win32/Spy.RTM/Redaman IP Check	☑ ET MALWARE Py/MechaFlounder CnC Checkin
☑ ET MALWARE Py/MechaFlounder CnC Activity - Reporting Sleep Command Success	☑ ET MALWARE Py/MechaFlounder CnC Activity - Reporting Download Command Success
☑ ET MALWARE Py/MechaFlounder CnC Activity - Reporting Download Command Error	☑ ET MALWARE Py/MechaFlounder CnC Activity - Reporting Upload Command Success
☑ ET MALWARE Py/MechaFlounder CnC Activity - Reporting Upload Command Error	☑ ET MALWARE Py/MechaFlounder CnC Activity - Reporting Directory Change Command Success
☑ ET MALWARE Chafer CnC DNS Query	☑ ET MALWARE Chafer CnC DNS Query
☑ ET MALWARE Sidewinder CnC DNS Query	☑ ET MALWARE MSIL/SkidRat CnC Checkin M1
☑ ET MALWARE FIN6 StealerOne CnC Domain in SNI	☑ ET MALWARE FIN6 StealerOne CnC DNS Query
☑ ET MALWARE MSIL/SkidRat User-Agent Observed	☑ ET MALWARE MSIL/SkidRat CnC Checkin M2
☑ ET MALWARE MSIL/SkidRat CnC Checkin M3	☑ ET MALWARE [AV] EarthWorm/Termite IoT Agent Reporting Infection
☑ ET MALWARE EarthWorm/Termite IoT Agent CnC Response	☐ ET MALWARE OSX/EvilOSX Client Receiving Commands
☑ ET MALWARE Observed Malicious SSL Cert (APT32 JEShell CnC)	☑ ET MALWARE Win32/Retadup CnC Checkin M1
☑ ET MALWARE Win32/Retadup CnC Checkin M2	☑ ET MALWARE Win32/Retadup Success Response from CnC
☑ ET MALWARE Win32/PirateMatryoshka CnC DNS Query	☑ ET MALWARE Observed Malicious SSL Cert (CobaltStrike CnC)
☑ ET MALWARE Win32/Termite Agent Implant CnC Checkin	☑ ET MALWARE Win32/Termite Agent Implant Keep-Alive
☑ ET MALWARE Possible Inbound PowerShell via Invoke-PSImage Stego	☑ ET MALWARE Observed Malicious SSL Cert (Gozi CnC)
☑ ET MALWARE Win32/Dorv Stealer Exfiltrating Data to CnC	☑ ET MALWARE Win32/Dorv InfoStealer CnC DNS Query
☑ ET MALWARE JasperLoader CnC Checkin	☑ ET MALWARE Observed Malicious SSL Cert (Gootkit CnC)
☑ ET MALWARE Inbound JasperLoader Using Array Push Obfuscation	☑ ET MALWARE ShadowHammer DNS Lookup
☑ ET MALWARE Possible ShadowHammer DNS Lookup	☑ ET MALWARE Possible ShadowHammer DNS Lookup
☑ ET MALWARE MSIL/DataMilk Stealer Communicating with CnC	☑ ET MALWARE ChaseBot CnC Checkin
☑ ET MALWARE Observed Malicious SSL Cert (ShadowHammer CnC)	☑ ET MALWARE W32/VBS.SLoad.Backdoor Initial Base64 Encoded OK Server Response
☑ ET MALWARE ELF/Mirai Variant UA Outbound (Rift)	☑ ET MALWARE ELF/Mirai Variant UA Inbound (Rift)
☑ ET MALWARE ELF/Mirai Variant UA Outbound (Tsunami)	☑ ET MALWARE ELF/Mirai Variant UA Inbound (Tsunami)
☑ ET MALWARE ELF/Mirai Variant UA Outbound (Yowai)	☑ ET MALWARE ELF/Mirai Variant UA Inbound (Yowai)
☑ ET MALWARE ELF/Mirai Variant UA Outbound (Yakuza)	☑ ET MALWARE ELF/Mirai Variant UA Inbound (Yakuza)
☑ ET MALWARE ELF/Mirai Variant UA Outbound (Hentai)	☑ ET MALWARE ELF/Mirai Variant UA Inbound (Hentai)
☑ ET MALWARE ELF/Mirai Variant UA Outbound (lessie)	☑ ET MALWARE ELF/Mirai Variant UA Inbound (lessie)
☑ ET MALWARE ELF/Mirai Variant UA Outbound (Cakle)	☑ ET MALWARE ELF/Mirai Variant UA Inbound (Cakle)
☑ ET MALWARE ELF/Mirai Variant UA Outbound (Damien)	☑ ET MALWARE ELF/Mirai Variant UA Inbound (Damien)
☑ ET MALWARE ELF/Mirai Variant UA Outbound (Solar)	☑ ET MALWARE ELF/Mirai Variant UA Inbound (Solar)
☑ ET MALWARE ELF/Mirai Variant UA Outbound (muhstik)	☑ ET MALWARE ELF/Mirai Variant UA Inbound (muhstik)
☑ ET MALWARE ELF/Mirai Variant UA Outbound (Shaolin)	☑ ET MALWARE ELF/Mirai Variant UA Inbound (Shaolin)
☑ ET MALWARE MalDoc Request for Payload (TA505 Related)	☑ ET MALWARE Xwo CnC Activity
☑ ET MALWARE Win32/Beapy/Lemon_Duck CnC Checkin	☑ ET MALWARE PS/Beapy CnC Checkin
☑ ET MALWARE Py/Beapy CnC Checkin	☑ ET MALWARE ELF.Initdz.Coinminer C2 Systeminfo (D2)
☑ ET MALWARE AHK/BKDR_HTV.ZKGD-A CnC Checkin	☑ ET MALWARE AHK/BKDR_HTV.ZKGD-A Fake HTTP 500 Containing Encoded Commands Inbound

- [x] ET MALWARE Observed Malicious SSL Cert (Gozi CnC)
- [x] ET MALWARE DNS Query for Known Malicious Domain Observed Serving Various Phish Campaigns
- [x] ET MALWARE DNS Query for Known Malicious Domain Observed Serving Various Phish Campaigns
- [x] ET MALWARE DNS Query for Known Malicious Domain Observed Serving Various Phish Campaigns
- [x] ET MALWARE DNS Query for Known Malicious Domain Observed Serving Various Phish Campaigns
- [x] ET MALWARE DustySky/Gaza Cybergang Group1 CnC Domain in DNS Lookup (time-loss .dns05 .com)
- [x] ET MALWARE Outbound POST Request with ps PowerShell Command Output
- [x] ET MALWARE Outbound POST Request with Base64 ps PowerShell Command Output M2
- [x] ET MALWARE Observed Malicious SSL Cert (DonotGroup CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (DonotGroup CnC)
- [x] ET MALWARE DonotGroup CnC Domain in DNS Lookup (drinkeatgood .space)
- [ ] ET MALWARE Observed Malicious SSL Cert (Unattributed CnC)
- [x] ET MALWARE Unattributed CnC Domain in DNS Lookup (xsecuremail .com)
- [x] ET MALWARE Unattributed CnC Domain in DNS Lookup (microsoftonline-secure-login .com)
- [x] ET MALWARE Unattributed CnC Domain in DNS Lookup (encrypt-email .online)
- [x] ET MALWARE Unattributed CnC Domain in DNS Lookup (internal-message .app)
- [x] ET MALWARE StealerNeko CnC Checkin
- [x] ET MALWARE APT DNSpionage/Karkoff CnC Domain in DNS Lookup
- [x] ET MALWARE APT DNSpionage/Karkoff CnC Domain in DNS Lookup
- [x] ET MALWARE Suspected Powershell Empire GET M1
- [x] ET MALWARE DonotGroup CnC Domain in DNS Lookup
- [x] ET MALWARE DonotGroup CnC Domain in DNS Lookup
- [x] ET MALWARE DonotGroup CnC Domain in DNS Lookup
- [x] ET MALWARE Observed Malicious SSL Cert (DonotGroup Stage 2 CnC)
- [x] ET MALWARE ServHelper CnC Command (Net User)
- [x] ET MALWARE ServHelper CnC Command (Whoami)
- [x] ET MALWARE ServHelper CnC Domain
- [x] ET MALWARE ServHelper CnC Domain
- [x] ET MALWARE ServHelper CnC Domain
- [ ] ET MALWARE AridViper CnC Domain in SNI
- [x] ET MALWARE IcedID Fake Resume Server in DNS Lookup
- [x] ET MALWARE Observed Malicious SSL Cert (ReactGet Group)
- [x] ET MALWARE Observed Malicious SSL Cert (Mirrortheif group)
- [x] ET MALWARE Covenant .NET Framework P2P C&C Protocol Gruntsvc Named Pipe Interaction
- [x] ET MALWARE Wide HTA with PowerShell Execution Inbound
- [x] ET MALWARE CSharp SMB Scanner Assembly in PowerShell Inbound M2
- [x] ET MALWARE Observed Malicious SSL Cert (MirrorThief CnC)
- [x] ET MALWARE ELF.SystemdMiner C2 Domain in DNS Lookup
- [x] ET MALWARE MSIL/Almashreq CnC Checkin
- [x] ET MALWARE Observed Malicious SSL Cert (MirrorThief CnC)
- [x] ET MALWARE Winnti Payload - XORed Check-in to Infected System (0xd4413890)
- [x] ET MALWARE BlackTech Plead Encrypted Payload Inbound
- [x] ET MALWARE Mirai Variant Checkin Response
- [x] ET MALWARE Unknown VBScript Loader with Encoded PowerShell Execution Inbound
- [x] ET MALWARE Shade Ransomware Payment Domain in DNS Lookup
- [ ] ET MALWARE Win32/ProtonBot CnC Response
- [x] ET MALWARE DNS Query for Known Malicious Domain Observed Serving Various Phish Campaigns
- [x] ET MALWARE DNS Query for Known Malicious Domain Observed Serving Various Phish Campaigns
- [x] ET MALWARE DNS Query for Known Malicious Domain Observed Serving Various Phish Campaigns
- [x] ET MALWARE DNS Query for Known Malicious Domain Observed Serving Various Phish Campaigns
- [x] ET MALWARE DNS Query for Known Malicious Domain Observed Serving Various Phish Campaigns
- [x] ET MALWARE DustySky/Gaza Cybergang Group1 CnC Domain in DNS Lookup (dji-msi .2waky .com)
- [x] ET MALWARE Outbound POST Request with Base64 ps PowerShell Command Output M1
- [x] ET MALWARE Outbound POST Request with Base64 ps PowerShell Command Output M3
- [x] ET MALWARE Observed Malicious SSL Cert (DonotGroup CnC)
- [x] ET MALWARE DonotGroup CnC Domain in DNS Lookup (drivethrough .top)
- [x] ET MALWARE Observed Malicious SSL Cert (Unattributed CnC)
- [ ] ET MALWARE Observed Malicious SSL Cert (Unattributed CnC)
- [x] ET MALWARE Unattributed CnC Domain in DNS Lookup (wipro365 .com)
- [x] ET MALWARE Unattributed CnC Domain in DNS Lookup (secure-message .online)
- [x] ET MALWARE Unattributed CnC Domain in DNS Lookup (secured-mail .online)
- [x] ET MALWARE Unattributed CnC Domain in DNS Lookup (encrypted-message .cloud)
- [ ] ET MALWARE Baldr Stealer Checkin M2
- [x] ET MALWARE APT DNSpionage/Karkoff CnC Domain in DNS Lookup
- [x] ET MALWARE Suspected Powershell Empire POST M1
- [x] ET MALWARE Novaloader Stage 2 VBS Request
- [x] ET MALWARE DonotGroup CnC Domain in DNS Lookup
- [x] ET MALWARE Megumin v2 Stealer User-Agent
- [x] ET MALWARE DonotGroup Stage 2 CnC Domain in DNS Lookup
- [x] ET MALWARE Observed Malicious SSL Cert (DonotGroup CnC)
- [x] ET MALWARE ServHelper CnC Command (Reg Add)
- [x] ET MALWARE ServHelper CnC Domain
- [x] ET MALWARE ServHelper CnC Domain
- [x] ET MALWARE ServHelper CnC Domain
- [x] ET MALWARE JAR/Qealler Stealer HTTP Headers Observed
- [x] ET MALWARE Win32/Krypton Stealer CnC Checkin
- [x] ET MALWARE Observed Malicious DNS Query (ReactGet Group)
- [x] ET MALWARE Observed Malicious DNS Query (Mirrorthief Group)
- [x] ET MALWARE CobaltStrike SMB P2P Default Msagent Named Pipe Interaction
- [x] ET MALWARE PS/Unk.EB.Spreader CnC Checkin
- [x] ET MALWARE CSharp SMB Scanner Assembly in PowerShell Inbound M1
- [x] ET MALWARE Win32/ElectricFish Authentication Packet Observed
- [x] ET MALWARE MirrorThief CnC Domain in DNS Lookup
- [x] ET MALWARE ELF.SystemdMiner C2 Domain in DNS Lookup
- [x] ET MALWARE MSIL/Almashreq Executing New Processes
- [x] ET MALWARE MirrorThief CnC in DNS Lookup
- [ ] ET MALWARE BlackTech Plead CnC in DNS Lookup
- [x] ET MALWARE HTA.BabyShark Checkin
- [x] ET MALWARE Suspected ExtraPulsar Backdoor
- [x] ET MALWARE HTA.BabyShark HTTP Exfil
- [x] ET MALWARE SSL/TLS Certificate Observed (Quasar Related)
- [x] ET MALWARE Win32/ProtonBot Stealer Activity

- [x] ET MALWARE Observed ProtonBot User-Agent
- [x] ET MALWARE Observed DNS Query to APT10 Related CnC Domain
- [x] ET MALWARE Observed DNS Query to APT10 Related CnC Domain
- [x] ET MALWARE Observed DNS Query to APT10 Related CnC Domain
- [x] ET MALWARE Maze/ID Ransomware Activity
- [x] ET MALWARE Linux/HiddenWasp CnC Request (set)
- [x] ET MALWARE Linux/HiddenWasp CnC Response
- [x] ET MALWARE DarkHotel Payload Uploading to CnC
- [x] ET MALWARE DarkHotel CnC Domain in DNS Lookup
- [x] ET MALWARE DarkHotel CnC Domain in DNS Lookup
- [x] ET MALWARE DarkHotel CnC Domain in DNS Lookup
- [x] ET MALWARE Executable contained in DICOM Medical Image SMB File Transfer
- [x] ET MALWARE Executable contained in DICOM Medical Image PACS DICOM Protocol Transfer
- [x] ET MALWARE Executable contained in DICOM Medical Image Received from PACS DICOM Device
- [x] ET MALWARE Possible APT28 Xtunnel Activity
- [x] ET MALWARE APT28 CnC Domain DNS Lookup
- [x] ET MALWARE APT28 CnC Domain DNS Lookup
- [x] ET MALWARE APT28 CnC Domain DNS Lookup
- [x] ET MALWARE APT28 CnC Domain DNS Lookup
- [x] ET MALWARE APT28 CnC Domain DNS Lookup
- [x] ET MALWARE APT28 CnC Domain DNS Lookup
- [ ] ET MALWARE Observed Malicious SSL Cert (BrushaLoader CnC) 2019-05-30
- [x] ET MALWARE ICEFOG-P Variant CnC Checkin M1
- [x] ET MALWARE ICEFOG-P Variant CnC Checkin M2
- [x] ET MALWARE PLATINUM Steganographic HTTP Response Page Inbound
- [x] ET MALWARE Win32/Phorpiex Template 3 Active - Outbound Malicious Email Spam
- [x] ET MALWARE Win32/Phorpiex Template 4 Active - Outbound Malicious Email Spam
- [x] ET MALWARE HAWKBALL CnC Initial Request
- [x] ET MALWARE HAWKBALL CnC Activity
- [x] ET MALWARE HAWKBALL CnC Sending System Information
- [x] ET MALWARE Observed Buran Ransomware UA (BURAN)
- [x] ET MALWARE Observed Buran Ransomware UA (GHOST)
- [ ] ET MALWARE Buran Ransomware Activity M2
- [x] ET MALWARE Buran Ransomware Activity M1
- [x] ET MALWARE WSHRAT CnC Checkin
- [x] ET MALWARE WSHRAT Keylogger Module Download Command Inbound
- [x] ET MALWARE WSHRAT Credential Dump Module Download Command Inbound
- [x] ET MALWARE Possible Encoded Wide PowerShell (IEX) in Certificate Inbound
- [x] ET MALWARE Observed Malicious SSL Cert (FIN8 ShellTea CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (FIN8 ShellTea CnC)
- [x] ET MALWARE FIN8 ShellTea CnC in DNS Lookup
- [x] ET MALWARE FIN8 ShellTea CnC in DNS Lookup
- [x] ET MALWARE FIN8 ShellTea CnC in DNS Lookup
- [x] ET MALWARE FIN8 ShellTea CnC in DNS Lookup
- [x] ET MALWARE FIN8 ShellTea CnC in DNS Lookup
- [x] ET MALWARE Win32/Vools Variant CnC Checkin
- [x] ET MALWARE Observed Malicious SSL Cert (MageCart CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (MageCart CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (MageCart CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (MageCart CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (MageCart CnC)
- [x] ET MALWARE SSL/TLS Certificate Observed (Maldoc CnC)
- [x] ET MALWARE Packed Perl with Eval Statement
- [x] ET MALWARE Chafer Win32/TREKX Uploading to CnC
- [x] ET MALWARE Chafer Win32/TREKX Uploading to CnC (Modified CAB)
- [x] ET MALWARE Chafer CnC Domain in DNS Lookup
- [x] ET MALWARE Chafer CnC Domain in DNS Lookup
- [x] ET MALWARE Chafer CnC Domain in DNS Lookup
- [x] ET MALWARE Observed Malicious SSL Cert (IcedID CnC)
- [x] ET MALWARE Danabot CnC Checkin
- [x] ET MALWARE Plurox CnC Domain in DNS Lookup
- [x] ET MALWARE Plurox CnC Domain in DNS Lookup
- [x] ET MALWARE Danabot UA Observed
- [x] ET MALWARE Observed Turla Domain (vision2030 .tk in TLS SNI)
- [x] ET MALWARE Turla DNS Lookup (vision2030 .cf)
- [x] ET MALWARE Observed Malicious UA (Skuxray)
- [x] ET MALWARE Win32/Plurox Backdoor CnC Checkin
- [x] ET MALWARE Linux.Ngioweb Stage 1 CnC Activity Client Request (set)
- [x] ET MALWARE Linux.Ngioweb Stage 1 CnC Activity Server Response (WAIT)
- [x] ET MALWARE Linux.Ngioweb Stage 1 CnC Activity Server Response (CONNECT)
- [x] ET MALWARE Linux.Ngioweb Stage 1 CnC Activity Server Response (DISCONNECT)
- [x] ET MALWARE Linux.Ngioweb Stage 1 CnC Activity Server Response (CERT)
- [x] ET MALWARE Possible PowerShell Empire Activity Outbound
- [x] ET MALWARE HYDSEVEN VBS CnC Host Information Checkin
- [x] ET MALWARE DonotGroup APT CnC Domain in DNS Lookup
- [x] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [x] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [x] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [x] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [x] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [x] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [x] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [x] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [x] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
- [ ] ET MALWARE Gift Cardshark CnC Domain in DNS Lookup

☐ ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
☐ ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
☐ ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
☐ ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
☐ ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
☐ ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
☐ ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE Win32/Unk HeavensGate Loader CnC in DNS Lookup
☑ ET MALWARE Win32/Unk HeavensGate Loader CnC in DNS Lookup
☑ ET MALWARE APT32 CnC in DNS Lookup
☑ ET MALWARE APT32 Win32/Ratsnif Submitting Output of Command to CnC
☑ ET MALWARE APT32 Win32/Ratsnif CnC Checkin
☑ ET MALWARE Operation Tripoli Related CnC Checkin
☐ ET MALWARE Observed Godlua Backdoor Domain (dd .heheda .tk in TLS SNI)
☑ ET MALWARE Observed Godlua Backdoor Domain (c .heheda .tk in TLS SNI)
☐ ET MALWARE Observed Godlua Backdoor Domain (d .cloudappconfig .com in TLS SNI)
☑ ET MALWARE Observed Turla/APT34 CnC Domain Domain (dubaiexpo2020 .cf in TLS SNI)
☑ ET MALWARE Godlua Backdoor Stage-3 Client Heartbeat (Jun 2019-Dec 2019) (set)
☑ ET MALWARE Godlua Backdoor Stage-3 Client Heartbeat (Jul 2020-Jan 2021) (set)
☑ ET MALWARE Godlua Backdoor Stage-3 Server Heartbeat Reply (Sep 2020 - Nov 2023)
☑ ET MALWARE Known Malicious Server in DNS Lookup (updatecache .com)
☑ ET MALWARE MuddyWater Payload Sending Command Output to CnC
☑ ET MALWARE MuddyWater Payload Requesting Command from CnC
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Inter Skimmer CnC Domain in DNS Lookup
☑ ET MALWARE Inter Skimmer CnC Domain in DNS Lookup
☑ ET MALWARE Inter Skimmer CnC Domain in DNS Lookup
☑ ET MALWARE Win32/Unk.VBScript Requesting Instruction from CnC
☑ ET MALWARE eCh0raix/QNAPCrypt CnC Activity - Started
☑ ET MALWARE eCh0raix/QNAPCrypt Requesting Key/Wallet/Note
☑ ET MALWARE Possible APT Sarhurst/Husar/Hussarini/Hassar CnC Check Response
☑ ET MALWARE Possible APT Sarhurst/Husar/Hussarini/Hassar CnC POST
☑ ET MALWARE SSL/TLS Certificate Observed (StrongPity)
☑ ET MALWARE SSL/TLS Certificate Observed (StrongPity)
☑ ET MALWARE SSL/TLS Certificate Observed (StrongPity)
☑ ET MALWARE SSL/TLS Certificate Observed (StrongPity)
☑ ET MALWARE SLUB Domain in DNS Lookup
☑ ET MALWARE Gamaredon CnC Domain in DNS Lookup
☑ ET MALWARE Gamaredon CnC Domain in DNS Lookup
☐ ET MALWARE Windigo SSH Connection Received (Ebury < 1.7.0)

☐ ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
☐ ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
☐ ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
☐ ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
☐ ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
☐ ET MALWARE Gift Cardshark CnC Domain in DNS Lookup
☑ ET MALWARE Observed Malicious SSL Cert (Quasar CnC)
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE APT33 CnC Domain in DNS Lookup
☑ ET MALWARE Win32/Unk HeavensGate Loader CnC in DNS Lookup
☑ ET MALWARE APT32 CnC in DNS Lookup
☑ ET MALWARE APT32 Win32/Ratsnif POSTing Log Message to CnC
☑ ET MALWARE APT32 Win32/Ratsnif Requesting Command from CnC
☑ ET MALWARE Win32/Remcos RAT Checkin 109
☐ ET MALWARE Observed Godlua Backdoor Domain (helegedada .github .io in TLS SNI)
☑ ET MALWARE Observed Godlua Backdoor Domain (d .heheda .tk in TLS SNI)
☐ ET MALWARE Observed Godlua Backdoor Domain (dd .cloudappconfig .com in TLS SNI)
☐ ET MALWARE Observed Godlua Backdoor Domain (c .cloudappconfig .com in TLS SNI)
☑ ET MALWARE Observed Malicious SSL Cert (Turla/APT34 CnC Domain)
☑ ET MALWARE Godlua Backdoor Stage-3 Client Heartbeat (Dec 2019-Jul 2020) (set)
☑ ET MALWARE Godlua Backdoor Stage-3 Server Heartbeat Reply (Jun 2019 - Sep 2020)
☑ ET MALWARE Godlua Backdoor Downloading Encrypted Lua
☑ ET MALWARE MuddyWater Payload Sending Screenshot to CnC
☑ ET MALWARE MuddyWater Payload Registering with CnC
☑ ET MALWARE MuddyWater Payload CnC Checkin
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Inter Skimmer CnC Domain in DNS Lookup
☑ ET MALWARE Inter Skimmer CnC Domain in DNS Lookup
☑ ET MALWARE VBA/TrojanDownloader.Agent.PAC Retreiving Malicious VBScript
☑ ET MALWARE Amadey CnC Check-In
☑ ET MALWARE eCh0raix/QNAPCrypt CnC Activity - Done
☑ ET MALWARE eCh0raix/QNAPCrypt Successful Server Response
☑ ET MALWARE Possible APT Sarhurst/Husar/Hussarini/Hassar CnC Command Response
☑ ET MALWARE Possible APT Sarhurst/Husar/Hussarini/Hassar CnC GET
☑ ET MALWARE SSL/TLS Certificate Observed (StrongPity)
☑ ET MALWARE SSL/TLS Certificate Observed (StrongPity)
☑ ET MALWARE SSL/TLS Certificate Observed (StrongPity)
☑ ET MALWARE SSL/TLS Certificate Observed (StrongPity)
☑ ET MALWARE Gamaredon CnC Domain in DNS Lookup
☑ ET MALWARE Gamaredon CnC Domain in DNS Lookup
☑ ET MALWARE Win32/Ketrican CnC Activity
☐ ET MALWARE Windigo SSH Connection Received (Ebury > 1.7.0)

- [x] ET MALWARE Win32/Blacknix CnC Checkin
- [x] ET MALWARE Win32/Blacknix CnC Heartbeat
- [x] ET MALWARE Proyecto RAT Variant - Yopmail Login attempt (set)
- [x] ET MALWARE Proyecto RAT Variant - Yopmail Stage 2 CnC Retrieval
- [x] ET MALWARE Possible Outbound WebShell GIF
- [x] ET MALWARE Possible Outbound WebShell JPEG
- [x] ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
- [x] ET MALWARE FIN8 ShellTea CnC in DNS Query
- [x] ET MALWARE FIN8 ShellTea CnC in DNS Query
- [x] ET MALWARE FIN8 ShellTea CnC in DNS Query
- [x] ET MALWARE FIN8 ShellTea CnC in DNS Query
- [x] ET MALWARE FIN8 ShellTea CnC in DNS Query
- [x] ET MALWARE FIN8 ShellTea CnC in DNS Query
- [x] ET MALWARE FIN8 ShellTea CnC in DNS Query
- [x] ET MALWARE FIN8 ShellTea CnC in DNS Query
- [x] ET MALWARE [GIGAMON_ATR] FIN8 BADHATCH CnC Checkin
- [x] ET MALWARE [GIGAMON_ATR] FIN8 BADHATCH Remote Shell Banner
- [x] ET MALWARE LooCipher Ransomware Onion Domain
- [x] ET MALWARE Observed Malicious SSL Cert (Various CnC)
- [x] ET MALWARE Possible ICMP Backdoor Tunnel Command - whoami
- [x] ET MALWARE Phorpiex CnC Domain in DNS Lookup
- [x] ET MALWARE Win32/ArtraDownloader Checkin
- [x] ET MALWARE Win32/Phorpiex Template 5 Active - Outbound Malicious Email Spam
- [x] ET MALWARE Covenant Framework HTTP Beacon
- [x] ET MALWARE Covenant Framework Default HTTP Beacon
- [x] ET MALWARE Possible Covenant Framework Grunt Stager HTTP Download (Grunt.GruntStager)
- [x] ET MALWARE Covenant Framework HTTP Hello World Server Response
- [x] ET MALWARE Possible Covenant Framework Grunt PowerShell Stager HTTP Download
- [x] ET MALWARE Possible Covenant Framework Grunt Stager HTTP Download (DynamicInvoke)
- [x] ET MALWARE Observed Malicious SSL Cert (AZORult CnC)
- [x] ET MALWARE Possible Covenant Framework Grunt MSBuild Stager HTTP Download
- [x] ET MALWARE Observed Malicious SSL Cert (Various CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (Various CnC)
- [ ] ET MALWARE Win32/Eris Ransomware CnC Checkin
- [x] ET MALWARE Win32/Onliner CnC Checkin
- [x] ET MALWARE Win32/Onliner Receiving Commands from CnC
- [x] ET MALWARE Win32/Onliner Requesting Additional Modules
- [ ] ET MALWARE Win32/Onliner Mailer Module Communicating with CnC
- [x] ET MALWARE Win32/Onliner Template 1 Active - Malicious Outbound Email Spam
- [x] ET MALWARE Nyanw0rm CnC Keep-Alive (Outbound) M1
- [x] ET MALWARE Nyanw0rm CnC Keep-Alive (Outbound) M2
- [x] ET MALWARE Win32/Varenyky Spambot CnC in DNS Query
- [x] ET MALWARE Win32/Varenyky Spambot CnC in DNS Query
- [x] ET MALWARE Win32/Varenyky Spambot CnC in DNS Query
- [x] ET MALWARE Win32/Varenyky Spambot CnC in DNS Query
- [x] ET MALWARE Win32/Varenyky Spambot CnC in DNS Query
- [x] ET MALWARE Win32/Varenyky Spambot CnC in DNS Query
- [x] ET MALWARE HVNC USR Init Detected
- [x] ET MALWARE HVNC BOT Detected
- [x] ET MALWARE ELF/Emptiness v1 CnC Checkin
- [x] ET MALWARE ELF/Emptiness v1.1 CnC Checkin
- [x] ET MALWARE ELF/Emptiness v2 XOR (b2bb01039307baa2) CnC Checkin
- [x] ET MALWARE ELF/Emptiness v1 UDP Flood Command Inbound
- [x] ET MALWARE ELF/Emptiness v1 DNS Flood Command Inbound
- [x] ET MALWARE ELF/Emptiness v1 HTTP Flood Command Inbound
- [x] ET MALWARE ELF/Emptiness v1.1 UDP Flood Command Inbound
- [x] ET MALWARE ELF/Emptiness v1.1 DNS Flood Command Inbound
- [x] ET MALWARE ELF/Emptiness v1.1 HTTP Flood Command Inbound
- [x] ET MALWARE ELF/Emptiness v2 XOR UDP Flood Command Inbound
- [x] ET MALWARE ELF/Emptiness v2 XOR DNS Flood Command Inbound
- [x] ET MALWARE ELF/Emptiness v2 XOR HTTP Flood Command Inbound
- [x] ET MALWARE ELF/Emptiness v2 XOR Exec Command Inbound
- [x] ET MALWARE ELF/Emptiness v2 XOR Update Command Inbound
- [x] ET MALWARE ELF/Mirai.shiina v3 CnC Checkin
- [x] ET MALWARE ELF/Emptiness CnC Domain in DNS Query
- [x] ET MALWARE ELF/Emptiness CnC Domain in DNS Query
- [x] ET MALWARE ELF/Emptiness CnC Domain in DNS Query
- [x] ET MALWARE ELF/Emptiness CnC Domain in DNS Query
- [x] ET MALWARE ELF/Emptiness CnC Domain in DNS Query
- [x] ET MALWARE ELF/Emptiness CnC Domain in DNS Query
- [x] ET MALWARE ELF/Mirai.shiina CnC Domain in DNS Query
- [x] ET MALWARE APT Related - BLACKCOFFEE Command Delimiters in HTTP Response M1
- [x] ET MALWARE APT Related - BLACKCOFFEE Command Delimiters in HTTP Response M2
- [x] ET MALWARE MedusaHTTP Variant CnC Checkin
- [x] ET MALWARE Win32/DarkRAT CnC Activity
- [x] ET MALWARE [TGI] Py.Machete HTTP CnC Exfil
- [x] ET MALWARE [TGI] Py.Machete FTP Exfil 1
- [x] ET MALWARE [TGI] Py.Machete FTP Exfil 2
- [x] ET MALWARE Win32/Dostre CnC Activity
- [x] ET MALWARE Clipsa Stealer - CnC Checkin
- [x] ET MALWARE Clipsa Stealer - Coinminer Download
- [x] ET MALWARE Clipsa Stealer - Exfiltration Activity
- [x] ET MALWARE BalkanDoor CnC Checkin
- [x] ET MALWARE BalkanDoor CnC Checkin - Server Response
- [x] ET MALWARE MyKings Bootloader Variant Requesting Payload M1
- [x] ET MALWARE MyKings Bootloader Variant Requesting Payload M2
- [x] ET MALWARE MyKings Bootloader Variant Requesting Payload M3
- [x] ET MALWARE TwoFace WebShell Detected
- [x] ET MALWARE GlitchPOS CnC Checkin
- [x] ET MALWARE Win32/Nemty Ransomware Style Geo IP Check M1
- [x] ET MALWARE Win32/Nemty Ransomware Style Geo IP Check M2
- [x] ET MALWARE Win32/Alpha Stealer v1.5 PWS Exfil via HTTP
- [x] ET MALWARE LYCEUM MSIL/DanBot CnC Checkin
- [x] ET MALWARE LYCEUM CnC Domain Observed in DNS Query
- [x] ET MALWARE LYCEUM CnC Domain Observed in DNS Query
- [x] ET MALWARE LYCEUM CnC Domain Observed in DNS Query
- [x] ET MALWARE LYCEUM CnC Domain Observed in DNS Query
- [x] ET MALWARE LYCEUM CnC Domain Observed in DNS Query
- [x] ET MALWARE LYCEUM CnC Domain Observed in DNS Query
- [x] ET MALWARE LYCEUM CnC Domain Observed in DNS Query
- [x] ET MALWARE Domen SocEng Redirect - Landing Page Observed
- [x] ET MALWARE Domen SocEng CnC Observed in DNS Query
- [x] ET MALWARE Domen SocEng CnC Observed in DNS Query
- [x] ET MALWARE Possible APT28 Maldoc CnC Checkin
- [x] ET MALWARE Win32/Laturo Stealer CnC Checkin
- [x] ET MALWARE Observed Glupteba CnC Domain (venoxcontrol .com in TLS SNI)

- [x] ET MALWARE Glupteba CnC Domain in DNS Lookup
- [x] ET MALWARE Glupteba CnC Domain in DNS Lookup
- [x] ET MALWARE Glupteba CnC Domain in DNS Lookup
- [x] ET MALWARE Glupteba CnC Domain in DNS Lookup
- [x] ET MALWARE HTTP Request for Possible ELF/LiLocked Ransomware Note
- [x] ET MALWARE Possible PHP.MAILER WebShell Generic Request Inbound
- [x] ET MALWARE [TGI] BlackRAT Checkin
- [x] ET MALWARE Observed Malicious SSL Cert (Sidewinder CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (Sidewinder CnC)
- [x] ET MALWARE Possible TransparentTribe APT CnC Activity
- [x] ET MALWARE Suspected Tunna Proxy M2
- [x] ET MALWARE Suspected Tunna Proxy M4
- [x] ET MALWARE Possible Tunna Proxy Closing Connection
- [x] ET MALWARE Suspected Tunna Proxy M2 (Outbound)
- [x] ET MALWARE Suspected Tunna Proxy M4 (Outbound)
- [x] ET MALWARE Possible Tunna Proxy Closing Connection
- [x] ET MALWARE Observed Malicious SSL Cert (DonotGroup CnC)
- [x] ET MALWARE DonotGroup CnC Observed in DNS Query
- [x] ET MALWARE [TGI] Cobalt Strike Malleable C2 Response (O365 Profile) M2
- [x] ET MALWARE [TGI] Cobalt Strike Malleable C2 Request (YouTube Profile)
- [x] ET MALWARE Glupteba CnC Observed in DNS Query
- [x] ET MALWARE Glupteba CnC Observed in DNS Query
- [ ] ET MALWARE Win32/Tflower Ransomware CnC Checkin
- [x] ET MALWARE Plead TSCookie CnC Checkin M1
- [x] ET MALWARE Plead TSCookie CnC Checkin M3
- [x] ET MALWARE Possible GhostMiner CCBOT Component - CnC Checkin
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE DonotGroup CnC Domain Observed in DNS Query
- [x] ET MALWARE Tortoiseshell/SysKit CnC Activity
- [x] ET MALWARE OSX/GMERA.B CnC Checkin
- [x] ET MALWARE DonotGroup CnC Domain Observed in DNS Query
- [x] ET MALWARE Possible DeadlyKiss APT CnC Domain Observed in DNS Query
- [x] ET MALWARE PHPStudy CnC Domain in DNS Lookup
- [x] ET MALWARE Win32/Flooder.Agent.NAS CnC Domain in DNS Lookup
- [x] ET MALWARE DNSBin Demo - Data Inbound
- [x] ET MALWARE DNSChanger CnC Domain in DNS Lookup
- [x] ET MALWARE DNSChanger CnC Domain in DNS Lookup
- [x] ET MALWARE Possible Win32/Get2 Downloader Activity
- [x] ET MALWARE Win32/Phoenix Keylogger Exfil via SMTP - Generic
- [x] ET MALWARE Win32/Phoenix Keylogger SMTP Exfil - Clipboard
- [x] ET MALWARE Nemours/Proyecto RAT CnC Checkin
- [x] ET MALWARE Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-03
- [x] ET MALWARE Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-02
- [x] ET MALWARE Observed Malicious SSL Cert (AZORult CnC Server) 2019-09-30
- [x] ET MALWARE Observed Malicious SSL Cert (AZORult CnC Server) in SNI 2019-09-27
- [x] ET MALWARE CASHY200 CnC Domain in DNS Lookup
- [x] ET MALWARE CASHY200 CnC Domain in DNS Lookup
- [x] ET MALWARE CASHY200 Style DNS Query - Initial Hello Beacon
- [x] ET MALWARE CASHY200 Style DNS Query - Sending Number of Queries
- [x] ET MALWARE CASHY200 Style DNS Query - Getting CnC Data
- [x] ET MALWARE Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-08

- [x] ET MALWARE Glupteba CnC Domain in DNS Lookup
- [x] ET MALWARE Glupteba CnC Domain in DNS Lookup
- [x] ET MALWARE Glupteba CnC Domain in DNS Lookup
- [x] ET MALWARE Glupteba CnC Domain in DNS Lookup
- [x] ET MALWARE ELF/LiLocked Ransom Note in HTTP Response
- [x] ET MALWARE Possible PHP.MAILER WebShell Register Shutdown Function Request Inbound
- [x] ET MALWARE [TGI] BlackRAT Checkin Response
- [x] ET MALWARE Observed Malicious SSL Cert (Sidewinder CnC)
- [x] ET MALWARE TransparentTribe APT Maldoc CnC Checkin
- [x] ET MALWARE Suspected Tunna Proxy M1
- [x] ET MALWARE Suspected Tunna Proxy M3
- [x] ET MALWARE Possible Tunna Proxy Activity (Response)
- [x] ET MALWARE Suspected Tunna Proxy M1 (Outbound)
- [x] ET MALWARE Suspected Tunna Proxy M3 (Outbound)
- [x] ET MALWARE Possible Tunna Proxy Activity (Response)
- [x] ET MALWARE Observed Malicious SSL Cert (DonotGroup CnC)
- [x] ET MALWARE DonotGroup CnC Observed in DNS Query
- [x] ET MALWARE [TGI] Cobalt Strike Malleable C2 Request (O365 Profile)
- [x] ET MALWARE [TGI] Cobalt Strike Malleable C2 Response (YouTube Profile)
- [x] ET MALWARE Glupteba CnC Observed in DNS Query
- [x] ET MALWARE Glupteba CnC Observed in DNS Query
- [x] ET MALWARE Observed Malicious SSL Cert (MalDoc DL 2019-09-17 1)
- [x] ET MALWARE Observed Cobalt Strike User-Agent
- [x] ET MALWARE Plead TSCookie CnC Checkin M2
- [x] ET MALWARE Plead TSCookie CnC Checkin M4
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE DonotGroup CnC Domain Observed in DNS Query
- [x] ET MALWARE Tortoiseshell/HMH Download Request
- [x] ET MALWARE Observed OSX/GMERA.A CnC Domain (appstockfolio .com in TLS SNI)
- [x] ET MALWARE Observed Malicious SSL Cert (DonotGroup CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (DeadlyKiss APT)
- [x] ET MALWARE Possible DeadlyKiss APT CnC Domain Observed in DNS Query
- [x] ET MALWARE DNSG - Data Exfiltration via DNS
- [x] ET MALWARE DNSBin Demo - Data Exfil
- [x] ET MALWARE DNSChanger CnC Domain in DNS Lookup
- [x] ET MALWARE DNSChanger CnC Domain in DNS Lookup
- [x] ET MALWARE DNSChanger CnC Domain in DNS Lookup
- [x] ET MALWARE Win32/Phoenix Keylogger SMTP Exfil - Passwords
- [x] ET MALWARE Win32/Phoenix Keylogger SMTP Exfil - Logs
- [x] ET MALWARE Win32/Phoenix Keylogger SMTP Exfil - Screenshot
- [x] ET MALWARE Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-07
- [x] ET MALWARE Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-03
- [x] ET MALWARE Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-01
- [x] ET MALWARE Observed Malicious SSL Cert (AZORult Cnc Server) 2019-09-27
- [x] ET MALWARE DonotGroup CnC Domain Observed in DNS Query
- [x] ET MALWARE CASHY200 CnC Domain in DNS Lookup
- [x] ET MALWARE CASHY200 CnC Domain in DNS Lookup
- [x] ET MALWARE CASHY200 Style DNS Query - Sending Hostname
- [x] ET MALWARE CASHY200 Style DNS Query - Finished Sending Results
- [x] ET MALWARE CASHY200 Style DNS Query - Sending Command Results
- [x] ET MALWARE Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-08

- [x] ET MALWARE CASHY200 Style DNS Query - Request Command Beacon
- [x] ET MALWARE NSO Group Pegasus CnC Domain Observed in DNS Query
- [x] ET MALWARE NSO Group Pegasus CnC Domain Observed in DNS Query
- [x] ET MALWARE NSO Group Pegasus CnC Domain Observed in DNS Query
- [x] ET MALWARE Observed Malicious SSL Cert (APT MustangPanda CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (MageCart Staging Domain)
- [x] ET MALWARE Possible APT 41 Fake Server Response
- [x] ET MALWARE APT 41 CnC Domain Observed in DNS Query
- [x] ET MALWARE APT 41 CnC Domain Observed in DNS Query
- [x] ET MALWARE PolyglotDuke Domain Observed
- [x] ET MALWARE PolyglotDuke Domain Observed
- [x] ET MALWARE PolyglotDuke Domain Observed
- [x] ET MALWARE PolyglotDuke Domain Observed
- [x] ET MALWARE PolyglotDuke Domain Observed
- [x] ET MALWARE PolyglotDuke Domain Observed
- [x] ET MALWARE MiniDuke Domain Observed
- [x] ET MALWARE FatDuke Domain Observed
- [x] ET MALWARE FatDuke Domain Observed
- [x] ET MALWARE LiteDuke Domain Observed
- [x] ET MALWARE APT-C-27 CnC Domain Observed in DNS Query
- [x] ET MALWARE APT-C-27 CnC Domain Observed in DNS Query
- [x] ET MALWARE APT-C-27 CnC Domain Observed in DNS Query
- [x] ET MALWARE Steganographic Encoded WAV File Inbound via HTTP M1
- [x] ET MALWARE Anchor_DNS Trickbot DNS CnC Command - Sending Data
- [x] ET MALWARE Anchor_DNS Trickbot DNS CnC Command - Receive Data
- [x] ET MALWARE APT 41 LOWKEY Backdoor - Ping Success Code sent to CnC
- [ ] ET MALWARE APT 41 LOWKEY Backdoor [TCP Relay Module] - PID Injection Command
- [ ] ET MALWARE APT 41 LOWKEY Backdoor [TCP Relay Module] - TCP Relay Successfully Activated on New Host
- [ ] ET MALWARE APT 41 LOWKEY Backdoor [TCP Relay Module] - Close Socket Command Observed
- [x] ET MALWARE Unk Spam Bot Template 1 Active - Outbound Malicious Email Spam
- [x] ET MALWARE Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-08
- [x] ET MALWARE Win32/Orion Logger SMTP Base64 Exfil
- [x] ET MALWARE Lazarus CnC Domain Observed in DNS Query
- [x] ET MALWARE Lazarus CnC Domain Observed in DNS Query
- [x] ET MALWARE Lazarus CnC Domain Observed in DNS Query
- [x] ET MALWARE Observed Malicious SSL Cert (CobInt CnC)
- [x] ET MALWARE MSIL/Diezen CnC Checkin M2
- [x] ET MALWARE Diezen/Sakabota CnC Domain Observed in DNS Query
- [x] ET MALWARE Observed Malicious SSL Cert (MalDoc DL) 2019-10-24
- [x] ET MALWARE Instagram Like Bot (like4u) CnC Activity M1
- [x] ET MALWARE Instagram Like Bot (like4u) CnC Domain in DNS Lookup
- [x] ET MALWARE Patchwork APT CnC Beacon 2
- [x] ET MALWARE Kimsuky CnC Domain Observed in DNS Query
- [x] ET MALWARE Unk/LNKR CnC Domain Observed in DNS Query
- [x] ET MALWARE Observed Malicious SSL Cert (StrongPity CnC)
- [x] ET MALWARE MSIL.L4L Stealer IP Check
- [x] ET MALWARE MSIL.L4L Stealer Systeminfo Exfiltration
- [x] ET MALWARE Possible Darkhotel Higasia Downloader Requesting Module
- [x] ET MALWARE Possible Darkhotel Higasia Downloader Checkin
- [x] ET MALWARE Keyboy CN APT CnC Domain in DNS Lookup
- [x] ET MALWARE NSO Group Pegasus CnC Domain Observed in DNS Query
- [x] ET MALWARE NSO Group Pegasus CnC Domain Observed in DNS Query
- [x] ET MALWARE NSO Group Pegasus CnC Domain Observed in DNS Query
- [x] ET MALWARE APT Mustang Panda Payload - CnC Checkin
- [x] ET MALWARE Observed Malicious SSL Cert (OSX/AppleJeus Variant CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (MageCart Staging Domain)
- [x] ET MALWARE APT 41 CnC Domain Observed in DNS Query
- [x] ET MALWARE APT 41 CnC Domain Observed in DNS Query
- [x] ET MALWARE PolyglotDuke Domain Observed
- [x] ET MALWARE PolyglotDuke Domain Observed
- [x] ET MALWARE PolyglotDuke Domain Observed
- [x] ET MALWARE PolyglotDuke Domain Observed
- [x] ET MALWARE PolyglotDuke Domain Observed
- [x] ET MALWARE PolyglotDuke Domain Observed
- [x] ET MALWARE MiniDuke Domain Observed
- [x] ET MALWARE FatDuke Domain Observed
- [x] ET MALWARE FatDuke Domain Observed
- [x] ET MALWARE FatDuke Domain Observed
- [x] ET MALWARE APT 41 LOWKEY Backdoor - Initalisation Bytes Received from CnC
- [x] ET MALWARE APT-C-27 CnC Domain Observed in DNS Query
- [x] ET MALWARE APT-C-27 CnC Domain Observed in DNS Query
- [x] ET MALWARE APT-C-27 CnC Domain Observed in DNS Query
- [x] ET MALWARE Steganographic Encoded WAV File Inbound via HTTP M2
- [x] ET MALWARE Anchor_DNS Trickbot DNS CnC Command - Prepare to Receive Data
- [ ] ET MALWARE APT 41 LOWKEY Backdoor - Ping Command Inbound
- [x] ET MALWARE APT 41 LOWKEY Backdoor - Ping Error Code sent to CnC
- [ ] ET MALWARE APT 41 LOWKEY Backdoor [TCP Relay Module] - Establishing Connection with New Host
- [ ] ET MALWARE APT 41 LOWKEY Backdoor [TCP Relay Module] - Exchanging RC4 & XOR Encrypted Data with Internal Host
- [ ] ET MALWARE APT 41 LOWKEY Backdoor [TCP Relay Module] - Close Named Pipe Command Observed
- [x] ET MALWARE Observed Malicious SSL Cert (DonotGroup CnC)
- [x] ET MALWARE Observed Win32/Orion Logger SMTP Exfil Subject Line
- [x] ET MALWARE Observed Malicious SSL Cert (APT32 CnC)
- [x] ET MALWARE Lazarus CnC Domain Observed in DNS Query
- [x] ET MALWARE Lazarus CnC Domain Observed in DNS Query
- [x] ET MALWARE Lazarus CnC Domain Observed in DNS Query
- [x] ET MALWARE Suspected Zebrocy Implant CnC Checkin
- [x] ET MALWARE MSIL/Diezen CnC Checkin M1
- [x] ET MALWARE Diezen/Sakabota CnC Domain Observed in DNS Query
- [x] ET MALWARE BadPatch CnC Activity
- [x] ET MALWARE Instagram Like Bot (like4u) CnC Activity M2
- [x] ET MALWARE Netwire RAT Client Check-in (socket created)
- [x] ET MALWARE Win32/Phorpiex CnC Checkin
- [x] ET MALWARE Kimsuky CnC Domain Observed in DNS Query
- [x] ET MALWARE Unk/LNKR CnC Domain Observed in DNS Query
- [x] ET MALWARE StrongPity CnC Domain Observed in DNS Query
- [x] ET MALWARE MSIL.L4L Stealer Screenshot Exfiltration
- [x] ET MALWARE Win32/CryptInject.BE!MTB Stealer CnC Checkin
- [x] ET MALWARE Possible Darkhotel Higasia Downloader Connectivity Check
- [x] ET MALWARE Observed Malicious SSL Cert (Turla CnC)
- [x] ET MALWARE Keyboy CN APT CnC Domain in DNS Lookup

- [x] ET MALWARE Keyboy CN APT CnC Domain in DNS Lookup
- [x] ET MALWARE Keyboy CN APT CnC Domain in DNS Lookup
- [x] ET MALWARE Keyboy CN APT CnC Domain in DNS Lookup
- [x] ET MALWARE Observed AHK Downloader Request Structure
- [x] ET MALWARE Platinum APT - Titanium Payload CnC Checkin (x64)
- [x] ET MALWARE Platinum APT - Titanium Hardcoded String Observed
- [x] ET MALWARE Gamaredon CnC Domain Observed in DNS Query
- [x] ET MALWARE DADJOKE/Rail Tycoon Payload Extraction
- [x] ET MALWARE Win32/AnteFrigus Ransomware Activity
- [x] ET MALWARE Observed Malicious SSL Cert (Possible APT33 CnC)
- [ ] ET MALWARE Win32/1xxbot CnC Checkin
- [x] ET MALWARE Observed Malicious SSL Cert (Sidewinder APT CnC)
- [x] ET MALWARE Observed CobInt CnC Domain in TLS SNI
- [x] ET MALWARE ELF/Mirai Variant UA Outbound (Ouija_x.86)
- [x] ET MALWARE SuperSocialat Plugin Backdoor Code Execution Attempt
- [x] ET MALWARE Possible Pipka JS Skimmer - Skimmer Payload Observed M1
- [x] ET MALWARE Possible Pipka JS Skimmer - Skimmer Payload Observed M3
- [x] ET MALWARE Possible Pipka JS Skimmer - Skimmer Payload Observed M5
- [x] ET MALWARE Possible Pipka JS Skimmer - Skimmer Payload Observed M7
- [x] ET MALWARE Win32/Agent Tesla SMTP Clipboard Exfil
- [x] ET MALWARE Observed Malicious SSL Cert (OSX/Nukesped CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (OSX/Nukesped CnC)
- [x] ET MALWARE Lemon_Duck Powershell - RDP Credential Exfil
- [x] ET MALWARE Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE ELF/Roboto - Possible Encrypted Roboto P2P Payload Requested M1
- [x] ET MALWARE ELF/Roboto - Communicating with Hardcoded Peer 1
- [x] ET MALWARE ELF/Roboto - Communicating with Hardcoded Peer 3
- [x] ET MALWARE ELF/Roboto - Communicating with Hardcoded Peer 5
- [x] ET MALWARE Observed Malicious SSL Cert (ACBackdoor CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (Possible Godlua CnC)
- [x] ET MALWARE SSL/TLS Certificate Observed (Various Crimeware)
- [x] ET MALWARE Win32/Beapy CnC Domain in DNS Lookup
- [x] ET MALWARE Win32/Emotet CnC Activity (POST) M6
- [x] ET MALWARE Legion Loader Activity Observed (YourUserAgent)
- [x] ET MALWARE Legion Loader Activity Observed (suspira)
- [x] ET MALWARE Legion Loader Activity Observed (legion)
- [x] ET MALWARE Legion Loader Activity Observed
- [x] ET MALWARE Legion Loader Activity Observed (satan)
- [x] ET MALWARE SSL/TLS Certificate Observed (Magecart)
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Buer Loader Download Request
- [x] ET MALWARE SSL/TLS Certificate Observed (Buer Loader)
- [x] ET MALWARE Tick Group Payload - Submitting Encrypted Data to CnC
- [x] ET MALWARE Malicious SSL Certificate detected (PyXie)
- [x] ET MALWARE Malicious SSL Certificate detected (PyXie)
- [x] ET MALWARE Malicious SSL Certificate detected (PyXie)
- [x] ET MALWARE Malicious SSL Certificate detected (PyXie)
- [x] ET MALWARE TickGroup ABK Backdoor CnC Check-in
- [x] ET MALWARE Possible TickGroup Coolbee/Avenger CnC Activity
- [x] ET MALWARE MedusaHTTP Variant CnC Checkin M2
- [x] ET MALWARE Observed Buran Ransomware UA
- [x] ET MALWARE Win32/Snatch Ransomware - Encryption Started
- [x] ET MALWARE Keyboy CN APT CnC Domain in DNS Lookup
- [x] ET MALWARE Keyboy CN APT CnC Domain in DNS Lookup
- [x] ET MALWARE Keyboy CN APT CnC Domain in DNS Lookup
- [x] ET MALWARE Win32/IcedID WebSocket Request M2
- [x] ET MALWARE Platinum APT - Titanium Payload CnC Checkin (x86)
- [x] ET MALWARE Platinum APT Activity
- [x] ET MALWARE Gamaredon CnC Domain Observed in DNS Query
- [x] ET MALWARE DADJOKE/Rail Tycoon Initial Macro Execution
- [x] ET MALWARE DADJOKE/Rail Tycoon Payload Execution
- [x] ET MALWARE Possible Gamaredon HEAD Request for .dot file on ddns.net
- [x] ET MALWARE Gamaredon CnC Domain Observed in DNS Query
- [x] ET MALWARE Observed Malicious SSL Cert (MalDoc DL 2019-11-15)
- [x] ET MALWARE Observed CobInt CnC Domain in TLS SNI
- [x] ET MALWARE ELF/Mirai Variant UA Outbound (ph0ne)
- [x] ET MALWARE Observed Buran Ransomware UA
- [x] ET MALWARE Possible Pipka JS Skimmer CnC Request
- [x] ET MALWARE Possible Pipka JS Skimmer - Skimmer Payload Observed M2
- [x] ET MALWARE Possible Pipka JS Skimmer - Skimmer Payload Observed M4
- [x] ET MALWARE Possible Pipka JS Skimmer - Skimmer Payload Observed M6
- [x] ET MALWARE Observed Malicious SSL Cert (AZORult CnC) 2019-11-18
- [x] ET MALWARE Observed Malicious SSL Cert (DonotGroup CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (OSX/Nukesped CnC)
- [x] ET MALWARE Lemon_Duck Powershell - Install Tracking
- [x] ET MALWARE Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE MuddyWater Payload - CnC Checkin
- [x] ET MALWARE ELF/Roboto - Possible Encrypted Roboto P2P Payload Requested M2
- [x] ET MALWARE ELF/Roboto - Communicating with Hardcoded Peer 2
- [x] ET MALWARE ELF/Roboto - Communicating with Hardcoded Peer 4
- [x] ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (ACBackdoor CnC)
- [x] ET MALWARE Cyborg Ransomware - Downloading Desktop Background
- [x] ET MALWARE Win32/Beapy CnC Domain in DNS Lookup
- [x] ET MALWARE Win32/Emotet CnC Activity (POST) M5
- [x] ET MALWARE Legion Loader Activity Observed (Mylegion666)
- [x] ET MALWARE Legion Loader Activity Observed (salmonella-symptome)
- [x] ET MALWARE Legion Loader Activity Observed (lilith)
- [x] ET MALWARE Legion Loader Activity Observed (the devil)
- [x] ET MALWARE Legion Loader Activity Observed (Amen)
- [x] ET MALWARE Legion Loader Activity Observed (neva-project)
- [x] ET MALWARE Possible Magecart Credit Card Information JS Script
- [x] ET MALWARE Buer Loader Update Request
- [x] ET MALWARE Buer Loader Successful Payload Download
- [x] ET MALWARE Tick Group Payload - Reporting Error to CnC
- [x] ET MALWARE Malicious SSL Certificate detected (PyXie)
- [x] ET MALWARE Malicious SSL Certificate detected (PyXie)
- [x] ET MALWARE Malicious SSL Certificate detected (PyXie)
- [x] ET MALWARE Malicious SSL Certificate detected (PyXie)
- [x] ET MALWARE TickGroup BROLER.F CnC Check-in
- [x] ET MALWARE Possible TickGroup Snack CnC Activity
- [x] ET MALWARE Possible TickGroup Casper CnC Activity
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Observed Malicious SSL Cert (MageCart)
- [ ] ET MALWARE Win32/Snatch Ransomware - Encryption Finished

- [x] ET MALWARE SSL/TLS Certificate Observed (Get2 CnC)
- [x] ET MALWARE Possible APT38 CnC Domain Observed in DNS Query
- [x] ET MALWARE [401TRG] Malicious SSL Cert (Dreambot CnC)
- [x] ET MALWARE [401TRG] Malicious SSL Cert (Dreambot CnC)
- [x] ET MALWARE [401TRG] Malicious SSL Cert (Dreambot CnC)
- [x] ET MALWARE [401TRG] Malicious SSL Cert (Dreambot CnC)
- [x] ET MALWARE [401TRG] Malicious SSL Cert (Dreambot CnC)
- [x] ET MALWARE [401TRG] Malicious SSL Cert (Dreambot CnC)
- [x] ET MALWARE AZORult v3.3 Server Response M1
- [x] ET MALWARE AZORult v3.3 Server Response M3
- [x] ET MALWARE AZORult v3.2 Server Response M2
- [x] ET MALWARE MalDoc Exfil (2019-12-12)
- [x] ET MALWARE DiamondFox HTTP Post CnC Checkin M3
- [x] ET MALWARE Win32/Unk.BrowserStealer CnC Checkin
- [ ] ET MALWARE Win32/Unk.BrowserStealer Data Exfil M2
- [x] ET MALWARE Observed DNS Query for APT40 Possible DADSTACHE CnC Domain
- [x] ET MALWARE ShivaGood Ransomware CnC Checkin
- [x] ET MALWARE Win32/BlackNET CnC Keep-Alive
- [x] ET MALWARE Observed Malicious SSL Cert (Sidewinder APT CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (DonotGroup CnC)
- [ ] ET MALWARE XServer Backdoor Communication Setup Initiate
- [x] ET MALWARE Possible XServer Backdoor Certificate Observed
- [x] ET MALWARE Win32/Valak
- [x] ET MALWARE Win32/Valak - Stage 2 - Response - Task
- [x] ET MALWARE Win32/Valak - Plugin Data Exfil
- [x] ET MALWARE Observed Malicious SSL Cert (Upatre CnC)
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Malicious SSL Cert (Magecart)
- [x] ET MALWARE Win32/ViSystem CnC Checkin
- [x] ET MALWARE Arechclient2 Backdoor CnC Checkin
- [x] ET MALWARE Observed Buran Ransomware UA
- [x] ET MALWARE Kimsuky Operation Blue Estimate CnC Activity
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Malicious SSL Cert (Magecart)
- [x] ET MALWARE Observed Magecart CnC Domain in TLS SNI
- [x] ET MALWARE DonotGroup CnC Domain Observed in DNS Query
- [x] ET MALWARE AstroBot CnC Activity
- [x] ET MALWARE Win32/Rarog Stealer CnC Checkin
- [x] ET MALWARE Magician/M461c14n Ransomware CnC Checkin
- [x] ET MALWARE DonotGroup Staging Domain Observed in DNS Query
- [x] ET MALWARE APT/TransparentTribe Style Request
- [x] ET MALWARE Win32/PSW.QQPass.OZV Variant Checkin
- [x] ET MALWARE Observed DNS Query to Ursnif SAIGON Variant CnC Domain
- [x] ET MALWARE Observed DNS Query to Ursnif SAIGON Variant CnC Domain
- [x] ET MALWARE Observed DNS Query to Ursnif SAIGON Variant CnC Domain
- [x] ET MALWARE Observed DNS Query to Ursnif SAIGON Variant CnC Domain
- [x] ET MALWARE DonotGroup CnC Domain Observed in DNS Query
- [x] ET MALWARE PowerTrick Task Checkin M1
- [x] ET MALWARE PowerTrick Task Answer
- [x] ET MALWARE PowerTrick Known Key 1
- [x] ET MALWARE PowerTrick download ver1 bot
- [x] ET MALWARE PowerTrick download bot known key
- [x] ET MALWARE PowerSploit/PowerView SMTP Data Exfil
- [x] ET MALWARE Observed Certificate Containing Possible Base64 Encoded Powershell Inbound
- [x] ET MALWARE Observed Certificate Base64 Encoded Executable Inbound
- [ ] ET MALWARE Win32/MillionLoader CnC Init Activity
- [x] ET MALWARE Win32/MillionLoader CnC Activity (Inbound)
- [x] ET MALWARE CrownAdPro CnC Activity M3
- [x] ET MALWARE Possible APT38 CnC Domain Observed in DNS Query
- [x] ET MALWARE [401TRG] Malicious SSL Cert (Dreambot CnC)
- [x] ET MALWARE [401TRG] Malicious SSL Cert (Dreambot CnC)
- [x] ET MALWARE [401TRG] Malicious SSL Cert (Dreambot CnC)
- [x] ET MALWARE Malicious SSL Cert (Magecart)
- [x] ET MALWARE [401TRG] Malicious SSL Cert (Dreambot CnC)
- [x] ET MALWARE [401TRG] Malicious SSL Cert (Dreambot CnC)
- [x] ET MALWARE [401TRG] Malicious SSL Cert (Dreambot CnC)
- [x] ET MALWARE AZORult v3.3 Server Response M2
- [x] ET MALWARE AZORult v3.2 Server Response M1
- [x] ET MALWARE AZORult v3.2 Server Response M3
- [x] ET MALWARE CrownAdPro CnC Activity M1
- [x] ET MALWARE Win32/Unk.BrowserStealer CnC Keep-Alive
- [x] ET MALWARE Win32/Unk.BrowserStealer Data Exfil M1
- [x] ET MALWARE Win32/Unk.BrowserStealer Data Exfil M3
- [x] ET MALWARE Observed Buran Ransomware UA
- [x] ET MALWARE Win32/BlackNET CnC Checkin
- [x] ET MALWARE Win32/BlackNET CnC Requesting Command
- [x] ET MALWARE Win32/MailerBot CnC Activity
- [ ] ET MALWARE XServer Backdoor Communication Setup Request
- [x] ET MALWARE OilRig APT PowDesk Powershell Check
- [x] ET MALWARE Win32/Valak
- [x] ET MALWARE Win32/Valak
- [x] ET MALWARE Win32/Valak - Stage 2 - Response - Plugin
- [ ] ET MALWARE Observed Malicious SSL Cert (jssLoader CnC)
- [x] ET MALWARE Observed Upatre CnC Domain in TLS SNI
- [x] ET MALWARE Observed Magecart CnC Domain in TLS SNI
- [x] ET MALWARE Dark Nexus IoT Variant User-Agent (Outbound)
- [x] ET MALWARE Arechclient2 Backdoor CnC Init
- [x] ET MALWARE Arechclient2 Backdoor CnC Keep-Alive
- [x] ET MALWARE Lampion CnC Activity
- [x] ET MALWARE Legion Loader Activity Observed (carlos_castaneda)
- [x] ET MALWARE Observed Magecart CnC Domain in TLS SNI
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Malicious SSL Cert (Magecart)
- [x] ET MALWARE Zeoticus Ransomware CnC Activity
- [x] ET MALWARE Mermaid Ransomware Variant CnC Activity M1
- [x] ET MALWARE Vidar/Arkei/Megumin/Oski Stealer Data Exfil
- [x] ET MALWARE Legion Loader Activity Observed
- [ ] ET MALWARE Win32/Filecoder.NZK Variant
- [x] ET MALWARE APT/TransparentTribe CnC Checkin
- [ ] ET MALWARE Observed Malicious SSL Cert (ServHelper CnC)
- [x] ET MALWARE Observed DNS Query to Ursnif SAIGON Variant CnC Domain
- [x] ET MALWARE Observed DNS Query to Ursnif SAIGON Variant CnC Domain
- [x] ET MALWARE Observed DNS Query to Ursnif SAIGON Variant CnC Domain
- [x] ET MALWARE [401TRG] PS/PowDesk Checkin (APT34)
- [x] ET MALWARE PowerTrick Task Request
- [x] ET MALWARE PowerTrick Task Checkin M2
- [x] ET MALWARE Satan/5ss5c Ransomware CnC Activity
- [x] ET MALWARE PowerTrick Known Key 2
- [x] ET MALWARE PowerTrick download ver2 bot
- [x] ET MALWARE Observed Possible PowerSploit/PowerView .ps1 Inbound
- [x] ET MALWARE Observed Certificate Containing Double Base64 Encoded Executable Inbound
- [x] ET MALWARE Win32/Emotet CnC Activity (POST) M7
- [x] ET MALWARE SMS-Bomber Activity
- [x] ET MALWARE Win32/MillionLoader CnC Activity (Outbound)
- [x] ET MALWARE CrownAdPro CnC Activity M2
- [x] ET MALWARE CrownAdPro CnC Activity M4

- [x] ET MALWARE CrownAdPro CnC Activity M5
- [x] ET MALWARE Nemty Ransomware CnC Checkin
- [x] ET MALWARE Nemty Ransomware Payment Page ID File Upload
- [x] ET MALWARE MilkyBoy CnC Data Exfil
- [ ] ET MALWARE Observed Malicious SSL Cert (AZORult CnC)
- [ ] ET MALWARE Nexus Stealer CnC Data Exfil
- [x] ET MALWARE Observed Magecart CnC Domain in TLS SNI
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Malicious SSL Cert (Magecart)
- [x] ET MALWARE Observed Malicious SSL Cert (ELF/Rekoobe CnC)
- [x] ET MALWARE Gamaredon CnC Observed in DNS Query
- [x] ET MALWARE Observed Malicious SSL Cert (BrushaLoader CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (BrushaLoader CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (BrushaLoader CnC)
- [x] ET MALWARE Mermaid Ransomware Variant CnC Activity M2
- [x] ET MALWARE Possible Generic RAT over Telegram API
- [x] ET MALWARE Diezen/Sakabota CnC Domain Observed in DNS Query
- [x] ET MALWARE Hisoka CnC Domain Observed in DNS Query
- [x] ET MALWARE Mimikatz x64 Executable Transfer Over SMB
- [x] ET MALWARE Mimikatz x64 Mimidrv.sys File Transfer Over SMB
- [x] ET MALWARE Mimikatz x64 Executable Download Over HTTP
- [x] ET MALWARE Mimikatz x64 Mimidrv.sys Download Over HTTP
- [x] ET MALWARE Possible Winnti TLS Certificate Observed
- [x] ET MALWARE Possible Winnti TLS SNI Observed
- [x] ET MALWARE Possible Winnti DNS Lookup
- [x] ET MALWARE DonotGroup CnC Observed in DNS Query
- [x] ET MALWARE Parallax CnC Activity M6 (set)
- [x] ET MALWARE Win32/Emotet CnC Activity (POST) M8
- [x] ET MALWARE APT34 TONEDEAF 2.0 Requesting Commands from CnC
- [x] ET MALWARE Possible APT34 TONEDEAF 2.0 User-Agent Observed
- [x] ET MALWARE Observed Malicious SSL Cert (BrushaLoader CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (MINEBRIDGE/MINEDOOR CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (MINEBRIDGE/MINEDOOR CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (MINEBRIDGE/MINEDOOR CnC)
- [x] ET MALWARE Malicious SSL Certificate detected (Patchwork CnC)
- [x] ET MALWARE Patchwork Backdoor - Sending Task Results
- [x] ET MALWARE Emotet Wifi Bruter Module Checkin
- [x] ET MALWARE Observed Malicious SSL Cert (TinyNuke Variant CnC) 2020-02-09
- [x] ET MALWARE Win32/AZORult V3.2 Client Checkin M2
- [x] ET MALWARE Win32/AZORult V3.3 Client Checkin M1
- [x] ET MALWARE Win32/AZORult V3.3 Client Checkin M3
- [x] ET MALWARE Mozart Loader Command Request (gettasks)
- [x] ET MALWARE Mozart Loader Command Request (reporttask)
- [x] ET MALWARE APT40/Dadstache Related DNS Lookup
- [x] ET MALWARE APT40/Dadstache Related DNS Lookup
- [x] ET MALWARE APT40/Dadstache Related DNS Lookup
- [x] ET MALWARE APT40/Dadstache Related DNS Lookup
- [x] ET MALWARE Possible APT40/Dadstache Stage 2 Payload Beacon
- [x] ET MALWARE DNS Query to MINEBRIDGE CnC Domain (conversia91 .top)
- [x] ET MALWARE DNS Query to MINEBRIDGE CnC Domain (creatorz123 .top)
- [x] ET MALWARE TA402/Molerats Pierogi Backdoor Activity
- [x] ET MALWARE TA402/Molerats Pierogi CnC Response (Download)
- [x] ET MALWARE TA402/Molerats Pierogi CnC Activity (Upload)
- [x] ET MALWARE Win32/AZORult V3.2 Client Checkin M5
- [x] ET MALWARE Win32/AZORult V3.3 Client Checkin M4
- [x] ET MALWARE Win32/AZORult V3.3 Client Checkin M6
- [x] ET MALWARE Win32/AZORult V3.2 Client Checkin M8
- [x] ET MALWARE Group 21 CnC Domain Observed in DNS Query
- [x] ET MALWARE Observed Nemty Ransomware Payment Page
- [ ] ET MALWARE MilkyBoy CnC Activity
- [ ] ET MALWARE Observed Malicious SSL Cert (AZORult CnC)
- [x] ET MALWARE MageCart CnC Domain Observed in DNS Query
- [ ] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Malicious SSL Cert (Magecart)
- [x] ET MALWARE Observed Magecart CnC Domain in TLS SNI
- [ ] ET MALWARE Observed Thanatos Ransomware Variant Pico User-Agent
- [x] ET MALWARE ELF/Rekoobe CnC Observed in DNS Query
- [x] ET MALWARE Observed Malicious SSL Cert (BrushaLoader CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (BrushaLoader CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (BrushaLoader CnC)
- [x] ET MALWARE ELF/Muhstik - IRC CnC Checkin
- [x] ET MALWARE Mermaid Ransomware Variant CnC Activity M3
- [x] ET MALWARE Observed Unk.PowerShell Loader CnC Domain in TLS SNI
- [x] ET MALWARE Diezen/Sakabota CnC Domain Observed in DNS Query
- [x] ET MALWARE Mimikatz x86 Executable Transfer Over SMB
- [x] ET MALWARE Mimikatz x86 Mimidrv.sys File Transfer Over SMB
- [x] ET MALWARE Mimikatz x86 Executable Download Over HTTP
- [x] ET MALWARE Mimikatz x86 Mimidrv.sys Download Over HTTP
- [ ] ET MALWARE Amadey Stealer CnC - BotKiller Module Checkin
- [x] ET MALWARE Possible Winnti TLS Certificate Observed
- [x] ET MALWARE Possible Winnti TLS SNI Observed
- [x] ET MALWARE Possible Winnti DNS Lookup
- [x] ET MALWARE CryptoPatronum Ransomware CnC Checkin
- [x] ET MALWARE Parallax CnC Response Activity M6
- [x] ET MALWARE Cobalt Strike Malleable C2 Request (Stackoverflow Profile)
- [x] ET MALWARE APT34 TONEDEAF 2.0 Uploading to CnC
- [x] ET MALWARE Observed Malicious SSL Cert (APT34 CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (BrushaLoader CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (MINEBRIDGE/MINEDOOR CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (MINEBRIDGE/MINEDOOR CnC)
- [x] ET MALWARE MINEBRIDGE/MINEDOOR CnC Checkin
- [x] ET MALWARE Patchwork Backdoor Checkin
- [x] ET MALWARE Patchwork Backdoor - Requesting Task
- [x] ET MALWARE Possible Satan Cryptor GeoIP Lookup
- [x] ET MALWARE Win32/AZORult V3.2 Client Checkin M1
- [x] ET MALWARE Win32/AZORult V3.2 Client Checkin M3
- [x] ET MALWARE Win32/AZORult V3.3 Client Checkin M2
- [x] ET MALWARE Mozart Loader CnC Checkin (getid)
- [x] ET MALWARE Mozart Loader Command Request (getupdates)
- [x] ET MALWARE Mozart Loader Command Request (reportupdates)
- [x] ET MALWARE APT40/Dadstache Related DNS Lookup
- [x] ET MALWARE APT40/Dadstache Related DNS Lookup
- [x] ET MALWARE APT40/Dadstache Related DNS Lookup
- [x] ET MALWARE APT40/Dadstache Related DNS Lookup
- [x] ET MALWARE DNS Query to MINEBRIDGE CnC Domain (123faster .top)
- [x] ET MALWARE DNS Query to MINEBRIDGE CnC Domain (fatoftheland .top)
- [x] ET MALWARE DNS Query to MINEBRIDGE CnC Domain (compilator333 .top)
- [x] ET MALWARE TA402/Molerats Pierogi CnC Response (Command)
- [x] ET MALWARE TA402/Molerats Pierogi CnC Response (Screenshot)
- [x] ET MALWARE Win32/AZORult V3.2 Client Checkin M4
- [x] ET MALWARE Win32/AZORult V3.2 Client Checkin M6
- [x] ET MALWARE Win32/AZORult V3.3 Client Checkin M5
- [x] ET MALWARE Win32/AZORult V3.2 Client Checkin M7
- [x] ET MALWARE Win32/AZORult V3.2 Client Checkin M9

☑ ET MALWARE Win32/AZORult V3.3 Client Checkin M7
☑ ET MALWARE Win32/AZORult V3.3 Client Checkin M9
☑ ET MALWARE Observed Malicious SSL Cert (FIN7/GRIFFON CnC)
☑ ET MALWARE Possible Kimsuky Related Exfil
☑ ET MALWARE Kimsuky Related CnC
☑ ET MALWARE Parallax CnC Activity M7 (set)
☑ ET MALWARE Win32/AZORult V3.2 Client Checkin M10
☑ ET MALWARE Win32/AZORult V3.2 Client Checkin M12
☑ ET MALWARE Win32/AZORult V3.3 Client Checkin M11
☑ ET MALWARE Win32/AZORult V3.2 Client Checkin M13
☑ ET MALWARE Win32/AZORult V3.2 Client Checkin M15
☑ ET MALWARE Win32/AZORult V3.3 Client Checkin M14
☑ ET MALWARE Observed Malicious SSL Cert (AgentTesla CnC)
☑ ET MALWARE ELF/Mirai User-Agent Observed (Outbound)
☑ ET MALWARE Win32/Sarwent Initial Checkin CnC Response
☑ ET MALWARE Possible NK APT SLICKSHOES Host Checkin
☑ ET MALWARE Win32/AZORult V3.2 Client Checkin M17
☑ ET MALWARE Win32/AZORult V3.3 Client Checkin M16
☑ ET MALWARE Win32/AZORult V3.3 Client Checkin M18
☑ ET MALWARE Win32/AZORult V3.2 Client Checkin M20
☑ ET MALWARE Win32/AZORult V3.3 Client Checkin M19
☑ ET MALWARE Win32/AZORult V3.3 Client Checkin M21
☑ ET MALWARE Spark Backdoor CnC Domain Query
☑ ET MALWARE Possible Charming Kitten Backdoor CnC Activity
☑ ET MALWARE PHPs Labyrinth Backdoor Stage2 CnC Activity M1
☑ ET MALWARE PHPs Labyrinth Backdoor Stage1 CnC Activity
☑ ET MALWARE Observed Malicious SSL Cert (MageCart CnC)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 12)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 12)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 12)
☑ ET MALWARE Observed PHPs Labyrinth Stage2 CnC Domain in TLS SNI
☑ ET MALWARE Observed PHPs Labyrinth Stage2 CnC Domain in TLS SNI
☑ ET MALWARE Observed PHPs Labyrinth Stage2 CnC Domain in TLS SNI
☑ ET MALWARE Observed PHPs Labyrinth Stage2 CnC Domain in TLS SNI
☑ ET MALWARE Observed PHPs Labyrinth Stage2 CnC Domain in TLS SNI
☑ ET MALWARE Observed PHPs Labyrinth Stage2 CnC Domain in TLS SNI
☑ ET MALWARE Observed Malicious SSL Cert (PHPs Labyrinth Stage1 CnC)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 12)
☑ ET MALWARE Observed Malicious SSL Cert (MalDoc DL 2020-02-21 2)
☑ ET MALWARE Observed Malicious SSL Cert (Get2 CnC)
☑ ET MALWARE ObliqueRAT CnC Checkin
☑ ET MALWARE Observed Adwind RAT CnC DNS Query
☑ ET MALWARE Observed Malicious SSL Cert (Get2 CnC)
☑ ET MALWARE Legion Loader Activity Observed (heil_satan)
☑ ET MALWARE Observed Ursnif Domain in TLS SNI
☑ ET MALWARE Win32/Qbot/Quakbot Downloader - Requesting Secondary Download
☑ ET MALWARE MalDoc Retrieving Possible Ostap Payload
☑ ET MALWARE Observed Malicious SSL Cert (SmokeLoader CnC)
☑ ET MALWARE Observed Malicious SSL Cert (SmokeLoader CnC)
☑ ET MALWARE BlackTech ELF/TSCookie CnC Observed in DNS Query
☑ ET MALWARE Observed GoBotKR Domain in TLS SNI
☑ ET MALWARE Observed GoBotKR Domain in TLS SNI
☑ ET MALWARE Magecart CnC Domain in DNS Lookup
☑ ET MALWARE Observed Malicious SSL Cert (Get2 CnC)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart)
☑ ET MALWARE SharpExec EXE Lateral Movement Tool Downloaded
☑ ET MALWARE Polaris Botnet User-Agent (Outbound)

☑ ET MALWARE Win32/AZORult V3.3 Client Checkin M8
☑ ET MALWARE POWERTON CnC Domain in DNS Lookup
☑ ET MALWARE Kimsuky Related CnC
☑ ET MALWARE Possible Kimsuky Related Download
☑ ET MALWARE Parallax RAT CnC Domain Observed in DNS Query
☑ ET MALWARE Parallax CnC Response Activity M7
☑ ET MALWARE Win32/AZORult V3.2 Client Checkin M11
☑ ET MALWARE Win32/AZORult V3.3 Client Checkin M10
☑ ET MALWARE Win32/AZORult V3.3 Client Checkin M12
☑ ET MALWARE Win32/AZORult V3.2 Client Checkin M14
☑ ET MALWARE Win32/AZORult V3.3 Client Checkin M13
☑ ET MALWARE Win32/AZORult V3.3 Client Checkin M15
☑ ET MALWARE Win32/Sarwent Variant CnC Activity
☑ ET MALWARE Win32/Sarwent Initial Checkin
☑ ET MALWARE Netwire RAT Check-in (set)
☑ ET MALWARE Win32/AZORult V3.2 Client Checkin M16
☑ ET MALWARE Win32/AZORult V3.2 Client Checkin M18
☑ ET MALWARE Win32/AZORult V3.3 Client Checkin M17
☑ ET MALWARE Win32/AZORult V3.2 Client Checkin M19
☑ ET MALWARE Win32/AZORult V3.2 Client Checkin M21
☑ ET MALWARE Win32/AZORult V3.3 Client Checkin M20
☑ ET MALWARE Malicious SSL Certificate detected (Cobalt Strike CnC)
☑ ET MALWARE Possible Charming Kitten Backdoor Checkin
☑ ET MALWARE Mermaid Ransomware Variant CnC Activity M4
☑ ET MALWARE PHPs Labyrinth Backdoor Stage2 CnC Activity M2
☑ ET MALWARE Suspected Gamaredon Downloader Activity
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 12)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 12)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 12)
☑ ET MALWARE Observed Malicious SSL Cert (MageCart Group 12)
☑ ET MALWARE Observed PHPs Labyrinth Stage2 CnC Domain in TLS SNI
☑ ET MALWARE Observed PHPs Labyrinth Stage2 CnC Domain in TLS SNI
☑ ET MALWARE Observed PHPs Labyrinth Stage2 CnC Domain in TLS SNI
☑ ET MALWARE Observed PHPs Labyrinth Stage2 CnC Domain in TLS SNI
☑ ET MALWARE Observed PHPs Labyrinth Stage2 CnC Domain in TLS SNI
☑ ET MALWARE Observed PHPs Labyrinth Stage2 CnC Domain in TLS SNI
☑ ET MALWARE Fake ProtonVPN/AZORult CnC Domain Query
☑ ET MALWARE Observed Malicious SSL Cert (MalDoc DL 2020-02-21)
☑ ET MALWARE Observed Malicious SSL Cert (MalDoc DL 2020-02-21 3)
☑ ET MALWARE ObliqueRAT CnC Heartbeat Packet
☑ ET MALWARE Observed Adwind RAT CnC DNS Query
☑ ET MALWARE Observed Adwind RAT CnC DNS Query
☑ ET MALWARE JS/Ostap Maldoc Check-in
☑ ET MALWARE GoLang Discord Token Grabber Exfil
☑ ET MALWARE Observed Ursnif Domain in TLS SNI
☑ ET MALWARE Baraka Ransomware CnC activity email SMTP
☑ ET MALWARE Observed Malicious SSL Cert (Get2 CnC)
☑ ET MALWARE Observed Malicious SSL Cert (SmokeLoader CnC)
☑ ET MALWARE BlackTech ELF/TSCookie CnC Observed in DNS Query
☑ ET MALWARE Observed GoBotKR Domain in TLS SNI
☑ ET MALWARE Observed GoBotKR Domain in TLS SNI
☑ ET MALWARE Observed GoBotKR Domain in TLS SNI
☑ ET MALWARE Observed Magecart Domain (webscriptly .com in TLS SNI)
☑ ET MALWARE CROSSWALK CnC Checkin
☑ ET MALWARE Observed Malicious SSL Cert (MageCart)
☑ ET MALWARE Kimsuky Related Host Data Exfil
☑ ET MALWARE Magniber Ransomware Retrieving Instructions

- [x] ET MALWARE Magniber Ransomware CnC Domain in DNS Lookup
- [x] ET MALWARE Kimsuky Related Host Data Exfil
- [x] ET MALWARE Legion Loader Activity Observed (heil_moloch)
- [x] ET MALWARE BlackTech ELF/TSCookie CnC Observed in DNS Query
- [x] ET MALWARE Inbound MonetizeUs/LNKR Struct
- [x] ET MALWARE Observed Malicious SSL Cert (MonetizUs/LNKR)
- [x] ET MALWARE Observed JS/Skimmer (likely Magecart) CnC Domain in DNS Lookup
- [x] ET MALWARE Observed Malicious SSL Cert (ServHelper CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (ServHelper CnC)
- [x] ET MALWARE MSIL/Firebird RAT CnC Checkin
- [x] ET MALWARE ViperSoftX CnC Activity M1
- [x] ET MALWARE Observed Malicious SSL Cert (ServHelper CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (ServHelper CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (ServHelper CnC)
- [x] ET MALWARE Suspected SandCat Related Communication (POST)
- [x] ET MALWARE VBS/TrojanDownloader.Agent.SEB Keep-Alive
- [ ] ET MALWARE Observed DNS Query to Vicious Panda CnC Domain
- [x] ET MALWARE Observed DNS Query to Vicious Panda CnC Domain
- [x] ET MALWARE Observed DNS Query to Vicious Panda CnC Domain
- [x] ET MALWARE HTTPTool User-Agent
- [x] ET MALWARE Higaisa CnC Activity
- [x] ET MALWARE Observed Malicious SSL Cert (Win32/SandCat CnC)
- [x] ET MALWARE [PTsecurity] MZRevenge Ransomware Server Response
- [x] ET MALWARE MZRevenge Ransomware CnC
- [x] ET MALWARE Observed Malicious SSL Cert (Get2 CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (Get2 CnC)
- [ ] ET MALWARE MSIL/Modi RAT CnC Command Inbound (aw)
- [x] ET MALWARE MSIL/Modi RAT CnC Command Inbound (plugin)
- [x] ET MALWARE Possible APT28 Phishing Domain in DNS Query
- [x] ET MALWARE Possible APT28 Phishing Domain in DNS Query
- [x] ET MALWARE Possible APT28 Phishing Domain in DNS Query
- [x] ET MALWARE Possible APT28 Phishing Domain in DNS Query
- [x] ET MALWARE CoreDDRAT Initial Checkin
- [x] ET MALWARE CoreDDRAT KeepAlive Message
- [x] ET MALWARE Sekhmet Ransomware CnC Activity
- [x] ET MALWARE Observed Malicious SSL Cert (Cobalt Strike CnC)
- [x] ET MALWARE Observed MSIL/n2019cov (COVID-19) Ransomware CnC Domain in TLS SNI
- [x] ET MALWARE Win32/Milum CnC
- [x] ET MALWARE Cobalt Strike Malleable C2 (Magnitude EK)
- [x] ET MALWARE Cobalt Strike Malleable C2 (OneDrive)
- [x] ET MALWARE Observed Glupteba CnC Domain in TLS SNI
- [x] ET MALWARE ELF/Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE Observed DNS Query to Stitch C2 Domain
- [x] ET MALWARE Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE Win32/Tofsee Malformed Spam Template String
- [x] ET MALWARE Linux/Agent.HX CnC Activity (set)
- [x] ET MALWARE Linux/Agent.HX CnC Activity M2
- [x] ET MALWARE ELF/Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE Suspected CHAOS CnC Inbound (download command)
- [x] ET MALWARE Suspected CHAOS CnC Inbound (screenshot command)
- [x] ET MALWARE Suspected CHAOS CnC Inbound (persistence enable)
- [x] ET MALWARE Suspected CHAOS CnC Inbound (openurl)
- [x] ET MALWARE FTCode Stealer CnC Activity
- [x] ET MALWARE Malicious VBE Script (COVID-19 Phish 2020-04-03)
- [x] ET MALWARE Parallax CnC Activity M8 (set)
- [x] ET MALWARE Sarwent CnC Response (cmd_exec)
- [x] ET MALWARE Sarwent CnC Response (rdp_exec)
- [x] ET MALWARE Sarwent CnC Response (download_exec)
- [x] ET MALWARE Sarwent CnC Command (download)
- [x] ET MALWARE Sarwent CnC Command (rdp)

- [x] ET MALWARE Magniber Ransomware CnC Domain in DNS Lookup
- [x] ET MALWARE Backdoor.Win32.Agent.myttae User-Agent
- [x] ET MALWARE Kimsuky Related Host Data Exfil
- [x] ET MALWARE Win32/LODEINFO CnC Checkin
- [x] ET MALWARE Observed Malicious SSL Cert (MonetizUs/LNKR)
- [x] ET MALWARE Observed Malicious SSL Cert (MalDoc 2020-03-09)
- [x] ET MALWARE Observed JS/Skimmer (likely Magecart) Domain in TLS SNI (imprintcenter .com)
- [x] ET MALWARE Observed Malicious SSL Cert (ServHelper CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (ServHelper CnC)
- [x] ET MALWARE MalDoc Retrieving msiexec Commands via DNS TXT
- [x] ET MALWARE ViperSoftX CnC Activity M2
- [x] ET MALWARE Observed Malicious SSL Cert (ServHelper CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (ServHelper CnC)
- [x] ET MALWARE PXJ Ransomware CnC Activity
- [x] ET MALWARE VBS/TrojanDownloader.Agent.SEB Checkin
- [x] ET MALWARE VBS/TrojanDownloader.Agent.SEB Reporting Network Info
- [x] ET MALWARE Observed DNS Query to Vicious Panda CnC Domain
- [x] ET MALWARE Observed DNS Query to Vicious Panda CnC Domain
- [ ] ET MALWARE Observed DNS Query to Vicious Panda CnC Domain
- [x] ET MALWARE Observed Malicious SSL Cert (Cobalt Strike CnC)
- [x] ET MALWARE Win32/Unk.Joia CnC Activity
- [x] ET MALWARE Win32/SandCat CnC Checkin
- [x] ET MALWARE Polaris Botnet User-Agent (Outbound)
- [x] ET MALWARE Observed Malicious SSL Cert (Get2 CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (Get2 CnC)
- [x] ET MALWARE MSIL/Modi RAT CnC Command Inbound (info)
- [x] ET MALWARE MSIL/Modi RAT CnC Checkin (DesktopPreview)
- [x] ET MALWARE Possible APT28 Phishing Domain in DNS Query
- [x] ET MALWARE Possible APT28 Phishing Domain in DNS Query
- [x] ET MALWARE Possible APT28 Phishing Domain in DNS Query
- [x] ET MALWARE Possible APT28 Phishing Domain in DNS Query
- [x] ET MALWARE Possible APT28 Phishing Domain in DNS Query
- [x] ET MALWARE CoreDDRAT CnC Activity
- [x] ET MALWARE CoreDDRAT Screenshot Exfil
- [x] ET MALWARE Observed Buer Loader CnC Domain (kkjjhhdff .site in TLS SNI)
- [x] ET MALWARE Win32/RaaLoader CnC Activity
- [x] ET MALWARE MSIL/n2019cov (COVID-19) Ransomware CnC Checkin
- [x] ET MALWARE Cobalt Strike Malleable C2 (Havex APT)
- [x] ET MALWARE Cobalt Strike Malleable C2 (Meterpreter)
- [x] ET MALWARE Cobalt Strike Malleable C2 (Adobe RTMP)
- [x] ET MALWARE ELF/Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE Observed DNS Query to Stitch C2 Domain
- [x] ET MALWARE Buer Loader Update Request
- [x] ET MALWARE Win32/Tofsee Covid19 Spam Template 1 Active - Outbound Email Spam
- [x] ET MALWARE Win32/Tofsee Unique Email Body Byte Sequence Observed
- [x] ET MALWARE Linux/Agent.HX CnC Activity M1
- [x] ET MALWARE ELF/Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE Suspected Stitch Variant Backdoor CnC
- [x] ET MALWARE Suspected CHAOS CnC Inbound (upload command)
- [x] ET MALWARE Suspected CHAOS CnC Inbound (keylogger start)
- [x] ET MALWARE Suspected CHAOS CnC Inbound (getos)
- [x] ET MALWARE FTCode Stealer Init Activity
- [x] ET MALWARE ELF/Mirai Variant User-Agent (Outbound)
- [ ] ET MALWARE Win32/MOOZ.THCCABO CoinMiner CnC Checkin
- [x] ET MALWARE Parallax CnC Response Activity M8
- [x] ET MALWARE Sarwent CnC Response (powershell_exec)
- [x] ET MALWARE Sarwent CnC Response (update_exec)
- [x] ET MALWARE Sarwent CnC Command (update)
- [x] ET MALWARE Sarwent CnC Command (powershell)
- [x] ET MALWARE Observed Sidewinder APT User-Agent

- [x] ET MALWARE KPOT Stealer Initial CnC Activity M4
- [x] ET MALWARE ELF Linux/Dnsamp.AB Variant CnC
- [x] ET MALWARE Win32/RocketX Stealer CnC Exfil
- [x] ET MALWARE Possible Kimsuky APT Connectivity Check via Document
- [x] ET MALWARE MSIL/Agent.TRM Checkin Response
- [x] ET MALWARE MSIL/Agent.TRM Data Exfil (sysinfo)
- [x] ET MALWARE Possible DACLS RAT CnC (Log Server Reporting)
- [x] ET MALWARE DCRat Initial CnC Activity
- [x] ET MALWARE DDG Botnet CnC Job Request
- [x] ET MALWARE DDG Botnet Miner Download
- [x] ET MALWARE Observed DNS Query to Redkeeper Ransomware Domain
- [x] ET MALWARE Observed Malicious SSL Cert (Sidewinder APT CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (FIN7/JSSLoader CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (Malicious Browser Ext CnC)
- [ ] ET MALWARE Win32/CONFUCIUS_B External IP Check to CnC M2
- [x] ET MALWARE AgentTesla Exfil via FTP
- [x] ET MALWARE ELF/Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE Various Ransomware/Stealer Style External IP Address Check (myip .ch)
- [x] ET MALWARE Observed Malicious SSL Cert (AsyncRAT CnC)
- [x] ET MALWARE Cobalt Strike Malleable C2 (Custom)
- [x] ET MALWARE MalDoc Requesting Payload 2020-04-21
- [x] ET MALWARE JS Skimmer Domain in DNS Lookup
- [x] ET MALWARE NanoCore RAT CnC 27
- [x] ET MALWARE METALJACK APT32 DNS Lookup (m.topiccore.com)
- [x] ET MALWARE METALJACK APT32 DNS Lookup (libjs.inquirerjs.com)
- [x] ET MALWARE SSL/TLS Certificate Observed (APT32 METALJACK)
- [x] ET MALWARE SSL/TLS Certificate Observed (APT32 METALJACK)
- [x] ET MALWARE Parallax CnC Activity M9 (set)
- [x] ET MALWARE Observed Malicious SSL Cert (Gozi ISFB)
- [x] ET MALWARE ASNAROK Related Domain in DNS Lookup
- [x] ET MALWARE ASNAROK CnC Domain in DNS Lookup
- [x] ET MALWARE AntSword Webshell User-Agent Observed
- [x] ET MALWARE Parallax CnC Response Activity M9
- [x] ET MALWARE BAZAR CnC Domain in DNS Lookup
- [x] ET MALWARE BAZAR CnC Domain in DNS Lookup
- [x] ET MALWARE Observed Malicious SSL Cert (W32/TrojanDownloader.Agent.FBF Variant CnC)
- [x] ET MALWARE IcedID CnC Domain in SNI
- [x] ET MALWARE Win32/IcedID Requesting Encoded Binary M4
- [ ] ET MALWARE NAZAR EYService Pong response
- [ ] ET MALWARE NAZAR EYService File exfiltrate response
- [x] ET MALWARE MINEBRIDGE CnC Response
- [x] ET MALWARE Rhabdo CnC Activity M2
- [x] ET MALWARE IXWARE Stealer Domain in DNS Lookup
- [x] ET MALWARE IXWARE Stealer CnC Activity
- [x] ET MALWARE Observed Malicious SSL Cert (Lazarus APT MalDoc DL 2020-05-05)
- [x] ET MALWARE Nazar Implant - Sending Basic System Info to CnC
- [x] ET MALWARE nspps Backdoor - Sending SOCKS Details
- [x] ET MALWARE Observed Default CobaltStrike SSL Certificate
- [x] ET MALWARE JsOutProx Variant CnC Activity
- [x] ET MALWARE Ragnarok Ransomware CnC Activity M2
- [x] ET MALWARE D-Link ShareCenter (DNS-320/325) RCE (Outbound)
- [x] ET MALWARE W32/Agent.XXZBEN Downloader Activity
- [x] ET MALWARE EVILNUM CnC Host Checkin
- [x] ET MALWARE MAZE Ransomware Payment Domain DNS Lookup
- [x] ET MALWARE Sorano Stealer CnC Checkin
- [x] ET MALWARE Suspicious Zipped Filename in Outbound POST Request (Passwords.txt)
- [x] ET MALWARE Lemon_Duck Powershell CnC Checkin M2
- [x] ET MALWARE Observed Malicious SSL Cert (MSIL/Agent.TRM CnC)
- [x] ET MALWARE MSIL/Agent.TRM Task Command
- [x] ET MALWARE Possible DACLS RAT CnC (Log Check)
- [x] ET MALWARE Possible DACLS RAT Log Collector Download
- [x] ET MALWARE Win32/Agent.AAIB Variant CnC
- [x] ET MALWARE DDG Botnet CnC Slave POST
- [x] ET MALWARE DCRat CnC Activity
- [ ] ET MALWARE Suspected SPECULOOS Backdoor CnC Init Packet Masquerading as SNI Request to live .com
- [x] ET MALWARE ELF/Mirai Variant CnC Activity
- [x] ET MALWARE Observed Malicious SSL Cert (Malicious Browser Ext CnC)
- [ ] ET MALWARE Win32/CONFUCIUS_B CnC Checkin
- [x] ET MALWARE Observed Malicious SSL Cert (CONFUCIOUS_B CnC)
- [x] ET MALWARE AgentTesla HTML System Info Report Exfil via FTP
- [ ] ET MALWARE 401TRG SMB Create AndX Request For Emotet Spreader
- [x] ET MALWARE Targeted Activity - CnC Domain in SNI
- [x] ET MALWARE Observed PoetRAT Domain (dellgenius .hoptop .org in TLS SNI)
- [x] ET MALWARE Cobalt Strike Malleable C2 (Custom)
- [x] ET MALWARE JS Skimmer Domain in DNS Lookup
- [x] ET MALWARE Suspicious Long NULL DNS Request - Possible DNS Tunneling
- [x] ET MALWARE METALJACK APT32 CnC Host Checkin
- [x] ET MALWARE METALJACK APT32 DNS Lookup (jcdn.jsoid.com)
- [x] ET MALWARE METALJACK APT32 DNS Lookup (vitlescaux.com)
- [x] ET MALWARE SSL/TLS Certificate Observed (APT32 METALJACK)
- [x] ET MALWARE SSL/TLS Certificate Observed (APT32 METALJACK)
- [x] ET MALWARE Observed Malicious SSL Cert (Gozi ISFB)
- [x] ET MALWARE Observed Malicious SSL Cert (Gozi ISFB)
- [x] ET MALWARE ASNAROK Related Domain in TLS SNI
- [x] ET MALWARE ASNAROK Domain in TLS SNI
- [x] ET MALWARE DonotGroup CnC Domain in DNS Query
- [x] ET MALWARE BAZAR CnC Domain in DNS Lookup
- [x] ET MALWARE BAZAR CnC Domain in DNS Lookup
- [x] ET MALWARE BAZAR CnC Domain in DNS Lookup
- [x] ET MALWARE ELF/Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE IcedID CnC Domain in SNI
- [x] ET MALWARE Win32/Kryptik.HCZR Variant Initial Checkin
- [ ] ET MALWARE NAZAR EYService OSInfo response
- [x] ET MALWARE MINEBRIDGE CnC Request
- [x] ET MALWARE Rhabdo CnC Activity M1
- [x] ET MALWARE JAWS Webserver Unauthenticated Shell Command Execution
- [x] ET MALWARE IXWARE Stealer Domain in DNS Lookup
- [x] ET MALWARE WEBMONITOR RAT CnC Domain in DNS Lookup (dabmaster.wm01 .to)
- [x] ET MALWARE Nazar Implant - Sending Ping Response to CnC
- [x] ET MALWARE nspps Backdoor CnC Activity
- [x] ET MALWARE nspps Backdoor - Task Response
- [x] ET MALWARE Observed Cobalt Strike Stager Domain in DNS Query
- [x] ET MALWARE Ragnarok Ransomware CnC Activity M1
- [x] ET MALWARE EVILNUM CnC Response
- [x] ET MALWARE Zebrocy Screenshot Upload
- [x] ET MALWARE EVILNUM CnC Connectivity Check
- [x] ET MALWARE MAZE Ransomware Payment Domain in DNS Lookup
- [x] ET MALWARE Unk.VBSLoader Retrieving Payload

- [x] ET MALWARE MSIL/Modi RAT CnC Command Outbound (aw)
- [x] ET MALWARE MSIL/Modi RAT CnC Command Outbound (ds)
- [x] ET MALWARE M3RAT CnC Checkin Outbound
- [x] ET MALWARE PowerShell Downloader CnC Activity
- [x] ET MALWARE Observed TrojanSpy.SH.HADGLIDER.A Exfil Domain in DNS Query
- [x] ET MALWARE Possible Win32/Qbot/Quakbot Checkin via HTTP GET
- [x] ET MALWARE Taurus Stealer CnC Exfil
- [x] ET MALWARE BACKCONFIG CnC Downloader Activity
- [x] ET MALWARE Suspected USBFERRY CnC
- [x] ET MALWARE Win32/Ramsay CnC Checkin
- [x] ET MALWARE Win32/Ramsay CnC Domain in DNS Query
- [x] ET MALWARE Parallax CnC Activity M10 (set)
- [x] ET MALWARE BigLock Ransomware CnC Activity (info)
- [ ] ET MALWARE BigLock Ransomware CnC Activity (id)
- [x] ET MALWARE BigLock Ransomware CnC Activity (name)
- [x] ET MALWARE NORTHSTAR Client Data POST
- [x] ET MALWARE NORTHSTAR Command Sent to Client
- [x] ET MALWARE Observed JS/Magecart Domain in TLS SNI (manag .icu)
- [x] ET MALWARE eleethub botnet CnC Domain in DNS Lookup (ghost.eleethub .com)
- [x] ET MALWARE ELF/Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE BF Botnet CnC Checkin
- [x] ET MALWARE Observed MAZE Ransomware CnC Domain (checksoffice .me in TLS SNI)
- [x] ET MALWARE Observed MAZE Ransomware CnC Domain (thesawmeinrew .net in TLS SNI)
- [x] ET MALWARE Possible Konni Encrypted Stage 2 Payload Inbound via HTTP
- [x] ET MALWARE Socelars Stealer CnC Activity
- [x] ET MALWARE Backdoor.Elise Style IP Check M2
- [x] ET MALWARE Gamaredon Style MalDoc .dot Download on freedynamicdns .org
- [x] ET MALWARE Observed OSX/NukeSped Variant CnC Domain (fudcitydelivers .com) in TLS SNI
- [x] ET MALWARE TURLA NETFLASH CnC
- [x] ET MALWARE ELF/Kinsing Payload Request M2
- [x] ET MALWARE Observed Malicious SSL Cert (CobaltStrike CnC)
- [x] ET MALWARE Blaze/Supreme Bot Activity
- [x] ET MALWARE Observed Malicious SSL Cert (OZH Rat)
- [x] ET MALWARE Observed Malicious DNS Query (BazarLoader/Team9 Backdoor CnC Domain)
- [x] ET MALWARE Observed Malicious DNS Query (BazarLoader/Team9 Backdoor CnC Domain)
- [x] ET MALWARE ELF/Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE Win32/LODEINFO v0.3.6 CnC Checkin
- [x] ET MALWARE Downloader Retrieving Malicious Powershell in DNS Response
- [x] ET MALWARE Observed Malicious SSL Cert (DonotGroup CnC)
- [x] ET MALWARE DonotGroup Staging Domain in DNS Query
- [x] ET MALWARE Request for Malicious .dat File
- [x] ET MALWARE Observed Malicious SSL Cert (OceanLotus APT CnC)
- [x] ET MALWARE FRat WebSockets Request M2
- [x] ET MALWARE Observed Malicious SSL Cert (Cobalt Strike Malleable C2 Domain)
- [x] ET MALWARE SSL/TLS Certificate Observed (DiplomatLoader)
- [x] ET MALWARE Operation Interception Beacon
- [x] ET MALWARE STRRAT CnC Checkin
- [x] ET MALWARE STRRAT Requesting License Check
- [x] ET MALWARE Win32/Adware.Agent.NSU CnC Activity
- [x] ET MALWARE HTTPCore CnC Task Response
- [x] ET MALWARE CollectorStealer CnC Exfil
- [x] ET MALWARE MSIL/Modi RAT CnC Command Inbound (in)
- [x] ET MALWARE MSIL/Modi RAT CnC Screenshot Outbound
- [x] ET MALWARE Unk.VBSLoader Retrieving Payload
- [x] ET MALWARE MASSLOGGER Client Data Exfil (POST)
- [x] ET MALWARE Hakbit/Thanos Ransomware Exfil via FTP
- [x] ET MALWARE Taurus Stealer CnC Host Checkin
- [x] ET MALWARE AutoHotkey Downloader Checkin via IPLogger
- [x] ET MALWARE GandCrab Style External IP Check (Spoofed Yahoo Host)
- [x] ET MALWARE AgentTesla Exfil Via SMTP
- [x] ET MALWARE Win32/Ramsay CnC Domain in DNS Query
- [x] ET MALWARE Observed Win32/DecryptStealer Exfil Domain (geroipanel .site in TLS SNI)
- [x] ET MALWARE Parallax CnC Response Activity M10
- [ ] ET MALWARE BigLock Ransomware CnC Activity (gen)
- [x] ET MALWARE BigLock Ransomware CnC Activity (ext)
- [x] ET MALWARE NORTHSTAR Client CnC Checkin
- [x] ET MALWARE NORTHSTAR Interactive Client CnC
- [x] ET MALWARE NORTHSTAR Command Response
- [x] ET MALWARE eleethub botnet CnC Domain in DNS Lookup (irc.eleethub .com)
- [x] ET MALWARE eleethub .com Domain in DNS Lookup (eleethub .com)
- [x] ET MALWARE SystemdMiner CnC Activity
- [x] ET MALWARE Suspected APT15/NICKEL KETRUM CnC Activity (GET)
- [x] ET MALWARE Observed MAZE Ransomware CnC Domain (plaintsotherest .net in TLS SNI)
- [x] ET MALWARE Konni Stage 2 Payload Exfiltrating Data
- [x] ET MALWARE Observed Malicious SSL Cert (MalDoc DL 2020-05-27)
- [x] ET MALWARE COMRAT CnC
- [x] ET MALWARE OSX/SHLAYER CnC Checkin
- [x] ET MALWARE Higasia CnC Activity
- [x] ET MALWARE Observed OSX/NukeSped Variant CnC Domain (sctemarkets .com) in TLS SNI
- [x] ET MALWARE ELF/Kinsing Payload Request M1
- [x] ET MALWARE Observed DNS Query to known Avaddon Ransomware Payment Domain
- [x] ET MALWARE Win32/Avaddon Ransomware Style External IP Address Check
- [x] ET MALWARE Blaze/Supreme Bot Activity M2
- [x] ET MALWARE Higaisa CnC (ipconfig)
- [x] ET MALWARE Observed Malicious DNS Query (BazarLoader/Team9 Backdoor CnC Domain)
- [x] ET MALWARE Observed Malicious DNS Query (BazarLoader/Team9 Backdoor CnC Domain)
- [x] ET MALWARE FRat WebSocket Request M1
- [x] ET MALWARE Win32/LODEINFO v0.3.5 CnC Checkin
- [x] ET MALWARE Echelon/Mist Stealer CnC Activity
- [x] ET MALWARE DonotGroup Staging Domain in DNS Query
- [x] ET MALWARE DonotGroup Staging Domain in DNS Query
- [x] ET MALWARE Observed Koadic Header Structure
- [x] ET MALWARE Cobalt Strike Malleable C2 (Safebrowse Profile) POST
- [x] ET MALWARE Cobalt Strike Malleable C2 (Safebrowse Profile) GET
- [x] ET MALWARE Observed Malicious SSL Cert (MalDoc DL 2020-06-18)
- [x] ET MALWARE Possible DNS Tunneling Observed
- [x] ET MALWARE Win32/Ispen BADNEWS CnC Beacon
- [x] ET MALWARE STRRAT Initial HTTP Activity
- [x] ET MALWARE Win32/Ispen BADNEWS Fake User-Agent
- [x] ET MALWARE HTTPCore CnC Task Request
- [x] ET MALWARE HTTPCore CnC Tasking File
- [x] ET MALWARE VikroStealer CnC Exfil

- ☑ ET MALWARE VikroStealer Retrieving Config
- ☑ ET MALWARE ELF/Mirai Variant User-Agent (Outbound)
- ☐ ET MALWARE Operation Interception Payload CnC Checkin
- ☑ ET MALWARE Observed VikroStealer CnC Domain in TLS SNI
- ☑ ET MALWARE HiveRAT CnC Activity M1
- ☑ ET MALWARE GoldenSpy CnC Activity
- ☑ ET MALWARE GoldenSpy CnC Activity
- ☑ ET MALWARE RCtrl Backdoor CnC Checkin M2
- ☑ ET MALWARE RCtrl Backdoor CnC Checkin M1
- ☑ ET MALWARE LumOffice Checkin
- ☑ ET MALWARE Trojan/MSIL.DOTHETUK CnC Activity
- ☑ ET MALWARE Observed StrongPity CnC Domain in TLS SNI
- ☑ ET MALWARE Observed StrongPity CnC Domain in TLS SNI
- ☑ ET MALWARE Observed StrongPity CnC Domain in TLS SNI
- ☑ ET MALWARE Observed StrongPity CnC Domain in TLS SNI
- ☑ ET MALWARE Observed StrongPity CnC Domain in TLS SNI
- ☑ ET MALWARE Observed StrongPity CnC Domain in TLS SNI
- ☑ ET MALWARE Observed StrongPity CnC Domain in TLS SNI
- ☑ ET MALWARE Observed StrongPity CnC Domain in TLS SNI
- ☑ ET MALWARE Observed StrongPity CnC Domain in TLS SNI
- ☑ ET MALWARE Observed StrongPity CnC Domain in TLS SNI
- ☑ ET MALWARE Observed StrongPity CnC Domain in TLS SNI
- ☑ ET MALWARE Suspected Glupteba Download
- ☑ ET MALWARE Glupteba CnC Checkin
- ☑ ET MALWARE AlinaPOS Exfiltration via DNS
- ☑ ET MALWARE AlinaPOS Exfiltration via DNS
- ☑ ET MALWARE AlinaPOS Exfiltration via DNS
- ☑ ET MALWARE Observed CobaltStrike CnC Domain in TLS SNI
- ☑ ET MALWARE Observed CobaltStrike CnC Domain in TLS SNI
- ☑ ET MALWARE Observed CobaltStrike CnC Domain in TLS SNI
- ☑ ET MALWARE Observed CobaltStrike CnC Domain in TLS SNI
- ☑ ET MALWARE Observed CobaltStrike CnC Domain in TLS SNI
- ☑ ET MALWARE Observed Malicious SSL Cert (CobaltStrike CnC)
- ☑ ET MALWARE Observed Malicious SSL Cert (CobaltStrike CnC)
- ☑ ET MALWARE Observed Malicious SSL Cert (CobaltStrike CnC)
- ☑ ET MALWARE Observed Malicious SSL Cert (CobaltStrike CnC)
- ☑ ET MALWARE Observed Malicious SSL Cert (CobaltStrike CnC)
- ☑ ET MALWARE ELF/Mirai Variant User-Agent (Outbound)
- ☑ ET MALWARE Observed Malicious SSL Cert (TaurusStealer CnC)
- ☑ ET MALWARE SuperKillerX Checkin Activity
- ☑ ET MALWARE Magecart/Skimmer Domain in DNS Lookup (cddn .site)
- ☑ ET MALWARE Magecart/Skimmer Domain in DNS Lookup (yzxi .net)
- ☑ ET MALWARE Observed Malicious SSL Cert (Zloader CnC)
- ☑ ET MALWARE ELF/MooBot Mirai DDoS Variant CnC Checkin M1 (Group String Len 1)
- ☑ ET MALWARE FRAT Downloader Activity
- ☑ ET MALWARE ELF/BASHLITE vbot Variant CnC
- ☑ ET MALWARE Supercharge Component Download (ps1)
- ☑ ET MALWARE EvilNum CnC Checkin
- ☐ ET MALWARE EvilNum CnC Client Data Exfil
- ☑ ET MALWARE EvilNum CnC Client Data Exfil
- ☑ ET MALWARE APT29/WellMess CnC Activity
- ☑ ET MALWARE BYOB - Python Backdoor Stager Download
- ☑ ET MALWARE NEWPASS CnC Client Checkin
- ☑ ET MALWARE Win32/Delf.BLL Variant CnC Activity (Inbound)
- ☑ ET MALWARE Observed IcedID CnC Domain in TLS SNI
- ☑ ET MALWARE Observed IcedID CnC Domain in TLS SNI
- ☑ ET MALWARE Observed IcedID CnC Domain in TLS SNI
- ☑ ET MALWARE Observed IcedID CnC Domain in TLS SNI
- ☑ ET MALWARE Observed IcedID CnC Domain in TLS SNI
- ☑ ET MALWARE Observed IcedID CnC Domain in TLS SNI
- ☑ ET MALWARE Win32/Fujacks Variant CnC Activity
- ☑ ET MALWARE IP Grabber CnC Activity
- ☑ ET MALWARE Observed Malicious SSL Cert (JS/Ostap CnC)
- ☑ ET MALWARE Observed VikroStealer CnC Domain in TLS SNI
- ☑ ET MALWARE ELF/Mirai Variant User-Agent (Outbound)
- ☑ ET MALWARE Patchwork Staging Domain in DNS Query
- ☑ ET MALWARE SluttyPutty isDebuggerPresent in Fake Putty Executable
- ☑ ET MALWARE Jupyter Stealer Reporting System Information
- ☑ ET MALWARE Rovnix CnC Domain in DNS Query
- ☑ ET MALWARE RHttpCtrl Backdoor CnC
- ☑ ET MALWARE Possible IndigoDrop/Cobalt Strike Download
- ☑ ET MALWARE RezoStealer CnC Checkin
- ☑ ET MALWARE Observed Malicious SSL Cert (AsyncRAT CnC)
- ☑ ET MALWARE Observed Malicious SSL Cert (StrongPity CnC)
- ☑ ET MALWARE Observed Malicious SSL Cert (StrongPity CnC)
- ☑ ET MALWARE Observed Malicious SSL Cert (StrongPity CnC)
- ☑ ET MALWARE Observed StrongPity CnC Domain in TLS SNI
- ☑ ET MALWARE Observed StrongPity CnC Domain in TLS SNI
- ☑ ET MALWARE Observed StrongPity CnC Domain in TLS SNI
- ☑ ET MALWARE Observed StrongPity CnC Domain in TLS SNI
- ☑ ET MALWARE Observed StrongPity CnC Domain in TLS SNI
- ☑ ET MALWARE Observed StrongPity CnC Domain in TLS SNI
- ☑ ET MALWARE Observed StrongPity CnC Domain in TLS SNI
- ☑ ET MALWARE Observed StrongPity CnC Domain in TLS SNI
- ☑ ET MALWARE Observed StrongPity CnC Domain in TLS SNI
- ☑ ET MALWARE Suspected Glupteba Download
- ☑ ET MALWARE Evil Google Drive Download
- ☑ ET MALWARE AlinaPOS Exfiltration via DNS
- ☑ ET MALWARE AlinaPOS Exfiltration via DNS
- ☑ ET MALWARE Lucifer CnC Checkin
- ☑ ET MALWARE Observed Malicious SSL Cert (CobaltStrike CnC)
- ☑ ET MALWARE Observed Malicious SSL Cert (CobaltStrike CnC)
- ☑ ET MALWARE Observed Malicious SSL Cert (CobaltStrike CnC)
- ☑ ET MALWARE Observed Malicious SSL Cert (CobaltStrike CnC)
- ☑ ET MALWARE Observed Malicious SSL Cert (CobaltStrike CnC)
- ☑ ET MALWARE Observed CobaltStrike CnC Domain in TLS SNI
- ☑ ET MALWARE Observed CobaltStrike CnC Domain in TLS SNI
- ☑ ET MALWARE Observed CobaltStrike CnC Domain in TLS SNI
- ☑ ET MALWARE Observed CobaltStrike CnC Domain in TLS SNI
- ☑ ET MALWARE Observed CobaltStrike CnC Domain in TLS SNI
- ☑ ET MALWARE Observed Malicious SSL Cert (Zeromax Stealer CnC)
- ☑ ET MALWARE Observed TaurusStealer CnC Domain in TLS SNI
- ☑ ET MALWARE SuperKillerX CnC Activity
- ☑ ET MALWARE Magecart/Skimmer Domain in DNS Lookup (cxizi .net)
- ☑ ET MALWARE Hakbit/Thanos Ransomware BMP Download
- ☑ ET MALWARE ELF/MooBot Mirai DDoS Variant Server Response
- ☑ ET MALWARE ELF/MooBot Mirai DDoS Variant CnC Checkin M2 (Group String Len 2+)
- ☑ ET MALWARE FRAT Downloader Error Report POST
- ☑ ET MALWARE Win32/DTStealer CnC Activity
- ☑ ET MALWARE Supercharge Component Download (exe)
- ☑ ET MALWARE EvilNum CnC Checkin Response
- ☑ ET MALWARE EvilNum CnC Client Data Exfil
- ☑ ET MALWARE EvilNum CnC Error Report
- ☑ ET MALWARE MASSLOGGER Client Data Exfil (POST) M2
- ☑ ET MALWARE BYOB - Python Backdoor Loader Download
- ☑ ET MALWARE Win32/Delf.BLL Variant CnC Activity (Outbound)
- ☑ ET MALWARE Win32/PSW.Agent.OIN CnC Activity
- ☑ ET MALWARE Observed IcedID CnC Domain in TLS SNI
- ☑ ET MALWARE Observed IcedID CnC Domain in TLS SNI
- ☑ ET MALWARE Observed IcedID CnC Domain in TLS SNI
- ☑ ET MALWARE Observed IcedID CnC Domain in TLS SNI
- ☑ ET MALWARE Observed IcedID CnC Domain in TLS SNI
- ☑ ET MALWARE Observed IcedID CnC Domain in TLS SNI
- ☑ ET MALWARE ELF/Mirai Variant User-Agent (Outbound)
- ☑ ET MALWARE JS/Ostap CnC Activity
- ☑ ET MALWARE Observed Malicious SSL Cert (MalDoc DL 2020-07-29)

- [x] ET MALWARE ThiefQuest CnC Domain in DNS Lookup
- [ ] ET MALWARE Observed Malicious SSL Cert (Lazarus APT MalDoc DL 2020-07-30)
- [ ] ET MALWARE Observed Lazarus APT MalDoc DL Domain in TLS SNI
- [ ] ET MALWARE Win32/PurpleWave Stealer Requesting Config
- [ ] ET MALWARE Win32/PurpleWave Stealer CnC Exfil
- [x] ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
- [x] ET MALWARE Matiex Keylogger Exfil Via Telegram
- [x] ET MALWARE OILRIG CnC POST
- [x] ET MALWARE Observed Malicious SSL Cert (Cobalt Strike CnC)
- [x] ET MALWARE Magecart/Skimmer Domain in DNS Lookup (cloud-sources .com)
- [x] ET MALWARE Magecart/Skimmer Domain in DNS Lookup (cdn-filestorm .com)
- [x] ET MALWARE TAIDOOR CnC Domain in DNS Lookup (www.cnaweb.mrslove .com)
- [x] ET MALWARE TAIDOOR CnC Domain in DNS Lookup (www.infonew.dubya .net)
- [x] ET MALWARE Observed Malicious SSL Cert (Get2 CnC)
- [x] ET MALWARE YAHOOYLO Stealer CnC Exfil
- [x] ET MALWARE Unknown AutoIt Bot - Initial Server Response
- [x] ET MALWARE Suspected APT32/Oceanlotus Maldoc CnC
- [x] ET MALWARE IcedID Observed Domain (loadfreeman .casa in TLS SNI)
- [x] ET MALWARE Observed IcedID Domain (deactivate .best in TLS SNI)
- [x] ET MALWARE Observed IcedID Domain (deactivate .pw in TLS SNI)
- [x] ET MALWARE Observed IcedID Domain (80frontluzkher .xyz in TLS SNI)
- [x] ET MALWARE Observed IcedID Domain (bruzilovv .top in TLS SNI)
- [x] ET MALWARE Observed IcedID Domain (ldrtoyota .casa in TLS SNI)
- [x] ET MALWARE AutoHotKey offthewall Downloader Requesting Payload
- [x] ET MALWARE Suspected Lockscreen Ransomware Activity
- [x] ET MALWARE Observed DCRat CnC Domain in TLS SNI
- [x] ET MALWARE Observed IcedID CnC Domain (nothingtodo .co in TLS SNI)
- [x] ET MALWARE APT Mustang Panda CnC Activity
- [x] ET MALWARE MSIL/JobCrypter Ransomware Checkin via SMTP
- [x] ET MALWARE Observed Malicious SSL Cert (AsyncRAT Server)
- [x] ET MALWARE Observed Malicious SSL Cert (More_eggs CnC)
- [x] ET MALWARE Win32/Tofsee Pharma Spam Template Active - Outbound Email Spam
- [x] ET MALWARE ELF/Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE Win32/TrojanDownloader.Agent.FC CnC Activity
- [x] ET MALWARE Ave Maria RAT CnC Domain in DNS Lookup (uknwn.linkpc .net)
- [x] ET MALWARE Qudox CnC Actiivty
- [x] ET MALWARE Drovorub cloud.auth Module Server Response
- [x] ET MALWARE Drovorub file Module Server Response
- [x] ET MALWARE Drovorub monitor Module Server Response
- [x] ET MALWARE Drovorub shell Module Server Response
- [x] ET MALWARE Drovorub tunnel Module Server Response
- [x] ET MALWARE Echelon/DarkStealer Variant CnC Exfil
- [x] ET MALWARE Suspected REDCURL CnC Activity M2
- [x] ET MALWARE Possible KONNI URI Path Observed
- [x] ET MALWARE Possible KONNI CnC Activity
- [x] ET MALWARE ELF/Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE Suspected REDCURL CnC Activity M1
- [x] ET MALWARE Trickbot/Anchor ICMP Request
- [x] ET MALWARE Echelon/DarkStealer Variant CnC Exfil M2
- [x] ET MALWARE Observed Malicious SSL Cert (GRIFFON CnC)
- [x] ET MALWARE GORGON APT Download Activity
- [x] ET MALWARE GORGON APT Download Activity M2
- [x] ET MALWARE Mekotio HTTP Method (111SA)
- [x] ET MALWARE Observed Malicious SSL Cert (Sidewinder CnC)
- [x] ET MALWARE Observed APT/SideWinder CnC Domain in TLS SNI
- [x] ET MALWARE Observed Malicious SSL Cert (BitRAT CnC)
- [x] ET MALWARE DeathStalker/Janicab CnC Checkin
- [x] ET MALWARE DeathStalker/Powersing CnC Checkin
- [x] ET MALWARE Win32/Agent.ACBD CnC Activity
- [ ] ET MALWARE Suspected Zebrocy Downloader Traffic
- [x] ET MALWARE Observed Malicious SSL Cert (AnubisStealer CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (AnubisStealer CnC)
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query

- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Observed Get2 CnC Domain in TLS SNI
- [x] ET MALWARE W32/Downloader_x.EJK!tr CnC Activity
- [x] ET MALWARE GoldenSpy Domain Observed
- [x] ET MALWARE Win32/AgentTesla Variant Exfil via Telegram
- [x] ET MALWARE Grandoreiro CnC Activity (iso)
- [x] ET MALWARE MSIL/CoinMiner Performing System Checkin
- [x] ET MALWARE Upatre User-Agent
- [x] ET MALWARE Zyklon CnC Activity
- [x] ET MALWARE Lemon_Duck Linux Shell Script CnC Activity
- [x] ET MALWARE Observed MageCart CnC Domain in TLS SNI
- [x] ET MALWARE Win32/TaskPerformer Downloader CnC Activity
- [x] ET MALWARE Observed Malicious SSL Cert (Baka Skimmer Staging CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (Baka Skimmer Staging CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (Baka Skimmer Staging CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (Baka Skimmer Staging CnC)
- [x] ET MALWARE Win32/Spy.Agent.PZE Variant CnC Activity
- [x] ET MALWARE Reimageplus Ransomware Checkin
- [x] ET MALWARE Observed Malicious SSL Cert (CobaltStrike CnC)
- [x] ET MALWARE Observed CoinMiner CnC Domain (enoyq5xy70oq .x .pipedream .net in TLS SNI)
- [x] ET MALWARE Observed CoinMiner CnC Domain (endpsbn1u6m8f .x .pipedream .net in TLS SNI)
- [ ] ET MALWARE DNSBin Demo (requestbin .net) - Data Exfil M1
- [x] ET MALWARE MassLogger Client Exfil (POST) M3
- [x] ET MALWARE Observed MageCart CnC Domain (mcdnn .me in TLS SNI)
- [x] ET MALWARE Observed Magecart Exfil Domain (imags .pw in TLS SNI)
- [x] ET MALWARE MageCart Exfil URI
- [x] ET MALWARE RedDelta Poison Ivy Domain in DNS Lookup
- [x] ET MALWARE RedDelta Poison Ivy Domain in DNS Lookup
- [x] ET MALWARE RampantKitten APT TelB Python Variant - CnC Checkin M1
- [x] ET MALWARE Observed Malicious SSL Cert (RampantKitten CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (Moist Stealer CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (Cobalt Strike CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (Cobalt Strike CnC)
- [x] ET MALWARE Win32/Sehyioa Variant Activity (Download)
- [x] ET MALWARE PS/SunCrypt Ransomware CnC Activity
- [x] ET MALWARE ELF/Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE FinSpy Related Flash Installer Activity
- [x] ET MALWARE APT39/Chafer Payload - CnC Checkin M2
- [x] ET MALWARE Mozi Botnet DHT Config Sent
- [x] ET MALWARE Vicious Panda CnC Activity
- [x] ET MALWARE Ttint XORed CnC Checkin
- [x] ET MALWARE Observed Ttint CnC Domain in DNS Query
- [x] ET MALWARE Observed Ttint Update CnC Domain in DNS Query
- [x] ET MALWARE Observed BLINDINGCAN Domain (www .automercado .co .cr in TLS SNI)
- [x] ET MALWARE BUILDINGCAN CnC Activity
- [x] ET MALWARE TA428 Tmanger Checkin
- [x] ET MALWARE XDMonitor Sending Debug Messages
- [x] ET MALWARE XDUpload Uploading Files
- [x] ET MALWARE XDUpload Sending Screenshot Upload Progress
- [x] ET MALWARE SLOTHFULMEDIA RAT CnC (POST)
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Phorpiex CnC Domain in DNS Query
- [x] ET MALWARE Observed Get2 CnC Domain in TLS SNI
- [x] ET MALWARE Grandoreiro Downloader Activity
- [x] ET MALWARE Babax Stealer Exfil via Telegram
- [x] ET MALWARE Grandoreiro CnC Activity (vbs)
- [x] ET MALWARE MassLogger Client Data Exfil SMTP
- [x] ET MALWARE C3Pool CoinMiner Setup Script Download
- [x] ET MALWARE Observed Malicious SSL Cert (Bazar Backdoor)
- [x] ET MALWARE Observed IcedID CnC Domain in TLS SNI
- [x] ET MALWARE Lemon_Duck CnC Activity
- [x] ET MALWARE TURLA APT CnC Activity
- [x] ET MALWARE MSIL/Juliens Botnet CnC Activity M1
- [x] ET MALWARE Observed Malicious SSL Cert (Baka Skimmer Staging CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (Baka Skimmer Staging CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (Baka Skimmer Staging CnC)
- [x] ET MALWARE APT29/Wellness CnC Host Checkin
- [x] ET MALWARE Observed Reimageplus Ransomware Domain in TLS SNI
- [x] ET MALWARE Win32/Valak Variant CnC
- [x] ET MALWARE Win32/Emotet CnC Activity (POST) M10
- [x] ET MALWARE Observed GoLang Dropper Domain (en7dftkjiipor .x .pipedream .net in TLS SNI)
- [x] ET MALWARE Observed CoinMiner CnC Domain (en24zuggh3ywlj .x .pipedream .net in TLS SNI)
- [ ] ET MALWARE DNSBin Demo (requestbin .net) - Data Inbound
- [x] ET MALWARE Observed MassLogger Domain in TLS SNI (ecigroup-tw .com)
- [x] ET MALWARE Observed MageCart CnC Domain (mcdnn .net in TLS SNI)
- [x] ET MALWARE MageCart JS Retrieval
- [x] ET MALWARE MSIL/Kryptik.XSY Data Exfil via SMTP
- [x] ET MALWARE RedDelta Poison Ivy Domain in DNS Lookup
- [x] ET MALWARE Unicorn Stealer Activity (POST)
- [x] ET MALWARE Observed Malicious SSL Cert (RampantKitten CnC)
- [x] ET MALWARE RampantKitten APT TelB Python Variant - CnC Checkin M2
- [ ] ET MALWARE Moist Stealer CnC Exfil
- [x] ET MALWARE Observed Malicious SSL Cert (Cobalt Strike CnC)
- [x] ET MALWARE Win32/Sehyioa Variant Activity (POST)
- [x] ET MALWARE Exorcist 2.0 Ransomware CnC Activity
- [x] ET MALWARE Win32/Predator Variant Dropper Activity
- [x] ET MALWARE FinSpy Related WinRAR Activity
- [x] ET MALWARE APT39/Chafer Payload - CnC Checkin M1
- [x] ET MALWARE Trojan.Win32.Codenox.gyezu CnC Activity
- [x] ET MALWARE Vicious Panda Checkin
- [x] ET MALWARE Observed Malicious SSL Cert (CoreDn/BLINDINGCAN Activity)
- [x] ET MALWARE Observed Ttint CnC Domain in DNS Query
- [x] ET MALWARE Observed Ttint CnC Domain in DNS Query
- [x] ET MALWARE Observed BLINDINGCAN Domain (www .sanlorenzoyacht .com in TLS SNI)
- [x] ET MALWARE Observed BLINDINGCAN Domain (www .ne-ba .org in TLS SNI)
- [x] ET MALWARE Observed Malicious SSL Cert (AsyncRAT CnC)
- [x] ET MALWARE TA428 Infostealer CnC Host Checkin
- [x] ET MALWARE XDUpload Uploading Directory Listting
- [x] ET MALWARE XDUpload Sending File Upload Progress
- [x] ET MALWARE XDMonitor Checkin Activity
- [x] ET MALWARE Observed FinSpy Domain (browserupdate .download in TLS SNI)

- [x] ET MALWARE Observed Malicious SSL Cert (MosaicRegressor WinHTTP Downloader)
- [x] ET MALWARE Observed Malicious SSL Cert (Fullz House CC Skimmer)
- [x] ET MALWARE Observed Malicious SSL Cert (Fullz House CC Skimmer)
- [x] ET MALWARE Observed Malicious SSL Cert (Fullz House CC Skimmer)
- [x] ET MALWARE Observed Malicious SSL Cert (Fullz House CC Skimmer)
- [x] ET MALWARE Observed Malicious SSL Cert (Fullz House CC Skimmer)
- [x] ET MALWARE Observed Malicious SSL Cert (Fullz House CC Skimmer)
- [x] ET MALWARE Observed Malicious SSL Cert (Fullz House CC Skimmer)
- [x] ET MALWARE Fullz House Credit Card Skimmer JavaScript Inbound
- [x] ET MALWARE Aerial Keylogger DNS Request
- [x] ET MALWARE Tonto_SPM Backdoor CnC Activity
- [x] ET MALWARE MontysThree HTTPTransport Module Activity
- [x] ET MALWARE PowerGhost Staging CnC in DNS Query
- [x] ET MALWARE PoetRAT Upload via HTTP
- [x] ET MALWARE StormKitty Data Exfil via Telegram
- [x] ET MALWARE StormKitty Exfil via AnonFiles
- [x] ET MALWARE Observed IcedID CnC Domain in TLS SNI
- [x] ET MALWARE Observed IcedID CnC Domain in TLS SNI
- [x] ET MALWARE GravityRAT CnC Domain (bollywoods .co .in in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (chuki .mozillaupdates .us in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (cvstyler .co .in in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (dailybuild .mozillaupdates .com in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (gozap .co .in in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (melodymate .co .in in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (nightly .windowsupdates .eu in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (orangevault .net in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (savitabhabi .co .in in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (strongbox .in in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (titaniumx .co .in in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (microsoftupdate .in in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (x-trust .net in DNS Lookup)
- [x] ET MALWARE Observed Malicious SSL Cert (AsyncRAT CnC)
- [x] ET MALWARE MSIL/GravityRAT CnC Checkin M2
- [x] ET MALWARE SolarSys CnC Activity M1
- [x] ET MALWARE Mustang Panda/RedDelta Downloader Activity
- [x] ET MALWARE Possible T-RAT Encrypted Zip Request M1
- [x] ET MALWARE Bazaloader Variant Activity
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Terse Upload to Free Image Hosting Provider (uploads .im) - Likely Malware
- [x] ET MALWARE DTLoader Binary Request
- [x] ET MALWARE DTLoader Domain (ahgwqrq .xyz in TLS SNI)
- [x] ET MALWARE Win32/Ficker Stealer Activity M3
- [x] ET MALWARE ELF/Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE Observed Malicious SSL Cert (Fullz House CC Skimmer)
- [x] ET MALWARE Observed Malicious SSL Cert (Fullz House CC Skimmer)
- [x] ET MALWARE Observed Malicious SSL Cert (Fullz House CC Skimmer)
- [x] ET MALWARE Observed Malicious SSL Cert (Fullz House CC Skimmer)
- [x] ET MALWARE Observed Malicious SSL Cert (Fullz House CC Skimmer)
- [x] ET MALWARE Observed Malicious SSL Cert (Fullz House CC Skimmer)
- [x] ET MALWARE Fullz House Credit Card Skimmer Data Exfil
- [x] ET MALWARE Observed Malicious SSL Cert (Strongpity CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (BazaLoader CnC)
- [x] ET MALWARE Observed PoetRAT Domain (slimip .accesscam .org in TLS SNI)
- [x] ET MALWARE ELF/Mirai Variant User-Agent (Outbound)
- [x] ET MALWARE PowerGhost Checkin CnC in DNS Query
- [x] ET MALWARE PoetRAT CnC Domain in DNS Lookup
- [x] ET MALWARE Likely Malware CnC Hosted on 000webhostapp - POST to gate.php
- [x] ET MALWARE Observed IcedID CnC Domain in TLS SNI
- [x] ET MALWARE Observed IcedID CnC Domain in TLS SNI
- [x] ET MALWARE Observed IcedID CnC Domain in TLS SNI
- [x] ET MALWARE GravityRAT CnC Domain (chat2hire .net in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (click2chat .org in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (daily .windowsupdates .eu in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (enigma .net .in in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (gyzu .mozillaupdates .us in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (nortonupdates .online in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (nightlybuild .mozillaupdates .com in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (sake .mozillaupdates .us in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (sharify .co .in in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (teraspace .co .in in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (msoftserver .eu in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (wesharex .net in DNS Lookup)
- [x] ET MALWARE GravityRAT CnC Domain (zen .mozillaupdates .us in DNS Lookup)
- [x] ET MALWARE Observed Malicious SSL Cert (AsyncRAT CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (Cobalt Strike CnC)
- [x] ET MALWARE Mustang Panda/RedDelta Activity
- [x] ET MALWARE Win32/Ficker Stealer Activity
- [x] ET MALWARE Bazaloader Variant Activity
- [x] ET MALWARE Win32/Spy.Pavica.FH Variant CnC Activity
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Magecart CnC Domain Observed in DNS Query
- [x] ET MALWARE Amarula IRC Botnet Connection Request
- [x] ET MALWARE Observed Malicious SSL Cert (Cobalt Strike CnC)
- [x] ET MALWARE DTLoader Encoded Binary - Server Response
- [x] ET MALWARE Win32/Ficker Stealer Activity M2
- [x] ET MALWARE Possible UNC1878/FIN12 Cobalt Strike CnC SSL Cert Inbound (lol)

- [x] ET MALWARE Possible UNC1878/FIN12 Cobalt Strike CnC SSL Cert Inbound (office)
- [x] ET MALWARE Possible UNC1878 Cobalt Strike CnC SSL Cert Inbound (Mountainvew)
- [x] ET MALWARE ComRAT CnC Domain in DNS Lookup
- [x] ET MALWARE ComRAT CnC Domain in DNS Lookup
- [x] ET MALWARE ComRAT CnC Domain in DNS Lookup
- [x] ET MALWARE Python/PBot Browser Hijacker Activity
- [x] ET MALWARE Observed BazarLoader Domain (cntrhum .xyz in TLS SNI)
- [x] ET MALWARE Observed BazarLoader Domain (sh78bug .xyz in TLS SNI)
- [x] ET MALWARE Observed BazarLoader Domain (bigjamg .xyz in TLS SNI)
- [x] ET MALWARE Observed BazarLoader Domain (gut45bg .xyz in TLS SNI)
- [x] ET MALWARE Trickbot Anchor ICMP Request
- [x] ET MALWARE D1onis Stealer Sending Data to CnC
- [x] ET MALWARE Observed Malicious SSL Cert (DonotGroup FireStarter CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (DonotGroup FireStarter CnC)
- [x] ET MALWARE Kimsuky KGH Malware Suite Checkin M2
- [x] ET MALWARE Kimsuky CSPY Downloader Activity
- [x] ET MALWARE W32/Kimsuky Sending Encrypted System Information to CnC
- [x] ET MALWARE Kimsuky WildCommand CnC Activity
- [x] ET MALWARE Pay2Key Ransomware - Sending RSA Key
- [ ] ET MALWARE Suspected Snugy DNS Backdoor CnC Activity (Hostname Send)
- [x] ET MALWARE Win32/HunterStealer/AlfonsoStealer/PhoenixStealer CnC Exfil
- [ ] ET MALWARE CCleaner Backdoor DGA Domain (ab1de19d80ae6 .com) in DNS Lookup
- [x] ET MALWARE ModPipe CnC Activity (POST)
- [x] ET MALWARE Win32/Phorpiex Template 6 Active - Outbound Malicious Email Spam
- [x] ET MALWARE Observed DonotGroup CnC in DNS Query
- [x] ET MALWARE Win32/Spy.Agent.QAQ Variant CnC Activity
- [x] ET MALWARE Observed Blackrota Domain (blackrato .ga in TLS SNI)
- [x] ET MALWARE Geocon CnC Request
- [x] ET MALWARE Win32/Trickbot Data Exfiltration
- [x] ET MALWARE Observed DNS Query to WHO Themed Malware Delivery Domain
- [x] ET MALWARE Observed DNS Query to WHO Themed Malware Delivery Domain
- [x] ET MALWARE Possible SombRAT Initial DNS Lookup
- [ ] ET MALWARE Turla/Crutch CnC Domain in DNS Lookup (highcolumn .webredirect .org)
- [ ] ET MALWARE Turla/Crutch CnC Domain in DNS Lookup (theguardian .webredirect .org)
- [x] ET MALWARE DeathStalker/PowerPepper CnC Domain in DNS Lookup (mediqhealthcare .com)
- [x] ET MALWARE DarkIRC Bot CnC Domain Lookup
- [x] ET MALWARE Observed Jupyter Stealer CnC Domain (blackl1vesmatter .org in TLS SNI)
- [x] ET MALWARE Win32/IcedID Requesting Encoded Binary M5
- [x] ET MALWARE APT LuckyMouse Polpo Malware CnC
- [x] ET MALWARE Suspected APT LuckyMouse BlueTraveller CnC
- [x] ET MALWARE [Fireeye] Backdoor.BEACON M2
- [x] ET MALWARE Possible UNC1878/FIN12 Cobalt Strike CnC SSL Cert Inbound (Texsa)
- [x] ET MALWARE ComRAT CnC Domain in DNS Lookup
- [x] ET MALWARE ComRAT CnC Domain in DNS Lookup
- [x] ET MALWARE ComRAT CnC Domain in DNS Lookup
- [x] ET MALWARE Win32/Ymacco.AA67 CnC Activity
- [x] ET MALWARE Observed BazarLoader Domain (vighik .xyz in TLS SNI)
- [x] ET MALWARE Observed BazarLoader Domain (doldig .xyz in TLS SNI)
- [x] ET MALWARE Observed BazarLoader Domain (dghns .xyz in TLS SNI)
- [x] ET MALWARE Observed BazarLoader Domain (numklo .xyz in TLS SNI)
- [x] ET MALWARE Observed BazarLoader Domain (moig .xyz in TLS SNI)
- [x] ET MALWARE LolliCrypt Ransomware Sending Data to CnC
- [x] ET MALWARE Observed Malicious SSL Cert (DonotGroup FireStarter CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (DonotGroup FireStarter CnC)
- [x] ET MALWARE Kimsuky KGH Malware Suite Checkin M1
- [x] ET MALWARE Kimsuky KGH Backdoor Secondary Payload Download Request
- [x] ET MALWARE Kimsuky KGH Backdoor CnC Activity
- [x] ET MALWARE Kimsuky KGH Backdoor CnC Activity M2
- [x] ET MALWARE Win32/PurpleWave Stealer CnC Exfil M2
- [ ] ET MALWARE Suspected Snugy DNS Backdoor Initial Beacon
- [ ] ET MALWARE DNS Reply Sinkhole - Anubis/BitSight - 35.205.61.67
- [x] ET MALWARE Observed Card Skimmer CnC Domain in TLS SNI
- [x] ET MALWARE APT Lazarus Nukesped Downloader
- [ ] ET MALWARE ModPipe CnC Activity (Response)
- [x] ET MALWARE Observed Malicious SSL Cert (DonotGroup CnC)
- [ ] ET MALWARE Win32/SDBbot CnC Checkin
- [x] ET MALWARE Observed DNS Query to Blackrota Domain
- [x] ET MALWARE Observed Malicious SSL Cert (Blackrota)
- [x] ET MALWARE Observed Malicious SSL Cert (Lazarus APT MalDoc 2020-11-30)
- [x] ET MALWARE Observed DNS Query to WHO Themed Malware Delivery Domain
- [x] ET MALWARE Observed DNS Query to WHO Themed Malware Delivery Domain
- [x] ET MALWARE Observed DNS Query to WHO Themed Malware Delivery Domain
- [ ] ET MALWARE Turla/Crutch CnC Domain in DNS Lookup (hotspot .accesscam .org)
- [ ] ET MALWARE Turla/Crutch CnC Domain in DNS Lookup (ethdns .mywire .org)
- [x] ET MALWARE DeathStalker/PowerPepper CnC Domain in DNS Lookup (allmedicalpro .com)
- [x] ET MALWARE DeathStalker/PowerPepper CnC Domain in DNS Lookup (gofinancesolutions .com)
- [x] ET MALWARE Observed Jupyter Stealer CnC Domain (gogohid .com in TLS SNI)
- [x] ET MALWARE Observed Jupyter Stealer CnC Domain (vincentolife .com in TLS SNI)
- [x] ET MALWARE APT LuckyMouse Polpo Malware CnC
- [x] ET MALWARE APT28/Sofacy Zebrocy CnC DNS Lookup (support-cloud .life)
- [x] ET MALWARE APT LuckyMouse Polpo Malware CnC
- [x] ET MALWARE [Fireeye] Backdoor.BEACON M6

- [x] ET MALWARE [Fireeye] Backdoor.BEACON M1
- [x] ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to thedoccloud .com
- [x] ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to freescanonline .com
- [x] ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to highdatabase .com
- [x] ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to databasegalore .com
- [x] ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to zupertech .com
- [x] ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to digitalcollege .org
- [x] ET MALWARE [Fireeye] Backdoor.SUNBURST M2
- [x] ET MALWARE [Fireeye] Backdoor.SUNBURST M3
- [x] ET MALWARE [Fireeye] Backdoor.SUNBURST SSL Cert Inbound (avsvmcloud .com)
- [x] ET MALWARE [Fireeye] Backdoor.SUNBURST SSL Cert Inbound (freescanonline .com)
- [x] ET MALWARE [Fireeye] Backdoor.SUNBURST SSL Cert Inbound (thedoccloud .com)
- [x] ET MALWARE [Fireeye] Backdoor.SUNBURST HTTP Request to digitalcollege .org
- [x] ET MALWARE [Fireeye] Backdoor.SUNBURST HTTP Request to deftsecurity .com
- [x] ET MALWARE [Fireeye] Backdoor.SUNBURST HTTP Request to virtualdataserver .com
- [x] ET MALWARE [Fireeye] Backdoor.BEACON SSL Cert Inbound (zupertech .com)
- [x] ET MALWARE [Fireeye] Backdoor.BEACON SSL Cert Inbound (panhardware .com)
- [x] ET MALWARE [Fireeye] Backdoor.BEACON M4
- [x] ET MALWARE [Fireeye] Observed SUNBURST DGA Request
- [x] ET MALWARE [Fireeye] Backdoor.SUNBURST SSL Cert Inbound (highdatabase .com)
- [x] ET MALWARE [Fireeye] Observed Backdoor.SUNBURST CnC Domain (incomeudpate .com in TLS SNI)
- [x] ET MALWARE [Fireeye] Observed Backdoor.SUNBURST CnC Domain (freescanonline .com in TLS SNI)
- [x] ET MALWARE [Fireeye] Observed Backdoor.SUNBURST CnC Domain (highdatabase .com in TLS SNI)
- [x] ET MALWARE [Fireeye] Observed Backdoor.SUNBURST CnC Domain (zupertech .com in TLS SNI)
- [x] ET MALWARE MICROPSIA CnC Checkin
- [x] ET MALWARE APT32/OceanLotus Associated Domain in DNS Lookup (qh2020 .org)
- [x] ET MALWARE APT32/OceanLotus Associated Domain in DNS Lookup (tocaoonline .org)
- [x] ET MALWARE APT32/OceanLotus Associated Domain in DNS Lookup (nhansudaihoi13 .org)
- [x] ET MALWARE Dark Halo/SUNBURST SSL Cert Inbound (solartrackingsystem .net)
- [x] ET MALWARE Dark Halo/SUNBURST SSL Cert Inbound (lcomputers .com)
- [x] ET MALWARE Dark Halo/SUNBURST SSL Cert Inbound (kubecloud .com)
- [x] ET MALWARE Dark Halo/SUNBURST Related DNS Lookup to solartrackingsystem .net
- [x] ET MALWARE Dark Halo/SUNBURST Related DNS Lookup to lcomputers .com
- [x] ET MALWARE Dark Halo/SUNBURST Related DNS Lookup to kubecloud .com
- [x] ET MALWARE Dark Halo/SUNBURST CnC Domain (solartrackingsystem .net in TLS SNI)
- [x] ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to avsvmcloud .com
- [x] ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to deftsecurity .com
- [x] ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to websitetheme .com
- [x] ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to incomeupdate .com
- [x] ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to panhardware .com
- [x] ET MALWARE [Fireeye] SUNBURST Related DNS Lookup to virtualdataserver .com
- [x] ET MALWARE [Fireeye] Backdoor.SUNBURST M1
- [x] ET MALWARE [Fireeye] Backdoor.SUNBURST HTTP Request to avsvmcloud .com
- [x] ET MALWARE [Fireeye] Backdoor.SUNBURST M4
- [x] ET MALWARE [Fireeye] Backdoor.SUNBURST SSL Cert Inbound (digitalcollege .org)
- [x] ET MALWARE [Fireeye] Backdoor.SUNBURST SSL Cert Inbound (deftsecurity .com)
- [x] ET MALWARE [Fireeye] Backdoor.SUNBURST SSL Cert Inbound (virtualdataserver .com)
- [x] ET MALWARE [Fireeye] Backdoor.SUNBURST HTTP Request to freescanonline .com
- [x] ET MALWARE [Fireeye] Backdoor.SUNBURST HTTP Request to thedoccloud .com
- [x] ET MALWARE [Fireeye] Backdoor.BEACON SSL Cert Inbound (incomeupdate .com)
- [x] ET MALWARE [Fireeye] Backdoor.BEACON SSL Cert Inbound (databasegalore .com)
- [x] ET MALWARE [Fireeye] Backdoor.BEACON M3
- [x] ET MALWARE [Fireeye] Backdoor.BEACON M5
- [x] ET MALWARE [Fireeye] Backdoor.SUNBURST SSL Cert Inbound (websitetheme .com)
- [x] ET MALWARE [Fireeye] Observed Backdoor.SUNBURST CnC Domain (thedoccloud .com in TLS SNI)
- [x] ET MALWARE [Fireeye] Observed Backdoor.SUNBURST CnC Domain (panhardware .com in TLS SNI)
- [x] ET MALWARE [Fireeye] Observed Backdoor.SUNBURST CnC Domain (databasegalore .com in TLS SNI)
- [x] ET MALWARE [Fireeye] Observed Backdoor.SUNBURST CnC Domain (websitetheme .com in TLS SNI)
- [x] ET MALWARE [Fireeye] Observed Backdoor.SUNBURST CnC Domain (deftsecurity .com in TLS SNI)
- [x] ET MALWARE APT32/OceanLotus Associated Domain in DNS Lookup (tocaoonline .com)
- [x] ET MALWARE APT32/OceanLotus Associated Domain in DNS Lookup (tinmoivietnam .com)
- [x] ET MALWARE APT32/OceanLotus Associated Domain in DNS Lookup (facebookdeck .com)
- [x] ET MALWARE APT32/OceanLotus Associated Domain in DNS Lookup (thundernews .org)
- [x] ET MALWARE Dark Halo/SUNBURST SSL Cert Inbound (webcodez .com)
- [x] ET MALWARE Dark Halo/SUNBURST SSL Cert Inbound (seobundlekit .com)
- [x] ET MALWARE Dark Halo/SUNBURST SSL Cert Inbound (globalnetworkissues .com)
- [x] ET MALWARE Dark Halo/SUNBURST Related DNS Lookup to webcodez .com
- [x] ET MALWARE Dark Halo/SUNBURST Related DNS Lookup to seobundlekit .com
- [x] ET MALWARE Dark Halo/SUNBURST Related DNS Lookup to globalnetworkissues .com
- [x] ET MALWARE Dark Halo/SUNBURST CnC Domain (webcodez .com in TLS SNI)

- [x] ET MALWARE Dark Halo/SUNBURST CnC Domain (lcomputers .com in TLS SNI)
- [x] ET MALWARE Dark Halo/SUNBURST CnC Domain (kubecloud .com in TLS SNI)
- [x] ET MALWARE Observed AridViper CnC Domain in TLS SNI
- [x] ET MALWARE Observed AridViper CnC Domain in TLS SNI
- [x] ET MALWARE Observed AridViper CnC Domain in TLS SNI
- [x] ET MALWARE Observed AridViper CnC Domain in TLS SNI
- [x] ET MALWARE Observed AridViper CnC Domain in TLS SNI
- [x] ET MALWARE Foudre Checkin M2
- [x] ET MALWARE FormBook CnC Checkin (GET)
- [x] ET MALWARE Foudre Checkin M3
- [x] ET MALWARE Observed SystemBC CnC Domain in DNS Query
- [x] ET MALWARE Observed SystemBC CnC Domain in DNS Query
- [x] ET MALWARE Observed SystemBC CnC Domain in DNS Query
- [x] ET MALWARE Observed SystemBC CnC Domain in DNS Query
- [x] ET MALWARE Observed SystemBC CnC Domain in DNS Query
- [x] ET MALWARE PhantomNet/Smanager CnC Domain in DNS Lookup (vgca.homeunix .org)
- [x] ET MALWARE AHK.CREDSTEALER.A MalDoc Retrieving Payload
- [ ] ET MALWARE AHK.CREDSTEALER.A CnC Exfil
- [x] ET MALWARE Smanager CnC Domain in DNS Lookup
- [x] ET MALWARE Observed Malicious SSL Cert (PhantomNet/Smanager CnC)
- [x] ET MALWARE Worm.Win32.Balucaf.A Checkin
- [x] ET MALWARE Observed CobaltStrike/TEARDROP CnC Domain Domain in DNS Query
- [x] ET MALWARE FIN7/Carbanak CnC Domain in DNS Lookup (sephardimension .com)
- [x] ET MALWARE FIN7/Carbanak CnC Domain in DNS Lookup (dmnadmin .com)
- [x] ET MALWARE FIN7/Carbanak CnC Domain in DNS Lookup (myrric-uses .singlejets .com)
- [x] ET MALWARE Observed Cobalt Strike CnC Domain in TLS SNI (cs .lg22l .com)
- [x] ET MALWARE APT32/OceanLotus CnC Domain in DNS Lookup (mykessef .com)
- [x] ET MALWARE APT32/OceanLotus CnC Domain in DNS Lookup (idtpl .org)
- [x] ET MALWARE ElectroRAT CnC Checkin
- [x] ET MALWARE ElectroRAT Command from Server (Get folder content)
- [x] ET MALWARE Malicious XSL file download (FTP)
- [x] ET MALWARE IceRat Backdoor Checkin
- [x] ET MALWARE Win32/Injector.ULH CnC Activity
- [x] ET MALWARE Amadey Stealer CnC
- [x] ET MALWARE PlugX DNS Lookup
- [x] ET MALWARE Arbitrium-RAT CnC Activity
- [x] ET MALWARE Observed OSX/WizardUpdate Domain in TLS SNI (.dlvplayer .com)
- [x] ET MALWARE ELF/Freakout IRC Checkin
- [x] ET MALWARE [401TRG] Observed Backdoor.SUNBURST CnC Domain (infinitysoftwares .com in TLS SNI)
- [x] ET MALWARE [401TRG] SUNBURST Related DNS Lookup to bigtopweb .com
- [x] ET MALWARE [401TRG] Backdoor.BEACON SSL Cert Inbound (bigtopweb .com)
- [x] ET MALWARE Observed Malicious SSL Cert (BitRAT CnC)
- [x] ET MALWARE Observed Targeted Attack Malicious Domain in TLS SNI (codevexillium .org)
- [x] ET MALWARE Observed Targeted Attack Malicious Domain in TLS SNI (krakenfolio .com)
- [x] ET MALWARE Observed Targeted Attack Malicious Domain in TLS SNI (transferwiser .io)
- [x] ET MALWARE Dark Halo/SUNBURST CnC Domain (seobundlekit .com in TLS SNI)
- [x] ET MALWARE Dark Halo/SUNBURST CnC Domain (globalnetworkissues .com in TLS SNI)
- [x] ET MALWARE Observed AridViper CnC Domain in TLS SNI
- [x] ET MALWARE Observed AridViper CnC Domain in TLS SNI
- [x] ET MALWARE Observed AridViper CnC Domain in TLS SNI
- [x] ET MALWARE Observed AridViper CnC Domain in TLS SNI
- [x] ET MALWARE Observed AridViper CnC Domain in TLS SNI
- [x] ET MALWARE Foudre Checkin M1
- [x] ET MALWARE FormBook CnC Checkin (POST) M2
- [x] ET MALWARE Foudre Checkin M4
- [x] ET MALWARE Observed SystemBC CnC Domain in DNS Query
- [x] ET MALWARE Observed SystemBC CnC Domain in DNS Query
- [x] ET MALWARE Observed SystemBC CnC Domain in DNS Query
- [x] ET MALWARE Observed SystemBC CnC Domain in DNS Query
- [ ] ET MALWARE Observed SystemBC CnC Domain in DNS Query
- [x] ET MALWARE PhantomNet/Smanager CnC Domain in DNS Lookup (office365.blogdns .com)
- [x] ET MALWARE AHK.CREDSTEALER.A CnC Activity
- [x] ET MALWARE Possible MSIL/Solorigate.G!dha/SUPERNOVA Webshell Access Request
- [x] ET MALWARE Smanager CnC Domain in DNS Lookup
- [ ] ET MALWARE FormBook CnC Checkin (GET)
- [x] ET MALWARE Observed CobaltStrike/TEARDROP CnC Domain Domain in TLS SNI (mobilnweb .com)
- [ ] ET MALWARE FormBook CnC Checkin (GET)
- [x] ET MALWARE FIN7/Carbanak CnC Domain in DNS Lookup (besaintegration .com)
- [x] ET MALWARE FIN7/Carbanak CnC Domain in DNS Lookup (sendbits .m2stor4ge .xyz)
- [x] ET MALWARE NuggetPhantom Module Download Request
- [x] ET MALWARE MSIL/Azula Logger CnC Activity
- [x] ET MALWARE APT32/OceanLotus CnC Domain in DNS Lookup (mihannevis .com)
- [x] ET MALWARE Win32/Ymacco.AA1C Activity
- [x] ET MALWARE ElectroRAT Command from Server (Screenshot)
- [x] ET MALWARE Jupyter Stealer Reporting System Information M2
- [x] ET MALWARE Possible IceRat CnC Acitivty
- [x] ET MALWARE IceRat CnC Acitivty M2
- [x] ET MALWARE Observed Malicious SSL Cert (ElegyRAT)
- [x] ET MALWARE Known Sinkhole Response Kryptos Logic
- [x] ET MALWARE Observed Malicious SSL Cert (MassLogger)
- [x] ET MALWARE Arbitrium-RAT Observed User-Agent (JustKidding)
- [x] ET MALWARE OSX/WizardUpdate CnC Activity
- [x] ET MALWARE [401TRG] SUNBURST Related DNS Lookup to infinitysoftwares .com
- [x] ET MALWARE [401TRG] Backdoor.BEACON SSL Cert Inbound (infinitysoftwares .com)
- [x] ET MALWARE [401TRG] Observed Backdoor.SUNBURST CnC Domain (bigtopweb .com in TLS SNI)
- [x] ET MALWARE Trojan-Dropper.Win32.Sysn.cdjy CnC Activity
- [x] ET MALWARE Observed Targeted Attack Malicious SSL Cert (angeldonationblog .com)
- [x] ET MALWARE Observed Targeted Attack Malicious SSL Cert (investbooking .de)
- [x] ET MALWARE Observed Targeted Attack Malicious SSL Cert (opsonew3org .sg)
- [x] ET MALWARE Observed Targeted Attack Malicious Domain in TLS SNI (transplugin .io)

- [x] ET MALWARE Gh0st Variant CnC Domain in DNS Lookup (rninhsss .com)
- [x] ET MALWARE Observed Targeted Attack Malicious Domain in TLS SNI (blog .br0vvnn .io)
- [x] ET MALWARE Sn0wsLogger CnC Exfil M2
- [x] ET MALWARE TeamTNT Gattling Gun CnC Domain in DNS Lookup
- [x] ET MALWARE NIGHTSCOUT Poison Ivy Variant CnC Domain in DNS Lookup (cdn. cloudistcdn .com)
- [x] ET MALWARE NIGHTSCOUT Malware CnC Domain in DNS Lookup (q. cloudistcdn .com)
- [x] ET MALWARE Win32/SystemBC CnC Checkin
- [x] ET MALWARE Win32/TrickBot maserv Module CnC Activity
- [x] ET MALWARE Win32/TrojanDownloader.Small.AWO CnC Activity
- [x] ET MALWARE Observed Buer Loader Domain (officewestunionbank .com in TLS SNI)
- [x] ET MALWARE MSIL/CoderVir Stealer Zip Upload
- [x] ET MALWARE AppleJeus - JMT Trading CnC Activity (Windows Variant)
- [x] ET MALWARE AppleJeus - JMT Trading CnC Domain in DNS Lookup (jmttrading .org)
- [x] ET MALWARE AppleJeus - Union Crypto CnC Activity
- [x] ET MALWARE FIN7/Carbanak Staging Domain in DNS Lookup (civilizationidium .com)
- [x] ET MALWARE AppleJeus - Kupay Wallet CnC Domain in DNS Lookup (levelframeblog .com)
- [x] ET MALWARE AppleJeus - CoinGoTrade CnC Domain in DNS Lookup (coingotrade .com)
- [x] ET MALWARE OSX/NukeSped Variant CnC Domain in DNS Lookup (globalkeystroke .com)
- [x] ET MALWARE OSX/NukeSped Variant CnC Activity
- [x] ET MALWARE AppleJeus - Ants2Whale CnC Domain in DNS Lookup (ants2whale .com)
- [x] ET MALWARE Win32/LODEINFO v0.4.x CnC Checkin
- [x] ET MALWARE Observed OSX/Silver Sparrow Download Domain in TLS SNI
- [x] ET MALWARE WRAT Dropper (TLS SNI)
- [x] ET MALWARE VoidRay Downloader CnC Activity
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (perfectscenario .top)
- [x] ET MALWARE MINEBRIDGE CnC Domain in DNS Lookup (billionaireshore .top)
- [x] ET MALWARE MINEBRIDGE CnC Domain in DNS Lookup (realityarchitector .top)
- [x] ET MALWARE MINEBRIDGE CnC Domain in DNS Lookup (brainassault .top)
- [x] ET MALWARE MINEBRIDGE CnC Domain in DNS Lookup (unicornhub .top)
- [x] ET MALWARE MINEBRIDGE CnC Domain in DNS Lookup (bloggersglobbers .top)
- [x] ET MALWARE MINEBRIDGE CnC Activity
- [x] ET MALWARE Observed Malicious SSL Cert (DonotGroup CnC)
- [x] ET MALWARE Inception Group CnC Observed in DNS Query (ms-check-new-update .com)
- [x] ET MALWARE Inception/CloudAtlas CnC Domain in DNS Lookup (ms-officeupdate .com)
- [x] ET MALWARE Suspected APT32/OceanLotus Activity
- [x] ET MALWARE Ursnif Payload Request (cook64.rar)
- [x] ET MALWARE Ursnif Payload Request (grab64.rar)
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (teastycandycoffe .top)
- [x] ET MALWARE SUNSHUTTLE CnC Activity
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (nyqualitypizza .top)
- [x] ET MALWARE Gh0st Variant CnC Domain in DNS Lookup (dexercisep .com)
- [x] ET MALWARE Sn0wsLogger CnC Exfil M1
- [x] ET MALWARE TeamTNT Gattling Gun AWS Creds Exfil
- [x] ET MALWARE Observed Malicious SSL Cert (Magecart/Skimmer CnC)
- [x] ET MALWARE Win32/PivNoxy CnC Activity
- [x] ET MALWARE NIGHTSCOUT Malware CnC Domain in DNS Lookup (update .boshiamys .com)
- [x] ET MALWARE Win32/TrickBot maserv Module Command
- [x] ET MALWARE Snake Keylogger CnC Exfil via Telegram
- [x] ET MALWARE Win32/Detplock Checkin via SMTP
- [x] ET MALWARE Observed Malicious SSL Cert (DonotGroup CnC)
- [x] ET MALWARE JEUSD CnC Domain Observed in DNS Query
- [x] ET MALWARE AppleJeus - JMT Trading CnC Activity (OSX Variant)
- [x] ET MALWARE AppleJeus - Union Crypto CnC Domain in DNS Lookup (unioncrypto .vip)
- [x] ET MALWARE Suspected Fancy Bear (APT28) Maldoc CnC
- [x] ET MALWARE AppleJeus - Kupay Wallet CnC Domain in DNS Lookup (kupaywallet .com)
- [x] ET MALWARE AppleJeus - Kupay Wallet CnC Activity
- [x] ET MALWARE OSX/NukeSped Variant CnC Domain in DNS Lookup (airbseeker .com)
- [x] ET MALWARE OSX/NukeSped Variant CnC Domain in DNS Lookup (woodmate .it)
- [x] ET MALWARE AppleJeus - Dorusio CnC Domain in DNS Lookup (dorusio .com)
- [x] ET MALWARE AppleJeus - Ants2Whale CnC Domain in DNS Lookup (qnalytica .com)
- [x] ET MALWARE Observed OSX/Silver Sparrow Download Domain in TLS SNI
- [x] ET MALWARE SSL/TLS Certificate Observed (WRAT)
- [x] ET MALWARE MSIL/Spy.Keylogger.ENJ Variant CnC Activity
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (simsimsalabim .top)
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (mariofart8 .top)
- [x] ET MALWARE MINEBRIDGE CnC Domain in DNS Lookup (vikingsofnorth .top)
- [x] ET MALWARE MINEBRIDGE CnC Domain in DNS Lookup (gentlebouncer .top)
- [x] ET MALWARE MINEBRIDGE CnC Domain in DNS Lookup (greatersky .top)
- [x] ET MALWARE MINEBRIDGE CnC Domain in DNS Lookup (corporatelover .top)
- [x] ET MALWARE MINEBRIDGE CnC Activity
- [x] ET MALWARE MINEBRIDGE CnC Activity
- [x] ET MALWARE BazaBackdoor Variant CnC Activity M4
- [x] ET MALWARE Gameredon Loader Activity
- [x] ET MALWARE Inception/CloudAtlas CnC Domain in DNS Lookup (newmsoffice .com)
- [x] ET MALWARE Ursnif Payload Request (cook32.rar)
- [x] ET MALWARE Ursnif Payload Request (grab32.rar)
- [x] ET MALWARE W32/Echmark CnC Activity M2
- [x] ET MALWARE Cobalt Strike CnC Activity
- [x] ET MALWARE Cobalt Strike Beacon CnC
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (thereisnoscheme .top)
- [x] ET MALWARE Cobalt Strike Beacon (WooCommerce Profile)

- [x] ET MALWARE Win32/CopperStealer CnC Activity
- [x] ET MALWARE Win32/CopperStealer CnC Activity M3
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (thelegendofberia .top)
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (autopartslarry .top)
- [x] ET MALWARE ELF/RedXOR CnC Response
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (mansizeprofile .top)
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (gogowormdealer .top)
- [x] ET MALWARE Lazarus Maldoc CnC
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (return2monkey .fun)
- [x] ET MALWARE ShadowPad CnC Domain in DNS Lookup (ns .rtechs .org)
- [x] ET MALWARE Project Plague CnC Activity
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (youaresoslow .top)
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (followmeasap13 .top)
- [x] ET MALWARE Observed Malicious SSL Cert (CopperStealer CnC)
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (finalcountdown .top)
- [x] ET MALWARE W32/Trickbot C2 (networkDll module)
- [x] ET MALWARE Possible Ransomware HTTP POST to Onion Link Domain
- [x] ET MALWARE Netbounce Related Activity (Program Wrapper)
- [x] ET MALWARE Netbounce Proxy Activity
- [x] ET MALWARE Netbounce Program Wrapper Download
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (habbybearshop .top)
- [x] ET MALWARE Cobalt Strike Beacon Activity
- [x] ET MALWARE Observed Malicious SSL Cert (chMiner/RAT)
- [x] ET MALWARE Observed Malicious SSL Cert (Bazar Backdoor)
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (companyllc .top)
- [ ] ET MALWARE Suspected Jobcrypter Ransomware Exfil (SMTP)
- [x] ET MALWARE HiddenTears Ransomware Activity (GET)
- [x] ET MALWARE Konni Related Activity
- [x] ET MALWARE Black KingDom Ransomware Related Activity
- [x] ET MALWARE X-Files Stealer CnC Exfil Activity M1
- [x] ET MALWARE Cobalt Strike Beacon Activity (GET)
- [x] ET MALWARE Cobalt Strike Beacon Activity (GET)
- [x] ET MALWARE Cobalt Strike Beacon Activity (Wordpress Profile)
- [x] ET MALWARE Win32/Unk Downloader CnC Activity
- [x] ET MALWARE GCleaner Downloader Activity M1
- [x] ET MALWARE GCleaner Downloader Activity M3
- [x] ET MALWARE Cobalt Strike Beacon (Amazon Profile) M2
- [x] ET MALWARE Ousaban Related Maldoc Activity
- [x] ET MALWARE WebMonitor/RevCode RAT CnC Domain in DNS Lookup
- [x] ET MALWARE Win32/NitroStealer/exoStub CnC Exfil
- [x] ET MALWARE Win32/MereTam.A Ransomware CnC Init Activity
- [x] ET MALWARE DonotGroup Template Download
- [x] ET MALWARE Pult Downloader Activity
- [x] ET MALWARE Parallax CnC Response Activity M14
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (heroofthe .top)
- [x] ET MALWARE Win32/CopperStealer CnC Activity M2
- [x] ET MALWARE Win32/CopperStealer Installer Started
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (hitfromthebong .top)
- [x] ET MALWARE ELF/RedXOR CnC Checkin
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (mynameisgarfield .top)
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (letsmakesome .fun)
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (seattlecarwash .fun)
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (pleaseletmesleep .fun)
- [x] ET MALWARE PlugX/Korplug CnC Activity
- [x] ET MALWARE ShadowPad CnC Domain in DNS Lookup (soft .mssysinfo .xyz)
- [x] ET MALWARE Jasmin Ransomware C2 Checkin
- [x] ET MALWARE ELF/BASHLITE CnC Activity (Response)
- [x] ET MALWARE Win32/IcedID Request Cookie
- [x] ET MALWARE Observed Malicious SSL Cert (CopperStealer CnC)
- [x] ET MALWARE Win32/TrickBot Anchor Variant Style External IP Check
- [x] ET MALWARE Trickbot Checkin Response
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (mydrinksare .top)
- [x] ET MALWARE Netbounce User-Agent (Netbounce)
- [x] ET MALWARE Netbounce Proxy User-Agent (idk)
- [x] ET MALWARE Win32/MALWARECAT Exfil via SMTP
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (youcanfindmeonthe .top)
- [x] ET MALWARE Kimsuky Maldoc Activity
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (nameyourcatlikeshedeserved .top)
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (onthewire1 .top)
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (rpirpiwhyyouleaveyourhorse .top)
- [x] ET MALWARE Win32/Girostat Stealer (POST)
- [x] ET MALWARE MSIL/TrojanDownloader.Small.CLJ CnC Activity
- [x] ET MALWARE Cobalt Strike Activity
- [x] ET MALWARE Cobalt Strike Activity
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (videomart .top)
- [x] ET MALWARE Cobalt Strike Beacon Activity (GET)
- [x] ET MALWARE Cobalt Strike Beacon Activity (GET)
- [x] ET MALWARE Observed Malicious SSL Cert (Win32/Unk Downloader CnC)
- [ ] ET MALWARE Valyria Maldoc Activity (GET)
- [x] ET MALWARE GCleaner Downloader Activity M2
- [x] ET MALWARE Campo Loader Activity (GET)
- [x] ET MALWARE Cobalt Strike Beacon (Bing Profile)
- [x] ET MALWARE Cobalt Strike Beacon Activity
- [x] ET MALWARE Cobalt Strike Beacon Activity
- [x] ET MALWARE Nitro Stealer Exfil Activity (Response)
- [x] ET MALWARE Win32/MereTam.A Ransomware CnC Checkin
- [x] ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (lifemaindecision .top)
- [x] ET MALWARE Parallax CnC Activity (set) M14
- [x] ET MALWARE Observed Malicious SSL Cert (Python RAT (Aurora Campaign))
- [x] ET MALWARE TA402/Molerats Related VBS Retrieval

- ET MALWARE Observed StrongPity CnC Domain (hierarchicalfiles .com in TLS SNI)
- ET MALWARE Observed StrongPity CnC Domain (pulmonyarea .com in TLS SNI)
- ET MALWARE Win32.Raccoon Stealer CnC Domain in TLS SNI (shehootastayonwhatshelirned .top)
- ET MALWARE Observed StrongPity CnC Domain (uppertrainingtool .com in TLS SNI)
- ET MALWARE Ozone/Darktrack RAT Variant - Client Hello (set)
- ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (lomhasnopryiyome .top in TLS SNI)
- ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (tapewormorchestra .top in TLS SNI)
- ET MALWARE Cobalt Strike Malleable C2 (QiHoo Profile)
- ET MALWARE Cobalt Strike Malleable C2 Webbug Profile
- ET MALWARE Cobalt Strike Malleable C2 OCSP Profile
- ET MALWARE Cobalt Strike Malleable C2 (Microsoft Update GET)
- ET MALWARE Cobalt Strike Malleable C2 (TrevorForget Profile)
- ET MALWARE Cobalt Strike Malleable C2 (WooCommerce Profile)
- ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (whatsthescore .top in TLS SNI)
- ET MALWARE Magecart/Skimmer - AngryBeaver Exfil Attempt
- ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (youareperfect2day .top in TLS SNI)
- ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (attentionmagnet .top in TLS SNI)
- ET MALWARE Remcos 3.x Unencrypted Server Response
- ET MALWARE Remcos Builder License Check
- ET MALWARE Cobalt Strike Stager Time Check M2
- ET MALWARE Possibly SLIGHTPULSE Related - Suspicious POST to Specific URI Path
- ET MALWARE Observed Magecart/Skimmer - _try_action CnC Domain (cdn-frontend .com in TLS SNI)
- ET MALWARE HabitsRAT Checkin
- ET MALWARE Likely Evil Request for uac.exe With Minimal Headers
- ET MALWARE Observed DNS Query to Ursnif CnC Domain (horulenuke .us)
- ET MALWARE Possible STEADYPULSE Webshell Accessed M1
- ET MALWARE 44 Caliber Stealer Data Exfil via Discord
- ET MALWARE Win32/CollectorStealer CnC Exfil M2
- ET MALWARE MSIL/MosaiqueRAT CnC Checkin
- ET MALWARE APT-C-23 MICROPSIA Variant CnC Domain in DNS Lookup (mikkelbourke .pro)
- ET MALWARE APT-C-23 MICROPSIA Variant CnC Domain in DNS Lookup (overingtonray .info)
- ET MALWARE APT-C-23 MICROPSIA Variant CnC Domain in DNS Lookup (belcherjacky .info)
- ET MALWARE APT-C-23 MICROPSIA Variant CnC Domain in DNS Lookup (ansonwhitmore .live)
- ET MALWARE APT-C-23 MICROPSIA Variant CnC Domain in DNS Lookup (norayowell .info)
- ET MALWARE MICROPSIA Screenshot Upload M2
- ET MALWARE Cobalt Strike Beacon Activity (Wordpress Profile)
- ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (footballstar .top in TLS SNI)
- ET MALWARE PHP Skimmer CnC Domain in DNS Lookup (secure-authorize .net)
- ET MALWARE SharpNoPSExec EXE Lateral Movement Tool Downloaded
- ET MALWARE Observed Lunar Builder Domain (lunarbuilder .000webhostapp .com in TLS SNI)
- ET MALWARE Lunar Builder CnC Activity
- ET MALWARE Observed StrongPity CnC Domain (resolutionplatform .com in TLS SNI)
- ET MALWARE Observed StrongPity CnC Domain (hardwareoption .com in TLS SNI)
- ET MALWARE Observed StrongPity CnC Domain (applicationrepo .com in TLS SNI)
- ET MALWARE Observed StrongPity CnC Domain (hostoperationsystems .com in TLS SNI)
- ET MALWARE Ozone/Darktrack RAT Variant - Server Hello
- ET MALWARE OilRig SideTwist CnC Domain in DNS Lookup (sarmsoftware .com)
- ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (belochkaneprihoditodna .top in TLS SNI)
- ET MALWARE Cobalt Strike Malleable C2 (MSDN Query Profile)
- ET MALWARE Cobalt Strike Malleable C2 Amazon Profile
- ET MALWARE Cobalt Strike Malleable C2 (jquery Profile)
- ET MALWARE Saint Bot CnC Activity
- ET MALWARE Cobalt Strike Malleable C2 (Wordpress Profile)
- ET MALWARE Cobalt Strike Malleable C2 (WooCommerce Profile)
- ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (annafraudy .top in TLS SNI)
- ET MALWARE Kimsuky Maldoc Activity (GET)
- ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (mindbreaker .top in TLS SNI)
- ET MALWARE Remcos 3.x Unencrypted Checkin
- ET MALWARE Observed Win32/Wacapew.A!ml Domain in TLS SNI (zytrox .tk)
- ET MALWARE Cobalt Strike Stager Time Check M1
- ET MALWARE Suspected PULSECHECK Webshell Access Inbound
- ET MALWARE Magecart/Skimmer - _try_action Exfil Attempt
- ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (newageiscoming .top in TLS SNI)
- ET MALWARE Unk.PSAttack Activity
- ET MALWARE Observed DNS Query to Ursnif CnC Domain (vorulenuke. us)
- ET MALWARE Possible STEADYPULSE Webshell Accessed M2
- ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (gimmegimmejimmy .top in TLS SNI)
- ET MALWARE Lunar Builder Exfil via Discord M1
- ET MALWARE Observed DNS Query to MoserPass Download Domain (passwordstate-18ed2 .kxcdn .com)
- ET MALWARE APT-C-23 MICROPSIA Variant CnC Domain in DNS Lookup (linda-callaghan .icu)
- ET MALWARE APT-C-23 MICROPSIA Variant CnC Domain in DNS Lookup (scorerabbate .site)
- ET MALWARE APT-C-23 MICROPSIA Variant CnC Domain in DNS Lookup (marwapetersson .info)
- ET MALWARE APT-C-23 MICROPSIA Variant CnC Domain in DNS Lookup (gallant-william .icu)
- ET MALWARE APT-C-23 MICROPSIA Variant CnC Domain in DNS Lookup (irenewansley .icu)
- ET MALWARE MICROPSIA CnC Checkin M2
- ET MALWARE MICROPSIA Screenshot Upload M3
- ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (birdmilk .top in TLS SNI)
- ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (stockme .top in TLS SNI)
- ET MALWARE PHP Skimmer Exfil Attempt
- ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (blogsolutions .top in TLS SNI)
- ET MALWARE Lunar Builder Exfil Attempt
- ET MALWARE Win32/Koubbeh Sending Windows System Info

- [x] ET MALWARE SupremeLogger CnC Checkin
- [x] ET MALWARE Win32/TrojanDropper.Agent.RLO CnC Acitivty
- [x] ET MALWARE PurpleFox EK Landing Page Domain in SNI
- [x] ET MALWARE Malicious lnk Activity
- [ ] ET MALWARE Observed DNS Query to Buer - DomainInfo Domain
- [x] ET MALWARE ELF/DarkNexus User-Agent
- [ ] ET MALWARE [FIREEYE] SLIGHTPULSE Webshell Activity M1 (set) M1
- [x] ET MALWARE [FIREEYE] SLIGHTPULSE Webshell Activity M2 (set) M1
- [x] ET MALWARE [FIREEYE] SLIGHTPULSE Webshell Activity M2
- [ ] ET MALWARE [FIREEYE] SLIGHTPULSE Webshell Activity M1
- [x] ET MALWARE Pingback Shell Command Issued
- [x] ET MALWARE Pingback Upload Command Issued
- [x] ET MALWARE Kimsuky APT CnC Domain in DNS Lookup
- [x] ET MALWARE Kimsuky APT CnC Domain in DNS Lookup
- [x] ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (number1g .top in TLS SNI)
- [x] ET MALWARE Pingback OK Issued
- [ ] ET MALWARE Unk.CoinMiner Loader Checkin
- [x] ET MALWARE Observed DarkSide Ransomware Domain (temisleyes .com in TLS SNI)
- [ ] ET MALWARE Suspected SombRAT DNS Activity (TXT)
- [x] ET MALWARE Cobalt Strike Beacon Activity (UNC2447)
- [ ] ET MALWARE Ares Activity (POST)
- [x] ET MALWARE Suspected Ares Loader Activity (GET)
- [x] ET MALWARE Observed Malicious SSL Cert (Fake Gmail Self Signed - Possible Cobalt Stirke)
- [x] ET MALWARE Observed Cobalt Strike CnC Domain (security-desk .com in TLS SNI)
- [x] ET MALWARE Cobalt Strike Malleable C2 (Unknown Profile)
- [x] ET MALWARE Remote Desktop Spy Install Checkin
- [x] ET MALWARE Cobalt Strike Malleable C2 Profile (btn_bg)
- [x] ET MALWARE Cobalt Strike Malleable C2 Profile (bg)
- [x] ET MALWARE VenusLocker Activity
- [x] ET MALWARE Observed MageCart Group 12 Domain (pathc .space in TLS SNI)
- [x] ET MALWARE Cobalt Strike Malleable C2 Profile (Teams) M1
- [x] ET MALWARE Win32/RiskWare.YouXun.AD CnC Activity
- [x] ET MALWARE Observed Malicious SSL Cert (WastedLoader CnC)
- [x] ET MALWARE Observed DecryptmyFiles Ransomware User-Agent (uniquesession)
- [x] ET MALWARE Observed Malicious SSL Cert (Silver Implant)
- [x] ET MALWARE NightfallGT Discord Token Grabber
- [x] ET MALWARE Win32/SystemBC CnC Checkin (null key) M1
- [x] ET MALWARE Cobalt Strike Malleable C2 JQuery Custom Profile M3
- [x] ET MALWARE Suspected Kimsuky Activity (GET)
- [x] ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (genericalphabet .top in TLS SNI)
- [x] ET MALWARE Teslarvng Ransomware CnC Activity M2
- [x] ET MALWARE Lemon_Duck Powershell CnC Activity M14
- [ ] ET MALWARE Lemon_Duck Powershell CnC Activity M15
- [x] ET MALWARE OSX/MapperState CnC Domain in DNS Lookup
- [x] ET MALWARE Suspected Sidewinder Activity (GET)
- [x] ET MALWARE Observed Malicious SSL Cert (BazaLoader CnC)
- [x] ET MALWARE Observed Malicious Domain Targeting Minority Groups (officemodel .org in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain Targeting Minority Groups (tcahf .org in TLS SNI)
- [x] ET MALWARE TA471 Malicious AutoIT File Upload
- [x] ET MALWARE Win32/XRat.AT Variant CnC Activity
- [x] ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (realonlinetrend .top in TLS SNI)
- [x] ET MALWARE Buer - DomainInfo User-Agent
- [x] ET MALWARE Observed DarkSide Ransomware Domain (baroquetees .com in TLS SNI)
- [x] ET MALWARE [FIREEYE] PULSECHECK Webshell Access Outbound
- [ ] ET MALWARE [FIREEYE] SLIGHTPULSE Webshell Activity M1 (set) M2
- [x] ET MALWARE [FIREEYE] SLIGHTPULSE Webshell Activity M2 (set) M2
- [x] ET MALWARE [FIREEYE] SLIGHTPULSE Webshell Activity M3
- [x] ET MALWARE Suspected HARDPULSE Request
- [x] ET MALWARE Pingback Download Command Issued
- [x] ET MALWARE Pingback Exec Command Issued
- [x] ET MALWARE Kimsuky APT CnC Domain in DNS Lookup
- [x] ET MALWARE lolzilla JS/PHP WebSkimmer - Data Exfil
- [x] ET MALWARE Pingback Exep Command Issued
- [x] ET MALWARE Suspected Sliver DNS CnC
- [x] ET MALWARE Observed DarkSide Ransomware Domain (catsdegree .com in TLS SNI)
- [x] ET MALWARE Observed DarkSide Ransomware Domain (rumahsia .com in TLS SNI)
- [x] ET MALWARE Cobalt Strike Beacon Activity (UNC2447)
- [x] ET MALWARE Cobalt Strike Beacon Observed (MASB UA)
- [x] ET MALWARE Win32/Tnega Activity (GET)
- [x] ET MALWARE Observed Cobalt Strike User-Agent
- [x] ET MALWARE Cobalt Strike Malleable C2 (Unknown Profile)
- [x] ET MALWARE Cobalt Strike Malleable C2 (Unknown Profile)
- [x] ET MALWARE Observed DarkSide Ransomware CnC Domain in TLS SNI
- [x] ET MALWARE Observed Cobalt Strike CnC Domain (dimentos .com in TLS SNI)
- [x] ET MALWARE Cobalt Strike Malleable C2 Profile (__session__id Cookie)
- [x] ET MALWARE VenusLocker Associated User-Agent Activity
- [x] ET MALWARE Observed MageCart Group 12 Domain (zolo .pw in TLS SNI)
- [x] ET MALWARE Observed Win32/Ymacco.AA36 User-Agent
- [x] ET MALWARE Cobalt Strike Malleable C2 Profile (Teams) M2
- [x] ET MALWARE Observed Malicious SSL Cert (WastedLoader CnC)
- [x] ET MALWARE DecryptmyFiles Ransomware CnC (POST)
- [x] ET MALWARE Observed Silver Implant Domain (raspoly .biz in TLS SNI)
- [x] ET MALWARE Suspected Bizarro Banker Activity (POST)
- [x] ET MALWARE NightfallGT Discord Nitro Ransomware
- [x] ET MALWARE Win32/SystemBC CnC Checkin (null key) M2
- [x] ET MALWARE Cobalt Strike Malleable C2 JQuery Custom Profile Response
- [x] ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (number2g .top in TLS SNI)
- [x] ET MALWARE Teslarvng Ransomware CnC Activity M1
- [x] ET MALWARE Teslarvng Ransomware CnC Activity M3
- [x] ET MALWARE Lemon_Duck Powershell CnC Checkin M6
- [ ] ET MALWARE Suspected Gootkit Activity
- [x] ET MALWARE OSX/MapperState CnC Activity
- [ ] ET MALWARE BazaLoader CnC Activity
- [x] ET MALWARE Unknown Actor Targeting Minority Groups Activity (GET)
- [x] ET MALWARE Unknown Actor Targeting Minority Groups Activity (POST)
- [x] ET MALWARE Observed Malicious Domain Targeting Minority Groups Domain (unohcr .org in TLS SNI)

- [x] ET MALWARE Unknown Actor Targeting Minority Groups CnC Activity
- [x] ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup
- [x] ET MALWARE NOBELIUM (TA421) EnvyScout Fingerprint Checkin
- [x] ET MALWARE NOBELIUM Win32/VaporRage Loader CnC Checkin
- [x] ET MALWARE Observed CobaltStrike Loader Domain (cybersecyrity .com in TLS SNI)
- [x] ET MALWARE Cobalt Strike C2 Profile (news_indexedimages)
- [x] ET MALWARE Observed Magecart Skimmer Domain (googie-analitycs .site in TLS SNI)
- [x] ET MALWARE Observed Magecart Skimmer Domain (googie-analytics .website in TLS SNI)
- [x] ET MALWARE Evilnum Activity (GET)
- [x] ET MALWARE Observed JSSLoader Variant Domain (legislationient .com in TLS SNI)
- [x] ET MALWARE CNRarypt Ransomware CnC Activity
- [x] ET MALWARE APT34 Related DNS Tunneling Activity
- [x] ET MALWARE SharpPanda APT Maldoc Activity
- [x] ET MALWARE FatalRAT CnC Activity
- [x] ET MALWARE ALFA Shell APT33 DNS Lookup (solevisible .com)
- [x] ET MALWARE APT28/SkinnyBoy Payload Request
- [x] ET MALWARE MSIL/NoCry Ransomware Checkin Via Discord
- [x] ET MALWARE ETag HTTP Header Observed at JPCERT Sinkhole
- [x] ET MALWARE Known Sinkhole Response Header
- [x] ET MALWARE QuasarRAT/zgRAT C2 Activity (set)
- [ ] ET MALWARE ELF/Facefish Empty Payload (set)
- [ ] ET MALWARE ELF/Facefish Client Response (202)
- [x] ET MALWARE Kimsuky Maldoc Activity (GET)
- [x] ET MALWARE Observed DNS Query to Known Gelsemium CnC
- [x] ET MALWARE Observed DNS Query to Known Gelsemium CnC
- [x] ET MALWARE Possible Puzzlemaker Remote Shell Activity (GET)
- [x] ET MALWARE Generic njRAT/Bladabindi CnC Activity (ll)
- [x] ET MALWARE Observed FIN7 CnC Domain (injuryless .com in TLS SNI)
- [x] ET MALWARE Cobalt Strike Malleable C2 (WooCommerce Profile)
- [x] ET MALWARE Cobalt Strike Beacon Activity (Wordpress Profile)
- [x] ET MALWARE Cobalt Strike Beacon Activity (GET)
- [x] ET MALWARE Andariel Backdoor Actvity (Response)
- [x] ET MALWARE UNC2628 BEACON Activity (GET)
- [x] ET MALWARE Observed Malicious SSL Cert (Gelsemium CnC)
- [x] ET MALWARE Matanbuchus CnC Domain in DNS Lookup (eonsabode .at)
- [x] ET MALWARE Cobalt Strike Malleable C2 Profile wordpress_ Cookie Test
- [x] ET MALWARE Linux DarkRadiation Ransomware Activity (curl)
- [x] ET MALWARE Win32/Vidar Variant/Mars Stealer CnC Exfil
- [x] ET MALWARE DonotGroup Maldoc Activity (GET)
- [x] ET MALWARE ReverseRAT Activity (POST) M3
- [x] ET MALWARE AllaKore CnC Activity
- [x] ET MALWARE ReverseRAT Activity (POST) M2
- [x] ET MALWARE lu0bot CnC Domain in DNS Lookup
- [x] ET MALWARE lu0bot CnC Domain in DNS Lookup
- [x] ET MALWARE lu0bot Loader HTTP Response
- [ ] ET MALWARE ChaChi RAT Server Response
- [x] ET MALWARE GCleaner Related Downloader User-Agent
- [x] ET MALWARE Malware Delivery Landing Page via JS Redirect (2021-06-24)
- [x] ET MALWARE Observed Malware Delivery Landing Page Domain (bigeront .top in TLS SNI)
- [x] ET MALWARE Kimsuky Related Activity (init)
- [x] ET MALWARE Kimsuky Related Activity (ping)
- [x] ET MALWARE NightfallGT Mercurial Grabber
- [x] ET MALWARE Malicious Second Stage Payload Inbound 2021-02-19
- [x] ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup
- [x] ET MALWARE SharpPanda APT Downloader Activity (GET)
- [x] ET MALWARE Observed JSSLoader Domain (deprivationant .com in TLS SNI)
- [x] ET MALWARE Observed CobaltStrike CnC Domain (defendersecyrity .com in TLS SNI)
- [x] ET MALWARE Vidar Stealer - FaceIt Checkin Response
- [x] ET MALWARE Observed Magecart Skimmer Domain (googie-analytics .online in TLS SNI)
- [x] ET MALWARE Observed Magecart Skimmer Domain (googletagsmanager .website in TLS SNI)
- [x] ET MALWARE FIN7 JSSLoader Variant Activity (POST)
- [x] ET MALWARE FIN7 JSSLoader Variant Activity (GET)
- [x] ET MALWARE APT34 Related Activity (GET)
- [x] ET MALWARE Lyceum Group Activity (DNS)
- [x] ET MALWARE Win32/DCRat CnC Exfil
- [x] ET MALWARE sysrv.ELF Exploit Success Payload Request
- [x] ET MALWARE APT28/SkinnyBoy Checkin
- [x] ET MALWARE Observed Magecart Skimmer Domain (analiticsweb .site in TLS SNI)
- [x] ET MALWARE Win32/PlagueBot User-Agent
- [x] ET MALWARE ETag HTTP Header Observed at CNCERT Sinkhole
- [x] ET MALWARE Known Sinkhole Response Header
- [x] ET MALWARE zgRAT Activity
- [ ] ET MALWARE ELF/Facefish Server Response (201)
- [ ] ET MALWARE ELF/Facefish Session Closing (400)
- [x] ET MALWARE Observed DNS Query to Known Gelsemium CnC
- [x] ET MALWARE Observed DNS Query to Known Gelsemium CnC
- [x] ET MALWARE Observed Puzzlemaker Remote Shell Domain (media-seoengine .com in TLS SNI)
- [x] ET MALWARE DonotGroup Maldoc Activity (GET)
- [x] ET MALWARE Observed Lazarus Maldoc CnC Domain (shopweblive .com in TLS SNI)
- [ ] ET MALWARE Observed APT41 Malicious SSL Cert (ColunmTK Campaign)
- [x] ET MALWARE Cobalt Strike Beacon Activity (GET)
- [x] ET MALWARE TA456 GrumpyGrocer Related Domain in DNS Lookup (hotjar .info)
- [x] ET MALWARE Andariel Backdoor Activity (Checkin)
- [x] ET MALWARE Cobalt Strike Malleable C2 Profile (extension.css)
- [x] ET MALWARE UNC2628 Malicious MSHTA Activity (GET)
- [x] ET MALWARE APT Operation Sidecopy lnk Activity (GET)
- [x] ET MALWARE Observed Malicious SSL Cert (Klingon RAT)
- [x] ET MALWARE Linux DarkRadiation Ransomware Activity (wget)
- [x] ET MALWARE Linux DarkRadiation Ransomware Activity Attack Check
- [x] ET MALWARE a310Logger Stealer Exfil (SMTP)
- [x] ET MALWARE Maldoc Downloading from Dropbox via API
- [x] ET MALWARE ReverseRAT Activity (POST) M4
- [x] ET MALWARE ReverseRAT Activity (POST) M1
- [x] ET MALWARE lu0bot Loader HTTP Request
- [x] ET MALWARE lu0bot CnC Domain in DNS Lookup
- [x] ET MALWARE lu0bot CnC Domain in DNS Lookup
- [ ] ET MALWARE ChaChi RAT Client CnC (POST)
- [ ] ET MALWARE ChaChi RAT Client CnC (POST)
- [x] ET MALWARE Observed Malicious SSL Cert (TA456 GrumpyGrocer)
- [x] ET MALWARE Observed Malware Delivery Domain (analyticsnet .top in TLS SNI)
- [x] ET MALWARE Kimsuky Related Activity (GET)
- [x] ET MALWARE Kimsuky Related Activity (down)
- [x] ET MALWARE Kimsuky Related Activity (GET)
- [ ] ET MALWARE APT-C-23 Activity (GET)

- [x] ET MALWARE Kimsuky Related Activity (POST)
- [x] ET MALWARE Ransomware Decryptor Domain in DNS Query (decryptor .top)
- [x] ET MALWARE Ursnif Variant CnC Beacon - URI Struct M1 (_2B)
- [x] ET MALWARE REvil Exfil SFTP Certificate Inbound
- [x] ET MALWARE Andariel Backdoor Activity (Checkin)
- [x] ET MALWARE QuasarRAT/zgRAT C2 Activity (set)
- [x] ET MALWARE Observed MageCart Group 12 Domain (toolser .pw in TLS SNI)
- [x] ET MALWARE IndigoZebra APT BoxCaon DropBox Activity (POST)
- [x] ET MALWARE Diavol Communicating with CnC - Register M1
- [x] ET MALWARE Diavol Communicating with CnC - Key Request
- [x] ET MALWARE Diavol Communicating with CnC - Priority Request
- [x] ET MALWARE Diavol Communicating with CnC - Ext Request
- [x] ET MALWARE Diavol Communicating with CnC - Landing Request
- [x] ET MALWARE Observed DNS Query to Known Indexsinas CnC Domain
- [x] ET MALWARE Mirai pTea Variant - Initial CnC Checkin Outbound
- [x] ET MALWARE Mirai pTea Variant - Bot Upload Command Outbound
- [x] ET MALWARE Mirai pTea Variant - Info Submission Inbound
- [ ] ET MALWARE Mirai pTea Variant - Attack Command Inbound
- [x] ET MALWARE xCaon Embedded Encrypted Command in Webpage
- [x] ET MALWARE Kaseya VSA Exploit Activity M2 (SET)
- [x] ET MALWARE Possible Kaseya VSA Exploit Activity Inbound M2
- [x] ET MALWARE Maldoc Retrieving Payload 2021-07-06
- [x] ET MALWARE WaterDropX PRISM CnC Checkin
- [x] ET MALWARE Observed Malicious SSL Cert (CryptoMimic Staging CnC)
- [x] ET MALWARE BazaLoader Activity (GET)
- [x] ET MALWARE Malicious Dropper Activity (GET)
- [x] ET MALWARE Cobalt Strike Beacon Activity (GET)
- [x] ET MALWARE BIOPASS RAT Python Activity (GET)
- [x] ET MALWARE Observed Malicious SSL Cert (SideWinder APT CnC)
- [x] ET MALWARE Operation SpoofedScholars Activity (GET)
- [x] ET MALWARE Suspected Solarwinds Serv-U Backdoor (Incoming)
- [x] ET MALWARE Observed AZORult CnC Domain (miscrosoftworrd .000webhostapp .com in TLS SNI)
- [x] ET MALWARE Win32/Tofsee Connectivity Check M3
- [x] ET MALWARE Candiru Spyware CnC Domain in DNS Lookup (msstore .io)
- [x] ET MALWARE Candiru Spyware CnC Domain in DNS Lookup (cdnmobile .io)
- [x] ET MALWARE MargulasRAT Checkin M1
- [x] ET MALWARE MargulasRAT Keep-Alive Inbound M1
- [x] ET MALWARE MargulasRAT Keep-Alive Outbound M2
- [x] ET MALWARE Gasket CnC Checkin
- [x] ET MALWARE Gasket Submitting Logs to CnC
- [x] ET MALWARE Observed Elysium Stealer Variant CnC Domain (all-brain-company .xyz in TLS SNI)
- [x] ET MALWARE Win32/NitroStealer CnC Exfil M2
- [ ] ET MALWARE Suspected DonotGroup Dropper Telegram API Activity
- [x] ET MALWARE ELF/Miner Loader Activity M1 (GET)
- [x] ET MALWARE Observed Win32.Raccoon Stealer Domain (cheapfacechange .top in TLS SNI)
- [x] ET MALWARE Possible DarkRats Tor Traffic
- [x] ET MALWARE Observed BOUNCEBEAM Backdoor CnC Domain (cloudflare .5156game .com in TLS SNI)
- [x] ET MALWARE Observed CobaltStrike CnC Domain (krinsop .com in TLS SNI)
- [x] ET MALWARE Observed CobaltStrike CnC Domain (gmbfrom .com in TLS SNI)
- [x] ET MALWARE Observed Magecart Skimmer Domain (cloudflare-cdnjs .com in TLS SNI)
- [x] ET MALWARE W32/Echmark/MarkiRAT CnC Host Checkin
- [x] ET MALWARE W32/Echmark/MarkiRAT CnC Response
- [x] ET MALWARE APT-C-23 Activity (POST)
- [x] ET MALWARE Ransomware Decryptor Domain in DNS Query (decoder .re)
- [x] ET MALWARE Ursnif Variant CnC Beacon - URI Struct M2 (_2F)
- [x] ET MALWARE Valyria Downloader Activity
- [x] ET MALWARE Reborn Stealer 2021 Exfil attempt via Telegram
- [x] ET MALWARE zgRAT Activity M2
- [x] ET MALWARE IndigoZebra APT xCaon/Textpadx Activity (POST)
- [x] ET MALWARE Diavol CnC Checkin
- [x] ET MALWARE Diavol Communicating with CnC - Register M2
- [x] ET MALWARE Diavol Communicating with CnC - Services Request
- [x] ET MALWARE Diavol Communicating with CnC - Ignore Request
- [x] ET MALWARE Diavol Communicating with CnC - Wipe Request
- [x] ET MALWARE Diavol HTTP Cookie Observed
- [x] ET MALWARE Observed DNS Query to Known Indexsinas CnC Domain
- [x] ET MALWARE Mirai pTea Variant - Initial CnC Checkin Inbound
- [x] ET MALWARE Mirai pTea Variant - Info Submission Outbound
- [ ] ET MALWARE Mirai pTea Variant - Attack Command Outbound
- [x] ET MALWARE Mirai pTea Variant - Bot Upload Command Inbound
- [x] ET MALWARE Kaseya VSA Exploit Activity M1 (SET)
- [x] ET MALWARE Possible Kaseya VSA Exploit Activity Inbound M1
- [x] ET MALWARE Possible Kaseya VSA Exploit URI Structure Inbound
- [x] ET MALWARE Possible Siloscape IRC CnC JOIN Command Observed
- [x] ET MALWARE WaterDropX PRISM CnC Response
- [x] ET MALWARE Observed Malicious SSL Cert (CryptoMimic Staging CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (NHS UK Covid Passport Phish)
- [x] ET MALWARE Cobalt Strike Beacon Activity (GET)
- [x] ET MALWARE BIOPASS RAT Related Domain in DNS Lookup (0x3s .com)
- [x] ET MALWARE BIOPASS RAT Go Activity (GET)
- [x] ET MALWARE WildPressure/Milum CnC Activity
- [x] ET MALWARE Observed Malicious SSL Cert (Maldoc/Zloader CnC)
- [x] ET MALWARE Win32/Fareit Variant Activity (POST)
- [x] ET MALWARE Win32/Tofsee Connectivity Check M2
- [x] ET MALWARE ReverseRAT Activity (POST) M5
- [x] ET MALWARE Candiru Spyware CnC Domain in DNS Lookup (adtracker .link)
- [x] ET MALWARE Unk.DPRK MalDoc SysInfo CnC Exfil
- [x] ET MALWARE MargulasRAT Keep-Alive Outbound M1
- [x] ET MALWARE MargulasRAT Checkin M2
- [x] ET MALWARE MargulasRAT Keep-Alive Inbound M2
- [x] ET MALWARE Gasket Requesting Commands from CnC
- [x] ET MALWARE Mespinoza Ransomware - Pre-Encryption File Exfil to CnC
- [x] ET MALWARE DTLoader Binary Request M2
- [x] ET MALWARE Suspected DonotGroup Dropper Activity
- [x] ET MALWARE ELF/Miner Activity (GET)
- [x] ET MALWARE ELF/Miner Loader Activity M2 (GET)
- [x] ET MALWARE Cobalt Strike Beacon Activity (GET)
- [x] ET MALWARE BOUNCEBEAM Backdoor CnC Activity
- [x] ET MALWARE Observed Malicious SSL Cert (Bazar Backdoor)
- [x] ET MALWARE Observed CobaltStrike CnC Domain (charity-wallet .com in TLS SNI)
- [x] ET MALWARE KPOT Stealer Initial CnC Activity M5
- [x] ET MALWARE Observed Magecart Skimmer Domain (static-zdassets .com in TLS SNI)
- [x] ET MALWARE W32/Echmark/MarkiRAT CnC Request
- [x] ET MALWARE Dmechant Exfil Cryptowallets via SMTP

- [x] ET MALWARE Dmechant Exfil Passwords via SMTP
- [x] ET MALWARE Webshell Landing Outbound - Possibly Iran-based
- [x] ET MALWARE Webshell Access with Known Password Inbound - Possibly Iran-based
- [x] ET MALWARE Anchor_DNS stickseed Variant CnC Checkin
- [x] ET MALWARE Observed ZLoader CnC Domain in SNI
- [x] ET MALWARE W32/Echmark/MarkiRAT CnC Activity M3
- [x] ET MALWARE Gamaredon CnC Domain in DNS Lookup (lump .semara .ru)
- [x] ET MALWARE Gamaredon CnC Domain in DNS Lookup (aconitum .xyz)
- [x] ET MALWARE Gamaredon CnC Domain in DNS Lookup (hierodula .online)
- [x] ET MALWARE ClipBanker Variant Activity (POST)
- [x] ET MALWARE Lunar Builder Exfil Response
- [x] ET MALWARE Maldoc Activity Sending Windows User Info (GET)
- [x] ET MALWARE Maldoc Activity Sending Windows User Info (GET)
- [x] ET MALWARE Kimsuky Related Activity (GET)
- [x] ET MALWARE MSIL/Heracles Variant CnC Activity
- [x] ET MALWARE Kimsuky Related Activity (GET)
- [x] ET MALWARE Kimsuky Related Maldoc Activity (GET)
- [x] ET MALWARE Kimsuky Related Maldoc Activity (HEAD)
- [x] ET MALWARE Lemon_Duck CnC Domain in DNS Lookup
- [x] ET MALWARE Lemon_Duck CnC Domain in DNS Lookup
- [x] ET MALWARE Lemon_Duck CnC Domain in DNS Lookup
- [x] ET MALWARE Lemon_Duck CnC Domain in DNS Lookup
- [x] ET MALWARE Lemon_Duck CnC Domain in DNS Lookup
- [x] ET MALWARE Lemon_Duck CnC Domain in DNS Lookup
- [x] ET MALWARE Observed Malicious SSL Cert (FIN8 Staging CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (FIN8 CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (Meterpreter Paranoid Mode CnC)
- [x] ET MALWARE Observed Win32.Raccoon Stealer Domain (hellowoodie .top in TLS SNI)
- [x] ET MALWARE Win32/CandyOpen/UniClient Activity (GET)
- [x] ET MALWARE TA421/YTTRIUM/APT29 TLS Certificate M2
- [x] ET MALWARE BlackMatter CnC Domain in DNS Lookup (paymenthacks .com)
- [x] ET MALWARE BlackMatter CnC Activity
- [x] ET MALWARE Suspected Jupyter Stealer Related Activity (GET)
- [x] ET MALWARE Unknown Rootkit Download Activity (GET)
- [x] ET MALWARE W32/Quasar 1.3/Venom RAT Connectivity Check 3
- [x] ET MALWARE Observed SSV Agent CnC Domain (edgecloudc .com in TLS SNI)
- [x] ET MALWARE Observed SSV Agent CnC Domain (gitcloudcache .com in TLS SNI)
- [x] ET MALWARE Observed SSV Agent CnC Domain (drmtake .tk in TLS SNI)
- [x] ET MALWARE Observed SSV Agent CnC Domain (flushcdn .com in TLS SNI)
- [ ] ET MALWARE Win32/TrickBot CnC Initial Checkin M2
- [x] ET MALWARE Maldoc CnC Domain in DNS Lookup
- [x] ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (gopstoporchestra .top in TLS SNI)
- [x] ET MALWARE Cobalt Strike Beacon Activity (GET)
- [x] ET MALWARE Quasar CnC Domain in DNS Lookup (societyf500 .ddns .net)
- [x] ET MALWARE Observed SSL/TLS Cert (Splashtop Remote Support)
- [x] ET MALWARE Cobalt Strike Infrastructure CnC Domain in DNS Lookup
- [x] ET MALWARE Cobalt Strike Infrastructure CnC Domain in DNS Lookup
- [x] ET MALWARE RustyBuer CnC Domain in SNI
- [x] ET MALWARE Webshell Upload Command Inbound - Possibly Iran-based
- [x] ET MALWARE Webshell Execute Command Inbound - Possibly Iran-based M1
- [x] ET MALWARE Observed Malsmoke Staging Domain in SNI
- [x] ET MALWARE Observed ZLoader CnC Domain in SNI
- [x] ET MALWARE Gamaredon CnC Domain in DNS Lookup (clank .hazari .ru)
- [x] ET MALWARE Gamaredon CnC Domain in DNS Lookup (lovers .semara .ru)
- [x] ET MALWARE Gamaredon CnC Domain in DNS Lookup (blattodea .ru)
- [x] ET MALWARE Gamaredon CnC Domain in DNS Lookup (tomond .ru)
- [x] ET MALWARE Lunar Builder Exfil via Discord M2
- [x] ET MALWARE Lazarus APT Related CnC Domain in DNS Lookup (page .googledocpage .com)
- [x] ET MALWARE 44Calibar Variant Exfil via Telegram
- [x] ET MALWARE Observed CobaltStrike CnC Domain (stg .pesrado .com in TLS SNI)
- [x] ET MALWARE Kimsuky Related Activity (GET)
- [x] ET MALWARE Observed MSIL/Heracles Variant CnC Domain (stainless .fun in TLS SNI)
- [x] ET MALWARE Kimsuky Related Maldoc Activity (POST)
- [x] ET MALWARE Kimsuky Related Script Activity (GET)
- [x] ET MALWARE Observed DCRat CnC Domain (dud-shotline .000webhostapp .com in TLS SNI)
- [x] ET MALWARE Lemon_Duck CnC Domain in DNS Lookup
- [x] ET MALWARE Lemon_Duck CnC Domain in DNS Lookup
- [x] ET MALWARE Lemon_Duck CnC Domain in DNS Lookup
- [x] ET MALWARE Lemon_Duck CnC Domain in DNS Lookup
- [x] ET MALWARE Lemon_Duck CnC Domain in DNS Lookup
- [x] ET MALWARE Lemon_Duck CnC Domain in DNS Lookup
- [x] ET MALWARE Observed Malicious SSL Cert (FIN8 CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (FIN8 CnC)
- [x] ET MALWARE Gamaredon Maldoc Activity (GET)
- [x] ET MALWARE Win32/CandyOpen/UniClient Activity (POST)
- [x] ET MALWARE TA421/YTTRIUM/APT29 TLS Certificate M1
- [x] ET MALWARE TA421/YTTRIUM/APT29 TLS Certificate M3
- [x] ET MALWARE BlackMatter CnC Domain in DNS Lookup (mojobiden .com)
- [x] ET MALWARE Observed Cobalt Strike CnC Domain (www .msfthelpdesk .com in TLS SNI)
- [x] ET MALWARE Jupyter Stealer Reporting System Information M2
- [x] ET MALWARE Unknown Rootkit Checkin Activity (getSystemInfo)
- [x] ET MALWARE SSV Agent CnC Activity
- [x] ET MALWARE Observed SSV Agent CnC Domain (be-government .com in TLS SNI)
- [x] ET MALWARE Observed SSV Agent CnC Domain (hostupoeui .com in TLS SNI)
- [x] ET MALWARE Observed SSV Agent CnC Domain (rsnet-devel .com in TLS SNI)
- [x] ET MALWARE Cobalt Strike Malleable C2 JQuery Custom Profile M2
- [x] ET MALWARE TrickBot Related Activity (GET)
- [x] ET MALWARE Observed Maldoc CnC Domain (cloud-documents .com in TLS SNI)
- [x] ET MALWARE Observed Cobalt Strike CnC Domain (onlineworkercz .com in TLS SNI)
- [x] ET MALWARE Thallium CnC Domain in DNS Lookup
- [x] ET MALWARE SideCopy Group Activity (GET)
- [x] ET MALWARE Cobalt Strike Infrastructure CnC Domain in DNS Lookup
- [x] ET MALWARE Cobalt Strike Infrastructure CnC Domain in DNS Lookup
- [x] ET MALWARE Cobalt Strike Infrastructure CnC Domain in DNS Lookup

- [x] ET MALWARE Cobalt Strike Infrastructure CnC Domain in DNS Lookup
- [x] ET MALWARE Observed Cobalt Strike CnC Domain (gojihu .com in TLS SNI)
- [x] ET MALWARE Observed Malicious SSL Cert (Ursnif Injects)
- [x] ET MALWARE IIStealer CnC Domain in DNS Lookup (xinxx .allsoulu .com)
- [x] ET MALWARE IIStealer Inbound Exfil Request M2
- [x] ET MALWARE Win32/DownloadAdmin Activity
- [x] ET MALWARE Cobalt Strike Beacon Observed
- [x] ET MALWARE MSIL/Black Hat Worm Server Response
- [x] ET MALWARE GoBrut/StealthWorker Requesting Brute Force List (flowbit set)
- [x] ET MALWARE GoBrut/StealthWorker Service Bruter CnC Checkin
- [x] ET MALWARE Unknown Chinese Threat Actor CnC Domain in DNS Lookup
- [x] ET MALWARE Gamaredon Maldoc Activity (GET)
- [x] ET MALWARE APT-C-48 Related Activity Retrieving ConsoleHost (GET)
- [x] ET MALWARE Stealbit Variant Data Exfil M1
- [x] ET MALWARE PCRat/Gh0st CnC Beacon Request (Xfire variant)
- [x] ET MALWARE DarkWay Client Checkin
- [x] ET MALWARE Win32/BLUELIGHT OAuth Login Attempt
- [x] ET MALWARE MSIL/Agent.DNL CnC Activity M1
- [x] ET MALWARE Win32/Malgent!MSR Dropper Requesting Payload
- [x] ET MALWARE SiameseKitten/Lyceum/Hexane MSIL/Shark CnC Checkin
- [x] ET MALWARE Cinobi Banking Trojan Domain in DNS Lookup (www .magicalgirlonlive .com)
- [x] ET MALWARE Cinobi Banking Trojan Domain in DNS Lookup (www .supapureigemu .com)
- [x] ET MALWARE Win32/Kryptik.HMCH Dropper User-Agent M1
- [x] ET MALWARE Win32/Kryptik.HMCH Dropper User-Agent M3
- [x] ET MALWARE Observed Karen Ransomware CnC Checkin
- [x] ET MALWARE Observed Karen Ransomware Domain (karen .h07 .wlh .io in TLS SNI)
- [x] ET MALWARE NSO Group Pegasus Related Data Exfil (POST) M2
- [x] ET MALWARE Win32/a310Logger Clipboard Exfil via SMTP
- [x] ET MALWARE SparklingGoblin/Winnti Group SideWalk Domain in DNS Lookup
- [x] ET MALWARE FerociousKitten CnC Domain in DNS Lookup (microsoft .microcaft .xyz)
- [x] ET MALWARE Konni RAT Exfiltrating Data
- [x] ET MALWARE Win32/Sinresby.B Downloader CnC Activity M2
- [x] ET MALWARE GCleaner Downloader Activity M4
- [x] ET MALWARE Observed Cobalt Strike CnC Domain (windowsupdatesc .com in TLS SNI)
- [x] ET MALWARE Observed Cobalt Strike CnC Domain (defenderupdateav .com in TLS SNI)
- [x] ET MALWARE SNIcat - Detected C2 Commands (LS)
- [x] ET MALWARE SNIcat - Detected C2 Commands (LD)
- [x] ET MALWARE SNIcat - Detected C2 Commands (CD)
- [x] ET MALWARE SNIcat - Detected C2 Commands (ALIVE)
- [x] ET MALWARE SNIcat - Detected C2 Commands (finito)
- [x] ET MALWARE FIN8 SARDONIC CnC Domain in DNS Lookup (api-cdn .net)
- [x] ET MALWARE FIN8 SARDONIC CnC Domain in DNS Lookup (api-cdnw5 .net)
- [x] ET MALWARE Javascript Displays malicious download page
- [x] ET MALWARE Suspected Cobalt Strike Beacon Activity (DNS)
- [x] ET MALWARE Win32/GenCBL.XS CnC Activity
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [x] ET MALWARE Observed Cobalt Strike CnC Domain (yuxicu .com in TLS SNI)
- [x] ET MALWARE Suspected TeamTNT Linux Miner Activity
- [x] ET MALWARE Suspected Malicious VBS Script Activity
- [x] ET MALWARE IIStealer Inbound Exfil Request
- [x] ET MALWARE Unknown DPRK Threat Actor Activity (GET)
- [x] ET MALWARE Suspected Praying Mantis Threat Actor Activity
- [x] ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (msresearchcenter .top in TLS SNI)
- [x] ET MALWARE MSIL/Black Hat Worm Checkin
- [x] ET MALWARE GoBrut/StealthWorker Service Bruter CnC Activity
- [ ] ET MALWARE Unknown Chinese Threat Actor Malicious Redirect Activity
- [x] ET MALWARE Gamaredon CnC Domain in DNS Lookup (office360-expert .online)
- [x] ET MALWARE APT-C-48 Related CnC Domain in DNS Lookup (ntc-pk .sytes .net)
- [x] ET MALWARE APT-C-48 Related CnC Domain in DNS Lookup (nitb .pk-gov .org)
- [x] ET MALWARE Stealbit Variant Data Exfil M2
- [x] ET MALWARE Win32/PSW.Agent.OMP Variant CnC Activity
- [x] ET MALWARE Observed BLUELIGHT Payload Domain (storage .jquery .services in TLS SNI)
- [x] ET MALWARE Win32/BLUELIGHT OAuth Login Attempt M2
- [x] ET MALWARE MSIL/Agent.DNL Server Response Task (whoami)
- [x] ET MALWARE Win32/Malgent!MSR User-Agent
- [x] ET MALWARE SiameseKitten/Lyceum/Hexane MSIL/Shark Uploading to CnC
- [x] ET MALWARE Cinobi Banking Trojan Domain in DNS Lookup (www .getkiplayer .com)
- [x] ET MALWARE Cinobi Banking Trojan Domain in DNS Lookup (www .chirigame .com)
- [x] ET MALWARE Win32/Kryptik.HMCH Dropper User-Agent M2
- [x] ET MALWARE Win32/Kryptik.HMCH Dropper User-Agent M4
- [x] ET MALWARE Observed Karen Ransomware Powershell Loader
- [x] ET MALWARE NSO Group Pegasus Related Data Exfil (POST)
- [x] ET MALWARE NSO Group Pegasus Related Data Exfil (POST) M3
- [x] ET MALWARE Win32/a310Logger Data Exfil via SMTP
- [x] ET MALWARE SparklingGoblin/Winnti Group SideWalk Domain in DNS Lookup
- [x] ET MALWARE FerociousKitten CnC Domain in DNS Lookup (microsoft .com-view .space)
- [x] ET MALWARE Win32/Sinresby.B Downloader CnC Activity M1
- [x] ET MALWARE Konni RAT Querying CnC for Commands
- [ ] ET MALWARE Cobalt Strike Malleable C2 (Custom Profile)
- [x] ET MALWARE Observed Cobalt Strike CnC Domain (securityupdateav .com in TLS SNI)
- [x] ET MALWARE SNIcat - Detected C2 Commands (LIST)
- [x] ET MALWARE SNIcat - Detected C2 Commands (SIZE)
- [x] ET MALWARE SNIcat - Detected C2 Commands (CB)
- [x] ET MALWARE SNIcat - Detected C2 Commands (EX)
- [x] ET MALWARE SNIcat - Detected C2 Commands (EXIT)
- [ ] ET MALWARE Cobalt Strike Beacon (Custom Wordpress Profile)
- [x] ET MALWARE FIN8 SARDONIC CnC Domain in DNS Lookup (git-api .com)
- [x] ET MALWARE W32/Witch.3FA0!tr CnC Actiivty
- [ ] ET MALWARE Javascript Click and Removal of Download Element
- [x] ET MALWARE MSIL/Document Stealer Exfil
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [x] ET MALWARE HCRootkit CnC Domain in DNS Lookup (ywbgrcrupasdiqxknwgceatlnbvmezti .com)

- [x] ET MALWARE HCRootkit CnC Domain in DNS Lookup (yhgrffndvzbtoilmundkmvbaxrjtqsew .com)
- [x] ET MALWARE HCRootkit CnC Domain in DNS Lookup (ruciplbrxwjscyhtapvlfskoqqgnxevw .name)
- [x] ET MALWARE HCRootkit CnC Domain in DNS Lookup (nfcomizsdseqiomzqrxwvtprxbljkpgd .name)
- [x] ET MALWARE HCRootkit CnC Domain in DNS Lookup (etzndtcvqvyxajpcgwkzsoweaubilflh .com)
- [x] ET MALWARE Win32/44Caliber Stealer Variant Activity (POST)
- [x] ET MALWARE Observed Pegasus Domain (api1r3f4 .redirectweburl .com in TLS SNI)
- [x] ET MALWARE Observed DNS Query to Pegasus Domain (news-now .co)
- [x] ET MALWARE Observed DNS Query to Pegasus Domain (helpusfind .biz)
- [x] ET MALWARE Magecart CnC Domain in DNS Lookup
- [x] ET MALWARE Magecart CnC Domain in DNS Lookup
- [x] ET MALWARE Magecart CnC Domain in DNS Lookup
- [x] ET MALWARE Magecart CnC Domain in DNS Lookup
- [x] ET MALWARE Magecart CnC Domain in DNS Lookup
- [x] ET MALWARE Magecart CnC Domain in DNS Lookup
- [x] ET MALWARE Magecart CnC Domain in DNS Lookup
- [x] ET MALWARE FIN7 JSSLoader Variant Activity (GET)
- [x] ET MALWARE Win32/Enemyfear Stealer Exfil
- [x] ET MALWARE FIN7 Related CnC Domain in DNS Lookup (bypassociation .com)
- [x] ET MALWARE BleachGap Ransomware Checkin (POST)
- [x] ET MALWARE Win32/Syndicasec Encoded Response Embedded in XML HTML Title Tags Inbound
- [x] ET MALWARE Win32/Unk.Coinminer Checkin
- [x] ET MALWARE W32/Bingoml!tr CnC Activity
- [x] ET MALWARE Maldoc Checkin Activity (GET)
- [x] ET MALWARE Win32/PSW.WOW.NLZ CnC Activity
- [x] ET MALWARE Observed ELF/HabitsRAT CnC Domain in TLS SNI
- [x] ET MALWARE Observed ELF/HabitsRAT CnC Domain in TLS SNI
- [x] ET MALWARE MSIL/Small.FU Variant CnC Activity M1
- [x] ET MALWARE MSIL/Small.FU Variant CnC Activity M3
- [x] ET MALWARE Cobalt Strike Beacon Activity (GET)
- [x] ET MALWARE Win32/Vermilion Stager Activity (GET)
- [x] ET MALWARE MSIL/Black Hat Worm Server Response
- [ ] ET MALWARE Sidewalk CnC Checkin
- [x] ET MALWARE SQUIRRELWAFFLE Loader Activity (POST)
- [x] ET MALWARE Win32/Delf.OKR Variant CnC M1
- [x] ET MALWARE Observed Malicious SSL Cert (CobaltStrike CnC)
- [x] ET MALWARE Fake Software Download Redirect Leading to Malware M2
- [x] ET MALWARE TransparentTribe Related CnC Activity
- [x] ET MALWARE Win32/Bisonal Backdoor CnC Activity (POST)
- [x] ET MALWARE Observed Elysium Stealer Domain (phonefix .bar in TLS SNI)
- [x] ET MALWARE Win32.Raccoon Stealer Data Exfil Attempt
- [x] ET MALWARE SQUIRRELWAFFLE Server Response
- [x] ET MALWARE Possible SQUIRRELWAFFLE Server Response
- [ ] ET MALWARE APT/Bitter Maldoc Activity
- [x] ET MALWARE NSIS/TrojanDownloader.Agent.NZK CnC Activity M1
- [x] ET MALWARE NSIS/TrojanDownloader.Agent.NZK Server Response
- [x] ET MALWARE GCleaner Downloader Activity M5
- [x] ET MALWARE MSIL/Monitor.PCTattletale.A Checkin (POST)
- [x] ET MALWARE APT/FamousSparrow CnC Domain in DNS Lookup (credits.offices-analytics .com)
- [ ] ET MALWARE JS/Spy.Agent.AW Download
- [x] ET MALWARE MirrorBlast CnC Activity M3
- [x] ET MALWARE HCRootkit CnC Domain in DNS Lookup (wcmbqxzeuopnvyfmhkstaretfciywdrl .name)
- [x] ET MALWARE HCRootkit CnC Domain in DNS Lookup (pdjwebrfgdyzljmwtxcoyomapxtzchvn .com)
- [x] ET MALWARE HCRootkit CnC Domain in DNS Lookup (hkxpqdtgsucylodaejmzmtnkpfvojabe .com)
- [x] ET MALWARE HCRootkit CnC Domain in DNS Lookup (esnoptdkkiirzewlpgmccbwuynvxjumf .name)
- [x] ET MALWARE Observed Pegasus Domain (hooklevel .com in TLS SNI)
- [x] ET MALWARE Observed DNS Query to Pegasus Domain (start-anew .net)
- [x] ET MALWARE Observed DNS Query to Pegasus Domain (reunionlove .net)
- [x] ET MALWARE Magecart CnC Domain in DNS Lookup
- [x] ET MALWARE Magecart CnC Domain in DNS Lookup
- [x] ET MALWARE Magecart CnC Domain in DNS Lookup
- [x] ET MALWARE Magecart CnC Domain in DNS Lookup
- [x] ET MALWARE Magecart CnC Domain in DNS Lookup
- [x] ET MALWARE Magecart CnC Domain in DNS Lookup
- [x] ET MALWARE Magecart CnC Domain in DNS Lookup
- [x] ET MALWARE Magecart CnC Domain in DNS Lookup
- [x] ET MALWARE BlackMatter CnC Domain in DNS Lookup (nowautomation .com)
- [x] ET MALWARE FIN7 Related CnC Domain in DNS Lookup (tnskvggujjqfcskwk .com)
- [x] ET MALWARE Go/Hack Browser Data Exfil Attempt
- [x] ET MALWARE Observed Lazarus Related Domain (share .bloomcloud .org in TLS SNI)
- [x] ET MALWARE Win32/Syndicasec Encoded Response Embedded in HTML Title Tags Inbound
- [ ] ET MALWARE Maldoc OneDrive Download Activity (GET)
- [ ] ET MALWARE Win32/Mingloa CnC Checkin
- [x] ET MALWARE Maldoc Checkin Activity (GET)
- [x] ET MALWARE Observed ELF/HabitsRAT CnC Domain in TLS SNI
- [x] ET MALWARE Observed ELF/HabitsRAT CnC Domain in TLS SNI
- [x] ET MALWARE Observed ELF/HabitsRAT CnC Domain in TLS SNI
- [x] ET MALWARE MSIL/Small.FU Variant CnC Activity M2
- [x] ET MALWARE Cobalt Strike Beacon Activity (GET)
- [x] ET MALWARE Cobalt Strike Beacon Activity (GET)
- [x] ET MALWARE Win32/Vermilion Stager Activity (GET)
- [x] ET MALWARE Win32/GenKryptik.FKJZ CnC Exfil
- [x] ET MALWARE Bladabindi/njrat CnC Checkin
- [x] ET MALWARE Cobalt Strike Beacon Activity (GET)
- [x] ET MALWARE Win32/Delf.OKR Variant CnC M2
- [x] ET MALWARE Fake Software Download Redirect Leading to Malware M1
- [x] ET MALWARE Fake Software Download Redirect Leading to Malware M3
- [x] ET MALWARE Win32/Bisonal Backdoor CnC Domain in DNS Lookup
- [x] ET MALWARE OSX/ZuRu Activity (POST)
- [x] ET MALWARE Win32.Raccoon Stealer CnC Activity (dependency download)
- [ ] ET MALWARE Gamaredon Maldoc Activity (GET)
- [x] ET MALWARE Win32/Numando Banker CnC Activity
- [x] ET MALWARE APT/Bitter Related CnC Domain in DNS Lookup
- [x] ET MALWARE Observed Malicious SSL Cert (CobaltStrike CnC)
- [x] ET MALWARE NSIS/TrojanDownloader.Agent.NZK CnC Activity M2
- [x] ET MALWARE Observed Malicious SSL Cert (Cobalt Strike)
- [x] ET MALWARE MirrorBlast Checkin
- [x] ET MALWARE APT/FamousSparrow Activity (POST)
- [x] ET MALWARE TinyTurla CnC Activity
- [x] ET MALWARE MirrorBlast CnC Activity M2
- [x] ET MALWARE Jupyter Stealer CnC Checkin

- [x] ET MALWARE Maldoc CnC Domain in DNS Lookup (r .significantbyte .com)
- [x] ET MALWARE Maldoc Sending Windows System Information (POST)
- [x] ET MALWARE FoggyWeb Backdoor Incoming Request (GET)
- [x] ET MALWARE Possible FoggyWeb Backdoor Server Response
- [ ] ET MALWARE Win32/Voltron/Spectre Stealer Download Activity (GET)
- [x] ET MALWARE Win32/Voltron/Spectre Stealer CnC Activity (POST)
- [ ] ET MALWARE Win64/TrojanDownloader.Age Download Activity (GET)
- [x] ET MALWARE Win32/AZORult V3.2 Client Checkin M22
- [x] ET MALWARE Win32/AZORult V3.2 Client Checkin M24
- [x] ET MALWARE Win32/AZORult V3.3 Client Checkin M23
- [x] ET MALWARE Megalodon/Gomorrah/CosaNostra HTTP Bot CnC Exfil
- [x] ET MALWARE TAG28 Associated CnC Domain in DNS Lookup (samuelblog .me)
- [x] ET MALWARE TAG28 Associated CnC Domain in DNS Lookup (samuelblog .info)
- [x] ET MALWARE TAG28 Associated CnC Domain in DNS Lookup (samuelblog .xyz)
- [x] ET MALWARE S400 RAT Server Response
- [x] ET MALWARE ChamelGang Related CnC Domain in DNS Lookup (newtrendmicro .com)
- [x] ET MALWARE ChamelGang Related CnC Domain in DNS Lookup (microsoft-support .net)
- [x] ET MALWARE ChamelGang Related CnC Domain in DNS Lookup (mcafee-upgrade .com)
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [x] ET MALWARE Cobalt Strike Malleable C2 Amazon Profile POST (JPEG)
- [x] ET MALWARE Cobalt Strike Malleable C2 Amazon Profile POST (RIFF)
- [ ] ET MALWARE ELF/MachO.Netwire Connectivity Check
- [x] ET MALWARE MirrorBlast KiXtart Downloader Client Request
- [ ] ET MALWARE Observed Cobalt Strike CnC Domain (sazoya .com in TLS SNI)
- [x] ET MALWARE Wintervivern Related CnC Domain in DNS Lookup (secure-daddy .com)
- [x] ET MALWARE Wintervivern Related CnC Domain in DNS Lookup (securemanag .com)
- [x] ET MALWARE Wintervivern Activity M2 (GET)
- [x] ET MALWARE Wintervivern Checkin
- [x] ET MALWARE MirrorBlast KiXtart Downloader Server Response
- [ ] ET MALWARE Observed HTTP Request to Known PUA Host Domain
- [x] ET MALWARE Winter Vivern Retrieving Commands
- [x] ET MALWARE Wintervivern Activity M5 (GET)
- [x] ET MALWARE Observed Elysium Stealer Domain in TLS SNI (get-europe-group .bar)
- [x] ET MALWARE Observed Elysium Stealer Domain in TLS SNI (manholi .xyz)
- [x] ET MALWARE Lazarus APT Related CnC Domain in DNS Lookup (sharemanage .elwoodasset .xyz)
- [x] ET MALWARE Lazarus APT Related CnC Domain in DNS Lookup (dev .sslsharecloud .net)
- [x] ET MALWARE Lazarus APT Related CnC Domain in DNS Lookup (gsheet .gdocsdown .com)
- [x] ET MALWARE Lazarus APT Related CnC Domain in DNS Lookup (share .devprocloud .com)
- [x] ET MALWARE Lazarus APT Related CnC Domain in DNS Lookup (www .googlesheetpage .org)
- [ ] ET MALWARE Observed Ursnif CnC Domain (Vloderuniok .website in TLS SNI)
- [ ] ET MALWARE Observed Cobalt Strike CnC Domain (Yuxicu .com in TLS SNI)
- [x] ET MALWARE DonotGroup APT DNS Lookup (bulk .fun)
- [x] ET MALWARE DonotGroup Related Domain in DNS Lookup (ppadoaolnwod .xyz)
- [ ] ET MALWARE Gamaredon Maldoc Remote Template Retrieval (GET)
- [x] ET MALWARE Maldoc Domain in DNS Lookup (aljazeera .cc)
- [x] ET MALWARE Win32/Sabsik.FL.B!ml CnC Activity
- [x] ET MALWARE FoggyWeb Backdoor Incoming Request (POST)
- [x] ET MALWARE Win32/Voltron/Spectre Stealer Checkin Activity (GET)
- [x] ET MALWARE Win32/Voltron/Spectre Stealer Sending OS Information (POST)
- [x] ET MALWARE ReflectiveGnome Download Activity
- [x] ET MALWARE Win32/Colibri Loader Activity
- [x] ET MALWARE Win32/AZORult V3.2 Client Checkin M23
- [x] ET MALWARE Win32/AZORult V3.3 Client Checkin M22
- [x] ET MALWARE Win32/AZORult V3.3 Client Checkin M24
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [x] ET MALWARE TAG28 Associated CnC Domain in DNS Lookup (samuelblog .site)
- [x] ET MALWARE TAG28 Associated CnC Domain in DNS Lookup (samuelblog .website)
- [x] ET MALWARE S400 RAT Client Checkin
- [x] ET MALWARE S400 RAT Client Checkin via Discord
- [x] ET MALWARE ChamelGang Related CnC Domain in DNS Lookup (centralgoogle .com)
- [x] ET MALWARE ChamelGang Related CnC Domain in DNS Lookup (cdn-chrome .com)
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [ ] ET MALWARE Win32/Fake Anti-Pegasus AV CnC Exfil
- [x] ET MALWARE Cobalt Strike Malleable C2 Amazon Profile POST (PNG)
- [ ] ET MALWARE Gamaredon Related Maldoc Activity (GET)
- [x] ET MALWARE W32.Netwire Connectivity Check
- [ ] ET MALWARE Observed Cobalt Strike CnC Domain (yawero .com in TLS SNI)
- [x] ET MALWARE Wintervivern Related CnC Domain in DNS Lookup (securetourspd .com)
- [x] ET MALWARE Wintervivern Related CnC Domain in DNS Lookup (centr-security .com)
- [x] ET MALWARE Wintervivern Activity (GET)
- [x] ET MALWARE Wintervivern Retrieving Task
- [x] ET MALWARE Wintervivern Activity (GET) M3
- [x] ET MALWARE Observed DNS Query to Known PUA Host Domain
- [ ] ET MALWARE Observed HTTP Request to Known PUA Host Domain
- [x] ET MALWARE Wintervivern Activity M4 (GET)
- [ ] ET MALWARE W32.Tomiris C2 (init)
- [x] ET MALWARE Observed Elysium Stealer Domain in TLS SNI (download-serv-234116 .xyz)
- [x] ET MALWARE Tordal/Hancitor/Chanitor Checkin
- [x] ET MALWARE Lazarus APT Related CnC Domain in DNS Lookup (dshellelink .gcloud-share .com)
- [x] ET MALWARE Lazarus APT Related CnC Domain in DNS Lookup (signverydn .sharebusiness .xyz)
- [x] ET MALWARE MirrorBlast KiXtart Downloader Client Request M2
- [x] ET MALWARE Lazarus APT Related CnC Domain in DNS Lookup (product .onlinedoc .dev)
- [ ] ET MALWARE Observed Ursnif CnC Domain (Gloderuniok .website in TLS SNI)
- [ ] ET MALWARE Observed Cobalt Strike CnC Domain (Gojihu .com in TLS SNI)
- [x] ET MALWARE ESPecter Bootkit Initialization Activity (GET)
- [ ] ET MALWARE Gamaredon Related Maldoc Activity (GET)
- [x] ET MALWARE DonotGroup Related Domain in DNS Lookup (officeframework .online)
- [ ] ET MALWARE Gamaredon Maldoc Remote Template Retrieval (GET)

- [x] ET MALWARE DonotGroup Related Domain in DNS Lookup (mimeversion .top)
- [x] ET MALWARE Android/AhMyth RAT Init Checkin
- [x] ET MALWARE Android/AhMyth RAT Command Inbound (Location Manager)
- [x] ET MALWARE Android/AhMyth RAT Command Inbound (SMS Manager)
- [x] ET MALWARE Android/AhMyth RAT Command Inbound (Files Manager)
- [x] ET MALWARE Observed Lazarus Related Domain (docs .gsheetpage .com in TLS SNI)
- [x] ET MALWARE Win32/Grimagent CnC Activity
- [x] ET MALWARE FIN12 Related ICECANDLE/Cobalt Strike Activity (GET)
- [x] ET MALWARE FIN12 Related WHITEDAGGER/Cobalt Strike Beacon Activity (GET)
- [x] ET MALWARE Suspected Lazarus APT Related Activity (GET)
- [x] ET MALWARE Win32/Agent.RTQ CnC Activity
- [x] ET MALWARE Win32/Limbozar Ransomware Activity (POST)
- [x] ET MALWARE Interactsh Control Panel (DNS)
- [x] ET MALWARE Observed Malicious SSL/TLS Certificate (Jasper CnC)
- [x] ET MALWARE Jasper URI Path Observed M2
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (IcedID CnC)
- [ ] ET MALWARE IcedID CnC Domain in SSL/TLS SNI
- [x] ET MALWARE Win32/Agent.UHC CnC Activity
- [ ] ET MALWARE Maldoc Activity (GET)
- [x] ET MALWARE Harvester Group Downloader Activity (GET)
- [x] ET MALWARE [CISA AA21-291A] Possible BlackMatter Ransomware Lateral Movement
- [x] ET MALWARE Observed Malicious SSL/TLS Certificate (MagnitudeEK Associated)
- [ ] ET MALWARE Win32/JSWORM Ransomware Style Geo IP Check M1
- [x] ET MALWARE Win32/Remcos RAT Checkin 756
- [x] ET MALWARE Ousaban Banker Server Response M1
- [x] ET MALWARE Ousaban Banker Server Response M2
- [x] ET MALWARE Ousaban Banker KeepAlive Response
- [x] ET MALWARE Recaptcha Magecart Skimmer Domain in DNS Lookup (magento-plugin .com)
- [x] ET MALWARE Recaptcha Magecart Skimmer Domain in DNS Lookup (trustdomains .net)
- [x] ET MALWARE Suspected Middle East Threat Group Domain in DNS Lookup (liveupdatedriver .com)
- [x] ET MALWARE Win32.Application.ThunderN.A Checkin
- [x] ET MALWARE Observed CloudAtlas APT Related Domain (checklicensekey .com in TLS SNI)
- [x] ET MALWARE CloudAtlas APT Maldoc Activity (GET)
- [ ] ET MALWARE DonotGroup Maldoc Related Domain in DNS Lookup (digitalresolve .live)
- [ ] ET MALWARE Win32/Sabsik Config Downloader
- [x] ET MALWARE JsOutProx CnC Activity - Inbound
- [x] ET MALWARE Casbaneiro CnC Host Checkin M2
- [ ] ET MALWARE Win32/Ciadoor.10.UPX CnC Activity M2
- [x] ET MALWARE Win32/Kryptik.HNBU CryptoMiner - Report Request
- [ ] ET MALWARE Observed Cobalt Strike Related Domain (croperdate .com in TLS SNI)
- [ ] ET MALWARE Observed Cobalt Strike Related Domain (cdnwin .xyz in TLS SNI)
- [ ] ET MALWARE Win32/Agent.UWW Variant Activity (Sending System Information)
- [x] ET MALWARE Win32/Sabsik.FL.B!ml Checkin
- [ ] ET MALWARE PinkBot CnC Domain in DNS Lookup (cnc .pinklander .com)
- [x] ET MALWARE Observed Win32/CollectorStealer User-Agent M2
- [x] ET MALWARE Win32/CollectorStealer - Uploading System Information
- [x] ET MALWARE Observed Malicious FIN12 Related SSL Cert (serviceswork .net)
- [x] ET MALWARE Android/AhMyth RAT WebSocket Session
- [x] ET MALWARE Android/AhMyth RAT Command Inbound (Contacts Manager)
- [x] ET MALWARE Android/AhMyth RAT Command Inbound (Call Manager)
- [ ] ET MALWARE Android/AhMyth RAT Command Inbound (Camera Manager)
- [x] ET MALWARE Observed Malicious FIN12 Related SSL Cert
- [x] ET MALWARE Observed FIN12 Related Cobalt Strike Domain (netrie .com in TLS SNI)
- [x] ET MALWARE Observed FIN12 Related Domain (hdhuge .com in TLS SNI)
- [x] ET MALWARE FIN12 Related WEIRDLOOP/Cobalt Strike Beacon Activity (GET)
- [x] ET MALWARE Win32/Spy.Socelars.S CnC Activity M3
- [x] ET MALWARE DCRAT Activity (GET)
- [x] ET MALWARE Win32/MysterySnail RAT CnC Domain in DNS Lookup
- [x] ET MALWARE Win32/Unk.HRESQ! MultiDownloader Checkin M2
- [x] ET MALWARE Jasper URI Path Observed M1
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (IcedID CnC)
- [ ] ET MALWARE IcedID CnC Domain in SSL/TLS SNI
- [ ] ET MALWARE IcedID CnC Domain in SSL/TLS SNI
- [x] ET MALWARE W32/Witch.3FA0!tr CnC Actiivty M2
- [x] ET MALWARE ELF/FontOnLake Related CnC Domain in DNS Lookup (hm2 .yrnykx .com)
- [x] ET MALWARE Win32/Backdoor.Graphon Checkin Activity (GET)
- [x] ET MALWARE Observed Malicious SSL/TLS Certificate (MagnitudeEK Associated)
- [x] ET MALWARE Trojan:Win32/Sabsik.FL.B!ml CnC Activity
- [ ] ET MALWARE Win32/JSWORM Ransomware Style Geo IP Check M2
- [x] ET MALWARE Ousaban Banker Checkin M1
- [x] ET MALWARE Ousaban Banker Checkin M2
- [x] ET MALWARE Ousaban Banker KeepAlive
- [x] ET MALWARE Win32/WinDealer CnC Activity (Checkin)
- [x] ET MALWARE Recaptcha Magecart Skimmer Domain in DNS Lookup (cdn-cgi .net)
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [x] ET MALWARE Suspected Middle East Threat Group Domain in DNS Lookup (dnsnamefinder .com)
- [x] ET MALWARE TinyNuke VNC Checkin
- [x] ET MALWARE CloudAtlas APT Related CnC Domain in DNS Lookup (checklicensekey .com)
- [ ] ET MALWARE Observed DonotGroup Maldoc Related Domain (digitalresolve .live in TLS SNI)
- [ ] ET MALWARE DonotGroup Maldoc Activity (GET)
- [x] ET MALWARE JsOutProx CnC Activity - Outbound
- [x] ET MALWARE slock Ransomware CnC Activity
- [ ] ET MALWARE Win32/Ciadoor.10.UPX CnC Activity M1
- [x] ET MALWARE Win32/Kryptik.HNBU CryptoMiner - GetTasks Request
- [x] ET MALWARE Win32/Small.NO Checkin
- [ ] ET MALWARE Observed Cobalt Strike Related Domain (kaslose .com in TLS SNI)
- [ ] ET MALWARE Win32/Agent.UWW Variant Activity (Retrieving Commands)
- [ ] ET MALWARE Fake Google Chrome Notifications Installer
- [x] ET MALWARE Go/PSW.Agent_AGen.A Data Exfil
- [x] ET MALWARE Win32/CollectorStealer - Returning Client GeoIP Information
- [x] ET MALWARE Observed Win32/CollectorStealer User-Agent M1
- [x] ET MALWARE Win32/CollectorStealer CnC Exfil M3

- [x] ET MALWARE TA450 Nagual CnC Activity
- [ ] ET MALWARE Downloaded .bat Disables Windows Defender
- [x] ET MALWARE Trojan-Dropper.MSIL CnC Traffic - GET
- [x] ET MALWARE Lazarus Related Maldoc Activity
- [x] ET MALWARE Win32/Pterodo.NG Checkin 2
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [x] ET MALWARE SolarMarker Backdoor Related Domain in DNS Lookup (noelfpar .com)
- [ ] ET MALWARE Gamaredon/Armageddon Related Domain in DNS Lookup (list-sert .ddns .net)
- [x] ET MALWARE Gamaredon/Armageddon Activity (Retrieving Remote .dot)
- [ ] ET MALWARE Malicious Cobalt Strike SSL Certificate (cloudflace-network .digital)
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [ ] ET MALWARE Win32/LNK/Agent.GX Javascript Downloader M2
- [x] ET MALWARE SiameseKitten/Lyceum/Hexane MSIL/Shark CnC Activity (Beacon)
- [x] ET MALWARE SiameseKitten/Lyceum/Hexane MSIL/Shark CnC Activity (Upload)
- [x] ET MALWARE Lyceum Backdoor CnC Activity M2
- [x] ET MALWARE LYCEUM CnC Domain in DNS Lookup
- [x] ET MALWARE LYCEUM CnC Domain in DNS Lookup
- [x] ET MALWARE LYCEUM CnC Domain in DNS Lookup
- [x] ET MALWARE LYCEUM CnC Domain in DNS Lookup
- [x] ET MALWARE LYCEUM CnC Domain in DNS Lookup
- [x] ET MALWARE LYCEUM CnC Domain in DNS Lookup
- [x] ET MALWARE LYCEUM CnC Domain in DNS Lookup
- [x] ET MALWARE LYCEUM CnC Domain in DNS Lookup
- [ ] ET MALWARE Cobalt Strike Related CnC Domain in DNS Lookup (rackspare-technology .digital)
- [ ] ET MALWARE Observed Cobalt Strike Domain (asureupdate .tech in TLS SNI)
- [ ] ET MALWARE Downloaded Script Disables Firewall/Antivirus
- [ ] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (akastat .app)
- [ ] ET MALWARE Observed Cobalt Strike Related Domain (azurestat .app in TLS SNI)
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [ ] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (akamalupdate .site)
- [ ] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (azuresecure .tech)
- [ ] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (akabox .tech)
- [ ] ET MALWARE LNK/Agent.GX CnC Traffic
- [x] ET MALWARE Jasper URI Path Observed M4
- [x] ET MALWARE Parallax CnC Activity (set) M15
- [x] ET MALWARE Parallax CnC Activity (set) M16
- [x] ET MALWARE Observed StrongPity Domain (lurkingnet .com in TLS SNI)
- [x] ET MALWARE Observed StrongPity Domain (singlefunctionapp .com in TLS SNI)
- [x] ET MALWARE Possible NGLite Backdoor C2 Traffic (NKN)
- [ ] ET MALWARE Win32/Trojan.Nymeria CnC Activity (GET) M1
- [x] ET MALWARE Win32/Trojan.Nymeria CnC Activity (GET) M3
- [ ] ET MALWARE Win32/Trojan.Nymeria CnC Activity (GET) M5
- [x] ET MALWARE Win32/Trojan.Nymeria CnC Activity (GET) M7
- [ ] ET MALWARE Win32/Trojan.Nymeria CnC Activity (GET) M9
- [ ] ET MALWARE Possible MalDoc Retrieving Payload 2021-07-19
- [x] ET MALWARE W32/Emotet CnC Beacon 3
- [ ] ET MALWARE Cobalt Strike CnC Domain in DNS Lookup (awsmcafee .com)
- [ ] ET MALWARE Possible MalDoc Retrieving Payload 2021-11-01
- [ ] ET MALWARE APT-C-59 Related Domain in DNS Lookup
- [ ] ET MALWARE Downloaded .bat Disables Real Time Monitoring
- [x] ET MALWARE Trojan-Dropper.MSIL CnC Traffic - POST
- [x] ET MALWARE W32/Pterodo.CL CnC Checkin
- [x] ET MALWARE W32/Pterodo CnC Checkin
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [ ] ET MALWARE Gamaredon/Armageddon Related Domain in DNS Lookup (bitsadmin .ddns .net)
- [x] ET MALWARE Gamaredon/Armageddon CnC Activity (Sending Windows System Information)
- [x] ET MALWARE Datoploader Activity (GET)
- [ ] ET MALWARE Observed Cobalt Strike Domain in TLS SNI (stackpatc-technologies .digital)
- [ ] ET MALWARE Win32/LNK/Agent.GX Javascript Downloader M1
- [x] ET MALWARE RedLine - GetArguments Request
- [x] ET MALWARE SiameseKitten/Lyceum/Hexane MSIL/Shark CnC Activity (Download)
- [x] ET MALWARE Lyceum Backdoor CnC Activity M1
- [x] ET MALWARE Lyceum Backdoor CnC Activity M3
- [x] ET MALWARE LYCEUM CnC Domain in DNS Lookup
- [x] ET MALWARE LYCEUM CnC Domain in DNS Lookup
- [x] ET MALWARE LYCEUM CnC Domain in DNS Lookup
- [x] ET MALWARE LYCEUM CnC Domain in DNS Lookup
- [x] ET MALWARE LYCEUM CnC Domain in DNS Lookup
- [x] ET MALWARE LYCEUM CnC Domain in DNS Lookup
- [x] ET MALWARE LYCEUM CnC Domain in DNS Lookup
- [x] ET MALWARE LYCEUM CnC Domain in DNS Lookup
- [x] ET MALWARE LYCEUM CnC Domain in DNS Lookup
- [x] ET MALWARE Malicious Cobalt Strike SSL Cert (asurecloud .tech)
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (asureupdate .pro)
- [ ] ET MALWARE WBK Download from dotted-quad Host
- [ ] ET MALWARE Observed Malicious Cobalt Strike SSL Cert (cdnengine .biz)
- [ ] ET MALWARE Cobalt Strike Related CnC Domain in DNS Lookup (akamaclouds .tech)
- [ ] ET MALWARE Observed Malicious Cobalt Strike SSL Cert (setupfastonline .com)
- [ ] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (c2 .hax .vg)
- [ ] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (securesurvey .cloud)
- [ ] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (electronicwhosaleonline .com)
- [x] ET MALWARE Jasper URI Path Observed M3
- [x] ET MALWARE Observed Malicious SSL/TLS Certificate (Jasper CnC)
- [x] ET MALWARE Parallax CnC Response Activity M15
- [x] ET MALWARE Parallax CnC Response Activity M16
- [x] ET MALWARE Observed StrongPity Domain (autoconfirmations .com in TLS SNI)
- [ ] ET MALWARE Win32/Trojan.Nymeria CnC
- [ ] ET MALWARE Observed Compromised Domain (cryptoarenastore .com in TLS SNI) (2021-11-12)
- [x] ET MALWARE Win32/Trojan.Nymeria CnC Activity (GET) M2
- [x] ET MALWARE Win32/Trojan.Nymeria CnC Activity (GET) M4
- [x] ET MALWARE Win32/Trojan.Nymeria CnC Activity (GET) M6
- [ ] ET MALWARE Win32/Trojan.Nymeria CnC Activity (GET) M8
- [ ] ET MALWARE Win32/Trojan.Nymeria CnC Activity (GET) M10
- [x] ET MALWARE Observed Malicious SSL Cert (BitRAT)
- [x] ET MALWARE MalDoc Retrieving Payload 2021-06-15
- [x] ET MALWARE Cobalt Strike Malleable C2 JQuery Custom Profile M5
- [x] ET MALWARE Danabot Key Exchange Request

☑ ET MALWARE Matanbuchus Loader CnC M1
☑ ET MALWARE Matanbuchus Loader CnC M3
☑ ET MALWARE Matanbuchus Loader Server Response
☐ ET MALWARE Cobalt Strike CnC Domain in DNS Lookup (bg .knonwsec .com)
☐ ET MALWARE Gamaredon Related Maldoc Activity (GET)
☐ ET MALWARE ABCbot CnC Exfil
☐ ET MALWARE ABCbot CnC Instruction (dns)
☑ ET MALWARE Unattributed WebShell Access - File Upload
☑ ET MALWARE ELF/AbcBot CnC Checkin
☑ ET MALWARE TA408 Related Activity (GET)
☑ ET MALWARE lu0bot Loader HTTP Response M2
☑ ET MALWARE Candiru Related Domain in DNS Lookup (cuturl .app)
☑ ET MALWARE Candiru Related Domain in DNS Lookup (bitly .tel)
☑ ET MALWARE Candiru Related Domain in DNS Lookup (cuturl .space)
☑ ET MALWARE Cobalt Strike Activity (GET)
☐ ET MALWARE Dridex Dotted Quad CnC Request (flowbit set)
☑ ET MALWARE W32/Snojan.BNQKZQH User-Agent
☑ ET MALWARE SideCopy Related Domain in DNS Lookup (securedesk .one)
☑ ET MALWARE Cobalt Strike Activity (GET)
☑ ET MALWARE Dridex CnC Request - Spam/Worm Component
☑ ET MALWARE DonotGroup Related Domain in DNS Lookup (wordfile .live)
☑ ET MALWARE Datoploader Activity M2 (GET)
☑ ET MALWARE Cobalt Strike Related Domain in DNS Lookup (checkauj .com)
☑ ET MALWARE Observed Win32.Raccoon Stealer CnC Domain (stanculinaryblog .top in TLS SNI)
☑ ET MALWARE Chinotto CnC Activity (hello)
☑ ET MALWARE Chinotto CnC Activity (result)
☑ ET MALWARE Magecart Exfil Domain in DNS Lookup (convert-server .com)
☑ ET MALWARE Lazarus APT Related Domain in DNS Lookup (ny .silvergatehr .com)
☑ ET MALWARE Gamaredon Related Maldoc Activity (GET)
☑ ET MALWARE SpyAgent C&C Activity (Response)
☑ ET MALWARE Win64/Agent.NL Variant CnC Activity
☑ ET MALWARE Win32/Hancitor Checkin
☑ ET MALWARE Sidecopy APT Related CnC Domain in DNS Lookup (newsroom247 .xyz)
☑ ET MALWARE Sidecopy APT Related CnC Domain in DNS Lookup (republicofaf .xyz)
☑ ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup
☑ ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup
☑ ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup
☑ ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup
☑ ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup
☑ ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup
☑ ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup
☑ ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup
☑ ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup
☑ ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup

☑ ET MALWARE Matanbuchus Loader CnC M2
☑ ET MALWARE Matanbuchus Loader CnC M4
☐ ET MALWARE Danabot Associated Activity (GET)
☐ ET MALWARE Cobalt Strike Activity (GET)
☐ ET MALWARE ABCbot CnC Instruction (stop)
☐ ET MALWARE ABCbot CnC Instruction (syn)
☐ ET MALWARE ABCbot CnC Instruction (bigudp)
☑ ET MALWARE Unattributed WebShell Access - Command Execution
☑ ET MALWARE ELF/AbcBot Requesting Commands from CnC
☑ ET MALWARE lu0bot Loader HTTP Request M2
☑ ET MALWARE Candiru Related Domain in DNS Lookup (llink .link)
☑ ET MALWARE Candiru Related Domain in DNS Lookup (url-tiny .co)
☑ ET MALWARE Candiru Related Domain in DNS Lookup (instagrarn .co)
☑ ET MALWARE Cobalt Strike Activity (GET)
☑ ET MALWARE Dridex CnC Request - Spam/Worm Component
☐ ET MALWARE Dridex CnC Returning Email Addresses - Possible Spam Module
☑ ET MALWARE W32/Snojan.BNQKZQH CnC Activity
☑ ET MALWARE Cobalt Strike CnC Domain in DNS Lookup (a .pwn-t .tk)
☑ ET MALWARE Cobalt Strike CnC Domain in DNS Lookup (zuppohealth .com)
☑ ET MALWARE Win32/InfoTester Checkin
☑ ET MALWARE DonotGroup Maldoc Activity (GET)
☑ ET MALWARE MSIL/Bobik CnC Traffic
☑ ET MALWARE W32.DarkVNC Variant Checkin
☐ ET MALWARE Kimsuky Related Activity Sending Windows Information (POST)
☑ ET MALWARE Chinotto CnC Activity (command)
☑ ET MALWARE Chinotto CnC Activity (file)
☑ ET MALWARE Sidewinder APT Maldoc Activity
☑ ET MALWARE Gamaredon Related Maldoc Activity (GET)
☑ ET MALWARE SpyAgent C&C Activity (Request)
☑ ET MALWARE AgentTesla Communicating with CnC Server
☑ ET MALWARE TA505 P2P CnC Checkin
☑ ET MALWARE Sidecopy APT Related CnC Domain in DNS Lookup (afrepublic .xyz)
☑ ET MALWARE Sidecopy APT Related CnC Domain in DNS Lookup (afghannewsnetwork .com)
☑ ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup
☑ ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup
☑ ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup
☑ ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup
☑ ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup
☑ ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup
☑ ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup
☑ ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup
☑ ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup
☑ ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup
☑ ET MALWARE NOBELIUM (TA421) CnC Domain in DNS Lookup

- [x] ET MALWARE NOBELIUM (TA421) CEELOADER CnC Domain in DNS Lookup
- [ ] ET MALWARE Maldoc Activity (set)
- [x] ET MALWARE APT15/NICKEL KETRUM CnC Activity (POST)
- [x] ET MALWARE ELF/MooBot Mirai DDoS Variant Server Keep Alive
- [ ] ET MALWARE APT15/NICKEL Related CnC Activity (POST)
- [x] ET MALWARE Ransomware.Hidden-Tear Variant CnC Checkin
- [x] ET MALWARE Maldoc Retrieving Remote Template (GET)
- [ ] ET MALWARE Linux/Tsunami Downloader
- [ ] ET MALWARE Linux/Tsunami Downloader
- [x] ET MALWARE Kimsuky Related Domain in DNS Lookup
- [x] ET MALWARE Kimsuky Related FTP File Download
- [x] ET MALWARE Kimsuky Related CnC Activity
- [x] ET MALWARE Kimsuky Related Malicious VBScript Inbound M4
- [x] ET MALWARE Possible Kimsuky Related Malicious VBScript
- [x] ET MALWARE MSIL/Khonsri Ransomware CnC Activity
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [x] ET MALWARE Win32/FunnyDream Backdoor Related Domain in DNS Lookup (www .weekendorg .com)
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (news .networkslaoupdate .com)
- [x] ET MALWARE lu0bot Loader HTTP Request M3
- [ ] ET MALWARE DCRat CnC Activity M12
- [x] ET MALWARE ELF/Muhstik Botnet CnC Activity
- [x] ET MALWARE Win32/DarkWatchman Checkin Activity (POST)
- [ ] ET MALWARE Win32/BazarLoader Activity (GET)
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (hiduwu .com)
- [x] ET MALWARE Phorpiex Botnet Downloader Activity (GET)
- [x] ET MALWARE Phorpiex Botnet Downloader Activity (GET)
- [x] ET MALWARE Phorpiex Botnet Downloader Activity (GET)
- [x] ET MALWARE MageCart Skimmer Domain in DNS Lookup (bootstrap2 .xyz)
- [ ] ET MALWARE OWOWA Stealer CnC Domain in DNS Lookup
- [x] ET MALWARE Kimsuky Related Maldoc Retrieving Template (GET)
- [x] ET MALWARE Suspected MuddyWater Related CnC Activity
- [x] ET MALWARE Win32/X-Files Stealer Activity
- [x] ET MALWARE Konni Group CnC Domain in DNS Lookup
- [x] ET MALWARE Konni Group CnC Domain in DNS Lookup
- [x] ET MALWARE PurpleFox Backdoor/Rootkit Download Request M1
- [x] ET MALWARE NOBELIUM - Cobalt Strike Malleable Profile M1
- [x] ET MALWARE PurpleFox Backdoor/Rootkit Download Request M2
- [x] ET MALWARE PurpleFox Backdoor/Rootkit Checkin
- [x] ET MALWARE APT/Bitter Related Checkin Activity (GET)
- [x] ET MALWARE APT/Donot Group CnC Domain in DNS Lookup (request .soundedge .live)
- [ ] ET MALWARE Quasar CnC Domain in DNS Lookup
- [x] ET MALWARE Win32/Emotet HTML Template Response
- [x] ET MALWARE TA453 ClumsyCover Maldoc Activity (GET)
- [x] ET MALWARE TA453 Related CnC Domain in DNS Lookup (0storageatools0 .xyz)
- [x] ET MALWARE TA453 Related Activity (POST)
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (jersydok .com)
- [x] ET MALWARE Win32/Delf.TJJ Variant CnC Activity
- [x] ET MALWARE APT/Bitter Related CnC Activity
- [x] ET MALWARE Possible Pegasus Related DNS Lookup (solo-hoy .com)
- [x] ET MALWARE Possible Pegasus Related DNS Lookup (deportes24-7 .com)

- [x] ET MALWARE NOBELIUM (TA421) CEELOADER CnC Domain in DNS Lookup
- [ ] ET MALWARE Maldoc Retrieving Binary
- [x] ET MALWARE ELF/MooBot Mirai DDoS Variant CnC Checkin M3
- [x] ET MALWARE ELF/MooBot Mirai DDoS Variant Server Response M2
- [x] ET MALWARE Cobalt Strike Beacon Activity (GET)
- [x] ET MALWARE Win32/Gasti.tm Checkin Activity
- [x] ET MALWARE SideCopy APT Related Activity (GET)
- [ ] ET MALWARE Linux/Tsunami Remote Shell M1
- [ ] ET MALWARE Linux/Tsunami Remote Shell M2
- [x] ET MALWARE Kimsuky Related Domain in DNS Lookup
- [x] ET MALWARE Kimsuky Related CnC Activity
- [x] ET MALWARE Kimsuky Related Malicious VBScript Inbound M3
- [x] ET MALWARE Kimsuky Related CnC Activity
- [x] ET MALWARE Kimsuky Related CnC Activity
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (bqtconsulting .com)
- [x] ET MALWARE Win32/FunnyDream Backdoor Related Domain in DNS Lookup (www .carelessnessing .com)
- [x] ET MALWARE Win32/FunnyDream Backdoor Related Domain in DNS Lookup (www .aexhausts .com)
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (koltary .com)
- [ ] ET MALWARE DCRat CnC Activity M11
- [ ] ET MALWARE DCRat CnC Activity M13
- [x] ET MALWARE ELF/Mirai Botnet CnC Activity
- [x] ET MALWARE Octopus Backdoor Related Domain in DNS Lookup
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (gawocag .com)
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [x] ET MALWARE Phorpiex Botnet Downloader Activity (GET)
- [x] ET MALWARE Phorpiex Botnet Downloader Activity (GET)
- [x] ET MALWARE Phorpiex Botnet Downloader Activity (GET)
- [x] ET MALWARE Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern
- [x] ET MALWARE Andariel Backdoor Activity (Checkin)
- [x] ET MALWARE MuddyWater APT Related Maldoc Checkin M1
- [x] ET MALWARE Observed Malicious SSL Cert (AsyncRAT)
- [ ] ET MALWARE Cobalt Strike Activity (GET)
- [x] ET MALWARE Konni Group CnC Domain in DNS Lookup
- [x] ET MALWARE PurpleFox Backdoor/Rootkit Download Server Response M1
- [x] ET MALWARE NOBELIUM Cobalt Strike CnC Domain in DNS Lookup
- [x] ET MALWARE NOBELIUM Cobalt Strike CnC Domain in DNS Lookup
- [x] ET MALWARE PurpleFox Backdoor/Rootkit Download Server Response M2
- [ ] ET MALWARE Maldoc Retrieving Remote Template (GET)
- [x] ET MALWARE APT/Sidewinder CnC Domain in DNS Lookup (afcat .xyz)
- [x] ET MALWARE APT/Donot Group Checkin Activity (GET)
- [x] ET MALWARE Quasar CnC Domain in DNS Lookup
- [x] ET MALWARE TA453 ClumsyCover Maldoc Activity (GET)
- [x] ET MALWARE TA453 Related CnC Domain in DNS Lookup (0standavalue0 .xyz)
- [x] ET MALWARE TA453 Related CnC Domain in DNS Lookup (0brandaeyes0 .xyz)
- [x] ET MALWARE TA453 Related Activity (FTP)
- [x] ET MALWARE Zloader Related Download Activity (GET)
- [ ] ET MALWARE TellYouThePass Ransomware Checkin Activity (GET)
- [x] ET MALWARE Maldoc Retrieving Additional Resources (GET)
- [x] ET MALWARE Possible Pegasus Related DNS Lookup (mobile-analytics .netweb-cloud-services .com)
- [x] ET MALWARE Observed DNS Query to Pegasus Domain

- [x] ET MALWARE Observed DNS Query to Pegasus Domain
- [x] ET MALWARE Possible Win32/SysJoker Retrieving CnC Information (GET)
- [x] ET MALWARE SysJoker Dropper Related Domain in DNS Lookup (github .url-mini .com)
- [x] ET MALWARE SysJoker Related Domain in DNS Lookup (bookitlab .tech)
- [x] ET MALWARE SysJoker Related Domain in DNS Lookup (graphic-updater .com)
- [x] ET MALWARE SysJoker Related Domain in DNS Lookup (office360-update .com)
- [x] ET MALWARE SysJoker Related Domain in DNS Lookup (winaudio-tools .com)
- [x] ET MALWARE Win32/Small.NQT!tr CnC Activity
- [x] ET MALWARE Kimsuky APT Related Domain in DNS Lookup (gooeglle .mypressonline .com)
- [x] ET MALWARE OceanLotus APT Related Domain in DNS Lookup (confusion-cerulean-samba .glitch .me)
- [x] ET MALWARE Powershell Octopus Backdoor Sending System Information (POST)
- [x] ET MALWARE Win32/Injector.DSQR CnC Activity (POST)
- [x] ET MALWARE Powershell Octopus Backdoor Activity (POST)
- [x] ET MALWARE Powershell Octopus Backdoor Activity (GET)
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [x] ET MALWARE Lazarus APT Related Domain in DNS Lookup (lm-career .com)
- [x] ET MALWARE Donot APT Related Domain in DNS Lookup (printerjobs .xyz)
- [x] ET MALWARE Donot APT Related Domain in DNS Lookup (seasonsbackup .xyz)
- [x] ET MALWARE Win32/Suspected Reverse Shell Connection
- [x] ET MALWARE Donot APT Related Domain in DNS Lookup (submitonline .club)
- [x] ET MALWARE Donot APT Related Domain in DNS Lookup (oceansurvey .club)
- [x] ET MALWARE MSIL/Injector.VVP Downloader Activity M1
- [x] ET MALWARE Donot APT Related Domain in DNS Lookup (dataupdates .live)
- [x] ET MALWARE MoonBounce Backdoor Related Domain in DNS Lookup (kinopoisksu .com)
- [x] ET MALWARE MoonBounce Backdoor Related Domain in DNS Lookup (glbaitech .com)
- [x] ET MALWARE Microcin Backdoor Related Domain in DNS Lookup (m .necemarket .com)
- [x] ET MALWARE Microcin Backdoor Related Domain in DNS Lookup (holdmem .dbhubspi .com)
- [x] ET MALWARE Lazarus APT Maldoc Related Domain in DNS Lookup (markettrendingcenter .com)
- [x] ET MALWARE W32/Witch.3FA0!tr CnC Activity M3
- [x] ET MALWARE Win32.Raccoon Stealer - Telegram Mirror Checkin (generic)
- [ ] ET MALWARE Win32/Tiggre Variant Activity Sending System Files (POST)
- [x] ET MALWARE Win32/Spark Backdoor Related Domain in DNS Lookup (bundanesia .com)
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (portal .gfinanzen .net)
- [x] ET MALWARE Suspected APT28 Related Domain in DNS Lookup (wordkeyvpload .net)
- [x] ET MALWARE Suspected APT28 Related Domain in DNS Lookup
- [x] ET MALWARE Suspected APT28 Related Domain in DNS Lookup (jimbeam .live)
- [x] ET MALWARE Maldoc Activity (GET)
- [x] ET MALWARE DazzleSpy Related Domain in DNS Lookup
- [x] ET MALWARE DazzleSpy Related Domain in DNS Lookup
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 109
- [x] ET MALWARE Powershell with Decimal Encoded RUNPE Downloaded
- [ ] ET MALWARE Win32/ClipBanker.OC CnC Activity M1
- [ ] ET MALWARE Win32/ClipBanker.OC CnC Activity M2
- [x] ET MALWARE Win32/GrandaMisha Sending System Information (POST)
- [x] ET MALWARE Lazarus APT Related Domain in DNS Lookup (yourblogcenter .com)
- [x] ET MALWARE Lazarus APT Related Domain in DNS Lookup (allinfostudio .com)
- [x] ET MALWARE Lazarus APT Related Domain in DNS Lookup (docusign .agency)
- [x] ET MALWARE PowerShell Script Downloading Emotet DLL
- [ ] ET MALWARE Gamaredon Related Maldoc Activity (GET)
- [ ] ET MALWARE Gamaredon Related Maldoc Activity (GET)
- [x] ET MALWARE Suspicious Zipped Filename in Outbound POST Request (passwords.txt) M2
- [x] ET MALWARE Suspicious Zipped Filename in Outbound POST Request (Passwords.txt) M2
- [x] ET MALWARE Win32.SpyEyes.bllw CnC Exfil
- [x] ET MALWARE Gamaredon MalDoc CnC Exfil
- [x] ET MALWARE VBS/Dojos Downloader Activity M2
- [ ] ET MALWARE StrifeWater Rat CnC Activity
- [x] ET MALWARE Gamaredon Related VBS Activity (GET)
- [ ] ET MALWARE StrifeWater RAT CnC Activity M2
- [x] ET MALWARE Win32/Variant.Zusy.402698 Checkin
- [x] ET MALWARE Emotet Post Drop C2 Comms
- [x] ET MALWARE Likely Geodo/Emotet Downloading PE
- [x] ET MALWARE Likely Geodo/Emotet Downloading PE - Fake UA
- [x] ET MALWARE Likely Geodo/Emotet CnC Beacon
- [x] ET MALWARE W32/Emotet Empty CnC Beacon
- [x] ET MALWARE W32/Emotet.v4 Checkin
- [ ] ET MALWARE W32/Emotet.v4 Checkin 2
- [x] ET MALWARE Emotet Post Drop C2 Comms M2
- [ ] ET MALWARE W32/Emotet.v4 Checkin 3
- [x] ET MALWARE IcedID/Emotet Certificate Observed M1
- [x] ET MALWARE W32/Emotet CnC Checkin
- [x] ET MALWARE Win32/Emotet CnC Checkin (POST)
- [x] ET MALWARE Win32/Emotet CnC Checkin Response
- [x] ET MALWARE Win32/Emotet CnC Activity (POST)
- [x] ET MALWARE Win32/Emotet CnC Activity (POST) M2
- [x] ET MALWARE Win32/Spy.Agent.POX Variant CnC
- [x] ET MALWARE Win32/Emotet CnC Activity (POST) M3
- [x] ET MALWARE Win32/Emotet CnC Activity (POST) M4
- [x] ET MALWARE Evil PDF Retrieving Emotet Payload
- [x] ET MALWARE Group 21 Payload CnC Checkin
- [x] ET MALWARE W32.Geodo/Emotet Checkin Fake 404 Response
- [x] ET MALWARE Emotet Certificate Observed M2
- [ ] ET MALWARE Office Macro Emotet Download URI Nov 24 2021
- [ ] ET MALWARE W32/Emotet.v4 Checkin Fake 404 Payload Response
- [x] ET MALWARE Parallax CnC Activity M17 (set)
- [x] ET MALWARE Parallax CnC Response Activity M17
- [x] ET MALWARE Subterranean Security Domain in DNS Lookup
- [x] ET MALWARE Subterranean Crimson Rat - GetInfo Command
- [x] ET MALWARE Subterranean Crimson Rat - AssignID Command
- [x] ET MALWARE Subterranean Crimson Rat - FileManager List Command
- [x] ET MALWARE Subterranean Crimson Rat - FileManager pwd Command

- [x] ET MALWARE Subterranean Crimson Rat - GetClientLog Command
- [x] ET MALWARE Emotet CnC Beacon
- [x] ET MALWARE Win32/Emotet CnC Activity (POST) M11
- [x] ET MALWARE Arid Viper APT Related Domain in DNS Lookup (earlahenry .com)
- [x] ET MALWARE Arid Viper APT Related Domain in DNS Lookup (cooperron .me)
- [x] ET MALWARE Arid Viper APT Related Domain in DNS Lookup (juliansturgill .info)
- [x] ET MALWARE MacOS/UpdateAgent.A CnC Activity M2
- [x] ET MALWARE SManager Backdoor Domain in DNS Lookup
- [x] ET MALWARE TinyNuke VNC Checkin M3
- [ ] ET MALWARE Win32/Trojan.Agent.FSTT CnC Activity
- [x] ET MALWARE Win32/Colibri Loader Activity M2
- [x] ET MALWARE TA402/Molerats CnC Checkin
- [x] ET MALWARE Observed Lazarus APT Related Domain (designautocad .org in TLS SNI)
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [x] ET MALWARE Win32/Pteranodon CnC Exfil (POST) M2
- [x] ET MALWARE TA402/Molerats External IP Lookup Activity
- [x] ET MALWARE TA402/Molerats Related Malware Domain in DNS Lookup
- [x] ET MALWARE Observed Cobalt Strike Related Domain (world .healthamericacu .com in TLS SNI)
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [x] ET MALWARE Maldoc Domain in DNS Lookup (travelcrimea .info)
- [x] ET MALWARE DangerousPassword APT Related Domain in DNS Lookup (shopapptech .com)
- [x] ET MALWARE Observed DangerousPassword APT Related Domain (shopapppro .com in TLS SNI)
- [x] ET MALWARE DangerousPassword APT Related Domain in DNS Lookup (www .datacentre .center)
- [x] ET MALWARE sLoad Related CnC Domain in DNS Lookup (angedionisu .eu)
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [x] ET MALWARE Gamaredon CnC Domain in DNS Lookup
- [ ] ET MALWARE Win32/PrivateLoader Related Domain in DNS Lookup (fouratlinks .com)
- [x] ET MALWARE Win32.Raccoon Stealer Checkin M6
- [x] ET MALWARE Win32.Raccoon Stealer Checkin Response M5
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (ledikexive .com)
- [ ] ET MALWARE Go/Anubis CnC Activity (POST)
- [x] ET MALWARE Suspected RULER.Hacktool HTML Payload
- [x] ET MALWARE Suspicious Domain (judgebryantweekes .com) in TLS SNI
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [x] ET MALWARE DangerousPassword APT Related Domain in DNS Lookup (doc .filesaves .cloud)
- [ ] ET MALWARE MSIL/GenKryptik.FQRH Download Request
- [ ] ET MALWARE MosesStaff APT Related Activity (POST)
- [x] ET MALWARE NOBELIUM - Cobalt Strike Malleable Profile M2
- [x] ET MALWARE Win32/Pterodo Activity (POST)
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [x] ET MALWARE Win32/Trojan.Valyria.6015 CnC Activity (GET)
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)

- [x] ET MALWARE Subterranean Crimson Rat - Client Traffic
- [x] ET MALWARE Win32/Emotet CnC Activity (POST) M9
- [x] ET MALWARE Arid Viper APT Related Domain in DNS Lookup (deangelomcnay .news)
- [x] ET MALWARE Arid Viper APT Related Domain in DNS Lookup (nicholasuhl .website)
- [x] ET MALWARE Arid Viper APT Related Domain in DNS Lookup (dorothymambrose .live)
- [x] ET MALWARE MacOS/UpdateAgent.A CnC Activity M1
- [x] ET MALWARE SManager Backdoor Domain in DNS Lookup
- [x] ET MALWARE TinyNuke VNC Checkin M2
- [x] ET MALWARE Suspected Win32/Hancitor Checkin
- [ ] ET MALWARE Win32/Pteranodon CnC Exfil (POST)
- [x] ET MALWARE Win32/Colibri Loader Activity M3
- [x] ET MALWARE TA402/Molerats Payload Downloaded
- [x] ET MALWARE Lazarus APT Related CnC Domain in DNS Lookup (designautocad .org)
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [x] ET MALWARE TA402/Molerats CnC Activity
- [x] ET MALWARE TA402/Molerats Related Malware Domain in DNS Lookup
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (sdilok .com)
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (world .healthamericacu .com)
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [x] ET MALWARE Observed ZLoader Related Domain (lkjhgfgsdshja .com in TLS SNI)
- [x] ET MALWARE Observed Maldoc Domain (travelcrimea .info in TLS SNI)
- [x] ET MALWARE Observed DangerousPassword APT Related Domain (shopapptech .com in TLS SNI)
- [x] ET MALWARE DangerousPassword APT Related Domain in DNS Lookup (shopapppro .com)
- [x] ET MALWARE Observed DangerousPassword APT Related Domain (datacentre .center in TLS SNI)
- [x] ET MALWARE Observed sLoad Related Domain (angedionisu .eu in TLS SNI)
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [x] ET MALWARE Redline Stealer Related Domain in DNS Lookup (windows-upgraded .com)
- [x] ET MALWARE Win32/PrivateLoader Related Activity (GET)
- [x] ET MALWARE Win32.Raccoon Stealer Checkin Response M4
- [x] ET MALWARE Bitter APT Activity (GET)
- [ ] ET MALWARE Go/Anubis Registration Activity
- [x] ET MALWARE Win32/DarkWatchman Activity (POST)
- [x] ET MALWARE Win32/Spy.Socelars.S CnC Activity M4 (GET)
- [x] ET MALWARE Suspicious Domain (lawyeryouwant .com) in TLS SNI
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [x] ET MALWARE Kimsuky APT Related Activity (GET)
- [x] ET MALWARE Moses Staff APT Related Domain in DNS Lookup (techzenspace .com)
- [ ] ET MALWARE Win32/QuasarRAT CnC Traffic
- [x] ET MALWARE Suspected Gamaredon APT Related Maldoc Activity (GET)
- [x] ET MALWARE Win32/Pterodo Activity (POST)
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)

- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [ ] ET MALWARE Gamaredon Maldoc Activity (GET)
- [x] ET MALWARE DonotGroup APT Related Domain in DNS Lookup (font .backuplogs .xyz)
- [x] ET MALWARE JS/TrojanDownloader.Agent.TXV CnC Activity
- [x] ET MALWARE APT10 Related Domain in DNS Lookup (microsofts .cc)
- [x] ET MALWARE APT10 Related Domain in DNS Lookup (microsofts .top)
- [x] ET MALWARE APT10 Related Domain in DNS Lookup (7cnbo .com)
- [x] ET MALWARE Buhtrap SourSnack Domain in DNS Lookup (widget .forum-pokemon .com)
- [x] ET MALWARE Gamaredon APT Related Activity (POST)
- [ ] ET MALWARE Malicious Downloader Activity (GET)
- [ ] ET MALWARE PlugX Activity (POST)
- [ ] ET MALWARE Suspected PlugX Checkin Activity (udp)
- [x] ET MALWARE Win32/Pterodo CnC Activity (POST)
- [x] ET MALWARE Win32/Pterodo CnC Activity (POST)
- [x] ET MALWARE Win32/Trickbot Data Exfiltration M2
- [x] ET MALWARE Win32/Trickbot Data Exfiltration M4
- [x] ET MALWARE SunSeed Downloader Retrieving Binary (set)
- [x] ET MALWARE Gamaredon APT Maldoc Related Activity (POST)
- [x] ET MALWARE Win32/Backdoor.Daxin CnC Activity
- [x] ET MALWARE MSIL/TrojanDownloader.Agent.JVN CnC Checkin
- [ ] ET MALWARE Kimsuky APT BabyShark/SHARPEXT Related Domain in DNS Lookup (worldinfocontact .club)
- [x] ET MALWARE Cobalt Strike Activity (POST)
- [x] ET MALWARE DangerousPassword APT Related Domain in DNS Lookup
- [x] ET MALWARE Win32/PurpleFox Retrieving File (GET)
- [x] ET MALWARE Win32/BumbleBee Loader Activity (GET)
- [ ] ET MALWARE Cobalt Strike Activity (GET)
- [x] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [x] ET MALWARE Win32/Arkei Stealer CnC Checkin (GET)
- [x] ET MALWARE TA402/Molerats Related Domain in DNS Lookup
- [x] ET MALWARE MSIL/BlackGuard Stealer Exfil Activity
- [ ] ET MALWARE JS/Skimmer Inbound (Likely MageCart) M2
- [ ] ET MALWARE TA450 Nagual/STARWHALE Beacon Activity (POST)
- [x] ET MALWARE TA450 GRAMDOOR Telegram CnC Activity (POST)
- [x] ET MALWARE TransparentTribe CnC Domain in DNS Lookup
- [x] ET MALWARE SoulSearcher Malware Domain in DNS Lookup (community .weblives .net)
- [x] ET MALWARE SoulSearcher Checkin M1
- [x] ET MALWARE HermeticWizard - WMI Spreader - File Copy via SMB2 (NT Create AndX Request)
- [x] ET MALWARE Win32/Pripyat Activity (POST)
- [x] ET MALWARE HermeticWizard - WMI Spreader - File Copy via SMB1 (NT Create AndX Request)
- [ ] ET MALWARE MuddyWater APT Related Activity (POST)
- [x] ET MALWARE HermeticWizard - SMB Spreader - Remote Process Creation
- [x] ET MALWARE HermeticWizard - SMB Spreader - File Copy via SMB1 (NT Create AndX Request)
- [x] ET MALWARE APT41 KEYPLUG Related Domain in DNS Lookup
- [x] ET MALWARE Successful Cobalt Strike Shellcode Download (x64) M1
- [x] ET MALWARE Kimsuky Related Host Data Exfil M3
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [x] ET MALWARE Ghostwriter/UNC1151 Related Domain in DNS Lookup (tvasahi .online)
- [x] ET MALWARE Ghostwriter/UNC1151 Related Domain in DNS Lookup

- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [x] ET MALWARE DonotGroup APT Related Domain in DNS Lookup (tobaccosafe .xyz)
- [x] ET MALWARE DonotGroup APT Related Domain in DNS Lookup (srvrfontsdrive .xyz)
- [x] ET MALWARE ReverseRat 2.0 CnC Checkin M2
- [x] ET MALWARE APT10 Related Domain in DNS Lookup (08mma .com)
- [x] ET MALWARE APT10 Related Domain in DNS Lookup (3mmlq .com)
- [x] ET MALWARE Gamaredon APT Related Activity (GET)
- [x] ET MALWARE Gamaredon APT Related Activity (GET)
- [x] ET MALWARE Malicious lnk Downloader Activity (GET)
- [ ] ET MALWARE Suspected PlugX Checkin Activity (GET)
- [x] ET MALWARE PurpleFox Backdoor Related Domain in DNS Lookup (qq .c1c .ren)
- [x] ET MALWARE Win32/Pterodo CnC Activity (GET)
- [x] ET MALWARE Win32/Pterodo CnC Activity (POST)
- [x] ET MALWARE Win32/PurpleFox Related Activity (GET)
- [x] ET MALWARE Win32/Trickbot Data Exfiltration M3
- [ ] ET MALWARE SunSeed Lua Downloader Activity (GET)
- [ ] ET MALWARE SunSeed Download Retrieving Binary
- [ ] ET MALWARE MuddyWater APT Related Telegram Activity
- [x] ET MALWARE Observed Malicious Filename in Outbound POST Request (Browsers/Cookies/Microsoft Edge_)
- [ ] ET MALWARE Cobalt Strike Activity (GET)
- [ ] ET MALWARE Suspected Gamaredon APT Related Maldoc Activity (GET)
- [x] ET MALWARE Observed DangerousPassword APT Related Domain (cop .osonlines .co in TLS SNI)
- [x] ET MALWARE Win32/PurpleFox Related Domain in DNS Lookup
- [x] ET MALWARE Win32/PlugX Related Domain in DNS Lookup
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (jaxebiridi .com)
- [x] ET MALWARE Win32/Pterodo Activity (POST)
- [x] ET MALWARE Win32/Arkei Stealer CnC Checkin (POST)
- [x] ET MALWARE TA402/Molerats Related Domain in DNS Lookup
- [x] ET MALWARE MSIL/BlackGuard Stealer Variant Exfil via Telegram
- [x] ET MALWARE SystemBC Powershell bot registration
- [ ] ET MALWARE TA445/Ghostwrite APT Related Domain in DNS Lookup (xbeta .online)
- [ ] ET MALWARE TA450 Nagual/STARWHALE GoLang Beacon Activity (POST)
- [x] ET MALWARE TransparentTribe CnC Domain in DNS Lookup
- [x] ET MALWARE SoulSearcher Malware Domain in DNS Lookup (gmy .cimadlicks .net)
- [x] ET MALWARE SoulSearcher Malware Domain in DNS Lookup (app .tomelife .com)
- [x] ET MALWARE SoulSearcher Checkin M2
- [x] ET MALWARE HermeticWizard - WMI Spreader - Remote Process Creation M1
- [ ] ET MALWARE Win32/ArmyOfUkraine Bot Activity
- [x] ET MALWARE HermeticWizard - File Copy via SMB
- [ ] ET MALWARE MuddyWater APT Related Activity (GET)
- [x] ET MALWARE HermeticWizard - WMI Spreader - Remote Process Creation M2
- [x] ET MALWARE Win32/Remcos RAT Checkin 781
- [x] ET MALWARE Successful Cobalt Strike Shellcode Download (x32)
- [x] ET MALWARE Successful Cobalt Strike Shellcode Download (x64) M2
- [x] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [x] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [x] ET MALWARE Win32/Webdor.NAC Variant CnC Activity
- [x] ET MALWARE Linux/B1txor20 Backdoor Related Domain in DNS Lookup

- [ ] ET MALWARE MSIL/TrojanDownloader.Agent.KUO CnC Activity M1
- [x] ET MALWARE Observed TA471/UNC2589 Go Downloader User-Agent (-hobot-)
- [x] ET MALWARE Observed Cobalt Stike CnC Domain (nirsoft .me in TLS SNI)
- [ ] ET MALWARE Win32/PlugX Related Activity
- [x] ET MALWARE rat-test CnC Response
- [x] ET MALWARE Loki Locker Ransomware CnC Activity
- [x] ET MALWARE Loki Locker Ransomware CnC Domain in DNS Lookup
- [x] ET MALWARE Loki Locker Ransomware Server Response (Public Key) M2
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [x] ET MALWARE VNCStartServer BOT Variant CnC Beacon
- [x] ET MALWARE Linux/B1txor20 Backdoor Connectivity Check
- [x] ET MALWARE Linux/B1txor20 Backdoor DNS Tunnel Activity M2
- [x] ET MALWARE Observed Qbot Style SSL Certificate
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (runfs .icu)
- [x] ET MALWARE DonotGroup Pult Downloader Activity (POST)
- [x] ET MALWARE StrongPity Host Checkin
- [x] ET MALWARE AllaKore RAT Set Keep-Alive Observed
- [x] ET MALWARE Lazarus APT Related Maldoc Activity (GET)
- [x] ET MALWARE Cobalt Strike Related Activity (POST)
- [x] ET MALWARE Arid Gopher Related Domain in DNS Lookup (pam-beesly .site)
- [ ] ET MALWARE Suspected Mustang Panda APT Related Activity (GET)
- [x] ET MALWARE StrongPity APT Related Domain in DNS Lookup (sessionprotocol .com)
- [x] ET MALWARE Scarab APT - HeaderTip CnC Domain in DNS Lookup (product2020 .mrbasic .com)
- [x] ET MALWARE Sidecopy APT Backdoor Related Domain in DNS Lookup (kokotech .xyz)
- [x] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [ ] ET MALWARE ConPtyShell Client Response
- [ ] ET MALWARE ConPtyShell Server Close Shell
- [x] ET MALWARE Generic AsyncRAT Style SSL Cert
- [x] ET MALWARE Nobelium APT Related Domain in DNS Lookup (ernesttheskoolie .com)
- [ ] ET MALWARE Win32/CrimsonRAT Variant Sending Command M2 (inbound)
- [x] ET MALWARE Observed GhostWriter APT Related Cobalt Strike Domain (ao3 .hmgo .pw in TLS SNI)
- [ ] ET MALWARE GhostWriter APT Related Cobalt Strike Activity (GET)
- [ ] ET MALWARE Win32/TrojanDownloader.Agent.GEM CnC Command Fetch
- [ ] ET MALWARE Observed Malicious SSL Cert (AsyncRAT Server)
- [x] ET MALWARE FIN7 JSSLoader Activity (POST)
- [x] ET MALWARE Kimsuky APT Related Host Data Exfil M5
- [x] ET MALWARE Win32/SodaMaster domain observed in TLS SNI (www. rare-coisns. com)
- [x] ET MALWARE Win32/SodaMaster CnC HTTPS Checkin M2
- [x] ET MALWARE PurpleFox Backdoor/Rootkit Download Server Response M4
- [ ] ET MALWARE TransparentTribe APT Related Activity (POST)
- [x] ET MALWARE PlugX Related Domain in DNS Lookup (ntpserver .xyz)
- [x] ET MALWARE Win32/Farfli.CUY KeepAlive M1
- [x] ET MALWARE Win32/Backdoor Retrieving Task (POST)
- [x] ET MALWARE Win32/Backdoor Related Domain in DNS Lookup (swordoke .com)
- [x] ET MALWARE Win32/Warzone RAT Variant CnC Domain in DNS Lookup (dost .igov-service .net)
- [x] ET MALWARE MSIL/TrojanDownloader.Agent.KUO CnC Activity M2
- [x] ET MALWARE Observed Cobalt Strike CnC Domain in DNS Lookup (nirsoft .me)
- [ ] ET MALWARE Win32/44Caliber Stealer Discord Activity (POST)
- [x] ET MALWARE SideCopy APT MargulasRAT Related Activity
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [x] ET MALWARE Loki Locker Ransomware User-Agent
- [x] ET MALWARE Loki Locker Ransomware Server Response (Public Key) M1
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup
- [x] ET MALWARE VNCStartServer USR Variant CnC Beacon
- [x] ET MALWARE Win32/Qbot CnC Activity M2
- [x] ET MALWARE Linux/B1txor20 Backdoor DNS Tunnel Activity M1
- [x] ET MALWARE Linux/B1txor20 Backdoor DNS Tunnel Activity M3
- [x] ET MALWARE TA471/UNC2589 Related Activity (GET)
- [x] ET MALWARE Bitter APT Backdoor Related Activity
- [ ] ET MALWARE Backdoor/Win.Gh0stRAT CnC Exfil
- [x] ET MALWARE AllaKore RAT CnC Checkin M1
- [x] ET MALWARE AllaKore RAT ID Command Observed
- [x] ET MALWARE Cobalt Strike Related Activity (GET)
- [x] ET MALWARE Arid Gopher Related Domain in DNS Lookup (grace-fraser .site)
- [x] ET MALWARE Arid Gopher Related Domain in DNS Lookup (mozelllittel .com)
- [ ] ET MALWARE Mustang Panda APT Related Activity (GET)
- [x] ET MALWARE Arid Gopher Related User-Agent (aimxxhwpcc)
- [x] ET MALWARE Sidecopy APT Backdoor Related Activity (POST)
- [ ] ET MALWARE Win32/Pterodo Activity (POST)
- [x] ET MALWARE Kimsuky APT Related Host Data Exfil M4
- [ ] ET MALWARE ConPtyShell Server Command (whoami)
- [x] ET MALWARE Win32/TrojanDownloader.Agent.GEM CnC Checkin
- [x] ET MALWARE Nobelium APT Related Domain in DNS Lookup (theskoolieblog .com)
- [ ] ET MALWARE Win32/CrimsonRAT Variant Sending Command (inbound)
- [ ] ET MALWARE Win32/CrimsonRAT Variant Sending System Information (outbound)
- [x] ET MALWARE GhostWriter APT Related Cobalt Strike Domain in DNS Lookup (hmgo .pw)
- [ ] ET MALWARE Observed DNS Query to Win32/TrojanDownloader.Agent.GEM Domain
- [ ] ET MALWARE Win32/TrojanDownloader.Agent.GEM CnC Domain Fetch
- [x] ET MALWARE FIN7 JSSLoader Activity (GET)
- [x] ET MALWARE FIN7 JSSLoader Related Domain in DNS Lookup
- [x] ET MALWARE Win32/SodaMaster domain observed in DNS query (www. rare-coisns. com)
- [x] ET MALWARE Win32/SodaMaster CnC HTTPS Checkin M1
- [x] ET MALWARE PurpleFox Backdoor/Rootkit Download Server Response M3
- [x] ET MALWARE Suspected SmokeLoader Retrieving Next Stage (GET)
- [ ] ET MALWARE TransparentTribe APT Related Backdoor Activity
- [x] ET MALWARE PlugX Related Domain in DNS Lookup (cxks8 .com)
- [x] ET MALWARE Win32/Backdoor Checkin (POST)
- [x] ET MALWARE Win32/Backdoor Sending Task Status (POST)
- [x] ET MALWARE Observed Win32/Backdoor Related Domain (swordoke .com in TLS SNI)
- [x] ET MALWARE Meterpreter or Other Reverse Shell SSL Cert

- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (wikipedia-book .vote)
- [x] ET MALWARE Trojan.Verblecon User Agent Observed
- [x] ET MALWARE Observed Trojan.Verblecon Related Domain (gaymers .ax in TLS SNI)
- [x] ET MALWARE Observed Trojan.Verblecon Related Domain (jonathanhardwick .me in TLS SNI)
- [x] ET MALWARE Observed Trojan.Verblecon Related Domain (.verble .rocks in TLS SNI)
- [x] ET MALWARE Observed Trojan.Verblecon Related Domain (verble .software in TLS SNI)
- [x] ET MALWARE Observed MSIL/Lightning Stealer Domain (panelss .xyz in TLS SNI)
- [x] ET MALWARE Win32/Eternity Stealer CnC Domain in DNS Lookup (eterprx .net)
- [x] ET MALWARE Observed Win32/Eternity Stealer Domain (eternitypr .net in TLS SNI)
- [x] ET MALWARE Win32/Eternity Stealer Activity (POST)
- [ ] ET MALWARE Suspected Lazarus APT Related Backdoor Activity (POST) M1
- [ ] ET MALWARE Win32/Killav.CM Checkin M2
- [x] ET MALWARE Win32/WindowsDefender Bypass Download Request
- [x] ET MALWARE Deep Panda Domain in DNS Lookup (vpn2 .smi1egate .com)
- [x] ET MALWARE Deep Panda Domain in DNS Lookup (giga .gnisoft .com)
- [ ] ET MALWARE Observed BlackGuard_v2 Domain in DNS Lookup (win .mirtonewbacker .com)
- [x] ET MALWARE Observed BlackGuard_v2 Domain in DNS Lookup (umpulumpu .ru)
- [x] ET MALWARE Observed BlackGuard_v2 Domain in DNS Lookup (greenblguard .shop)
- [ ] ET MALWARE Observed BlackGuard_v2 Domain in DNS Lookup (onetwostep .at)
- [x] ET MALWARE BlackGuard_v2 Data Exfiltration Observed
- [ ] ET MALWARE Observed DNS Query to POWERPLANT Domain
- [ ] ET MALWARE Observed DNS Query to POWERPLANT Domain
- [ ] ET MALWARE Observed DNS Query to POWERPLANT Domain
- [ ] ET MALWARE Observed DNS Query to POWERPLANT Domain
- [ ] ET MALWARE Observed DNS Query to POWERPLANT Domain
- [x] ET MALWARE Win32/POWERPLANT CnC Exfil (INIT)
- [ ] ET MALWARE Observed DNS Query to LOADOUT Domain
- [ ] ET MALWARE Observed DNS Query to LOADOUT Domain
- [x] ET MALWARE ELF/Mirai Variant UA Inbound (b3astmode)
- [x] ET MALWARE Win32/Agent.USB Variant CnC Activity
- [ ] ET MALWARE SSL/TLS Certificate Observed (FIN7 JSSLoader)
- [ ] ET MALWARE SSL/TLS Certificate Observed (FIN7 JSSLoader)
- [x] ET MALWARE Android Infostealer CnC Check-In
- [x] ET MALWARE Spytector Domain (mail .spytector .com) in TLS SNI
- [ ] ET MALWARE Pegasus Domain in DNS Lookup (akhbar-islamyah .com)
- [ ] ET MALWARE Pegasus Domain in DNS Lookup (al-nusr .net)
- [ ] ET MALWARE Pegasus Domain in DNS Lookup (al-taleanewsonline .net)
- [ ] ET MALWARE Pegasus Domain in DNS Lookup (alrainew .com)
- [x] ET MALWARE Win32/FFDroider CnC Activity
- [x] ET MALWARE TA455 CnC Domain in DNS Lookup
- [x] ET MALWARE TA455 Related CnC Domain in DNS Lookup
- [x] ET MALWARE TA455 Related CnC Domain in DNS Lookup
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (careers-finder .com)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (supportskype .com)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (cortanaupdate .co)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (cloudgoogle .co)
- [ ] ET MALWARE Cobalt Strike Related Activity (GET)
- [x] ET MALWARE Trojan.Verblecon Related Domain in DNS Lookup (gaymers .ax)
- [x] ET MALWARE Trojan.Verblecon Related Domain in DNS Lookup (jonathanhardwick .me)
- [x] ET MALWARE Trojan.Verblecon Related Domain in DNS Lookup (.verble .rocks)
- [x] ET MALWARE Trojan.Verblecon Related Domain in DNS Lookup (verble .software)
- [x] ET MALWARE MSIL/Lightning Stealer Exfil Activity
- [ ] ET MALWARE MustangPanda APT Dropper Activity (POST)
- [x] ET MALWARE Win32/Eternity Stealer CnC Domain in DNS Lookup (eternitypr .net)
- [x] ET MALWARE Observed Win32/Eternity Stealer Domain (eterprx .net in TLS SNI)
- [ ] ET MALWARE Win32/PlugX/Talisman Activity (POST)
- [ ] ET MALWARE Win32/Killav.CM CnC Response
- [x] ET MALWARE MSIL/Unk.CoinMiner Downloader
- [x] ET MALWARE Deep Panda Downloader User-Agent (mozilla_horizon) GET request observed
- [x] ET MALWARE Deep Panda Domain in DNS Lookup (svn1 .smi1egate .com)
- [x] ET MALWARE Deep Panda CnC Check-In
- [x] ET MALWARE Observed BlackGuard_v2 Domain (win .mirtonewbacker .com) in TLS SNI
- [x] ET MALWARE Observed BlackGuard_v2 Domain (umpulumpu .ru) in TLS SNI
- [x] ET MALWARE Observed BlackGuard_v2 Domain (greenblguard .shop) in TLS SNI
- [ ] ET MALWARE Observed BlackGuard_v2 Domain (onetwostep .at) in TLS SNI
- [ ] ET MALWARE Observed DNS Query to POWERPLANT Domain
- [ ] ET MALWARE Observed DNS Query to POWERPLANT Domain
- [ ] ET MALWARE Observed DNS Query to POWERPLANT Domain
- [ ] ET MALWARE Observed DNS Query to POWERPLANT Domain
- [x] ET MALWARE Win32/POWERPLANT CnC Exfil (Query)
- [ ] ET MALWARE Observed DNS Query to LOADOUT Domain
- [ ] ET MALWARE Observed DNS Query to LOADOUT Domain
- [x] ET MALWARE Win32/LOADOUT CnC Activity
- [x] ET MALWARE ELF/Mirai Variant UA Outbound (b3astmode)
- [ ] ET MALWARE MSIL/Unk.CoinMiner Downloader
- [ ] ET MALWARE SSL/TLS Certificate Observed (FIN7 JSSLoader)
- [x] ET MALWARE Suspected Lazarus APT Related Backdoor Activity (POST) M2
- [ ] ET MALWARE Spytector Domain DNS Lookup (mail .spytector .com)
- [x] ET MALWARE Pegasus Domain in DNS Lookup (akhbar-almasdar .com)
- [ ] ET MALWARE Pegasus Domain in DNS Lookup (akhbarnew .com)
- [ ] ET MALWARE Pegasus Domain in DNS Lookup (al-taleanews .net)
- [ ] ET MALWARE Pegasus Domain in DNS Lookup (al7erak247 .com)
- [ ] ET MALWARE Pegasus Domain in DNS Lookup (arabia-islamion .com)
- [x] ET MALWARE TA455 CnC Domain in DNS Lookup
- [x] ET MALWARE Win32/FFDroider CnC Activity M2
- [x] ET MALWARE TA455 Related CnC Domain in DNS Lookup
- [x] ET MALWARE TA455 Related CnC Domain in DNS Lookup
- [x] ET MALWARE Observed DNS Query to TA455 Domain (enerflex .org)
- [x] ET MALWARE Observed DNS Query to TA455 Domain (alharbitelecom .co)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (cortanaservice .com)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (onedrivelive .me)

- [ ] ET MALWARE Observed DNS Query to TA455 Domain (edge-cloudservices .com)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (updatedefender .net)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (helpdesk-product .com)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (enerflex .ddns .net)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (khaleejtimes .co)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (outlookde .live)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (online-chess .live)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (saipem .org)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (sauditourismguide .com)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (updateservices .co)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (office-shop .me)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (globaltalent .in)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (microsoftedgesh .info)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (remgrogroup .com)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (getadobe .ddns .net)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (librarycollection .org)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (elecresearch .org)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (updateddns .ddns .net)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (appslocallogin .online)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (funnychess .online)
- [x] ET MALWARE Observed DNS Query to TA455 Domain (googleupdate .co)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (thefreemovies .net)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (etisalatonline .com)
- [ ] ET MALWARE Pegasus Domain in DNS Lookup
- [ ] ET MALWARE Pegasus Domain in DNS Lookup
- [x] ET MALWARE Pegasus Domain in DNS Lookup
- [x] ET MALWARE Pegasus Domain in DNS Lookup
- [x] ET MALWARE Pegasus Domain in DNS Lookup
- [x] ET MALWARE Vidar Stealer CnC Domain in DNS Lookup
- [ ] ET MALWARE Observed DNS Query to Winnti Domain
- [x] ET MALWARE Win32/Farfli.CUY CnC Server Response
- [x] ET MALWARE Base64 Encoded Stealer Config from Server - APPDATA or USERPROFILE Environment Variable M1
- [x] ET MALWARE Base64 Encoded Stealer Config from Server - APPDATA or USERPROFILE Environment Variable M3
- [x] ET MALWARE MSIL/Revenge-RAT Keep-Alive Activity (Outbound) M2
- [x] ET MALWARE Linux/Denonia DNS Request Over HTTPS (denonia .xyz) M1
- [x] ET MALWARE NetSupport RAT with System Information
- [x] ET MALWARE Snatch Ransomware Checkin (POST)
- [ ] ET MALWARE Win32/Farfli.CUY Downloader
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (online-audible .com)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (sparrowsgroup .org)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (defenderupdate .ddns .net)
- [x] ET MALWARE Observed DNS Query to TA455 Domain (linkedinz .me)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (microsoftdefender .info)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (lukoil .in)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (exprogroup .org)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (mastergatevpn .com)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (listen-books .com)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (microsoftcdn .co)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (sharepointnotify .com)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (savemoneytrick .com)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (outlookdelivery .com)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (onedriveupdate .net)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (googleservices .co)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (freechess .live)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (applytalents .com)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (mideasthiring .com)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (apply-jobs .com)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (talent-recruitment .org)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (updatedns .ddns .net)
- [ ] ET MALWARE Observed DNS Query to TA455 Domain (talktalky .azurewebsites .net)
- [x] ET MALWARE Observed DNS Query to TA455 Domain (getadobe .net)
- [ ] ET MALWARE Pegasus Domain in DNS Lookup
- [x] ET MALWARE Pegasus Domain in DNS Lookup
- [x] ET MALWARE Pegasus Domain in DNS Lookup
- [x] ET MALWARE Pegasus Domain in DNS Lookup
- [x] ET MALWARE Pegasus Domain in DNS Lookup
- [ ] ET MALWARE Observed Vidar Stealer Domain (computerprotect .me) in TLS SNI
- [ ] ET MALWARE Observed DNS Query to Winnti Domain
- [x] ET MALWARE Win32/Farfli.CUY KeepAlive M2
- [x] ET MALWARE Base64 Encoded Stealer Config from Server - APPDATA or USERPROFILE Environment Variable M2
- [x] ET MALWARE Base64 Encoded Stealer Config from Server - APPDATA or USERPROFILE Environment Variable M4
- [x] ET MALWARE Linux/Denonia DNS Request Over HTTPS (denonia .xyz) M2
- [x] ET MALWARE Possible Ursnif/Gamaredon Related VNC Module CnC Beacon
- [ ] ET MALWARE Observed SocGholish Domain in TLS SNI
- [ ] ET MALWARE Colibri Loader Domain in DNS Lookup (securetunnel .co)
- [x] ET MALWARE Win32/TrojanDownloader.Agent.GEM Maldoc Remote Template Request M1

- [x] ET MALWARE Win32/TrojanDownloader.Agent.GEM Maldoc Remote Template Request M2
- [x] ET MALWARE MSIL/Crimson Receiving Command (ping) M1
- [x] ET MALWARE Scarab APT - HeaderTip CnC Domain in DNS Lookup (ebook .port25 .biz)
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (mail .igov-service .net)
- [x] ET MALWARE Observed Cobalt Strike Related Domain (mail .igov-service .net in TLS SNI)
- [ ] ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (showsvc .com)
- [ ] ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (upservicemc .com)
- [ ] ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (allmyad .com)
- [ ] ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (gvgnci .com)
- [ ] ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (polanicia .com)
- [ ] ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (worldchangeos .com)
- [ ] ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (jmarrycs .com)
- [x] ET MALWARE Fodcha Bot CnC Checkin
- [x] ET MALWARE Fodcha Bot CnC Heartbeat Response
- [ ] ET MALWARE Observed DNS Query to Fodcha Bot Domain
- [ ] ET MALWARE Observed DNS Query to VBS/Agent.PUK Domain
- [x] ET MALWARE VBS/Agent.PUK Data Exfiltration Request M2
- [x] ET MALWARE Lyceum Golang HTTP Backdoor CnC Checkin
- [x] ET MALWARE Lyceum Golang HTTP Backdoor Submitting Data to CnC
- [ ] ET MALWARE Malicious VBS Sending System Information (POST)
- [ ] ET MALWARE Gamaredon APT Related Activity (GET)
- [ ] ET MALWARE Observed DNS Query to ShadowPad Domain (supership .dynv6 .net)
- [ ] ET MALWARE Observed DNS Query to ShadowPad Domain (supermarket .ownip .net)
- [ ] ET MALWARE Observed DNS Query to Hilal RAT Domain (bnt2 .live)
- [ ] ET MALWARE Observed DNS Query to Hilal RAT Domain (archery .dedyn .io)
- [ ] ET MALWARE Observed DNS Query to Hilal RAT Domain (market .dedyn .io)
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (notixow .com)
- [x] ET MALWARE MSIL/Crimson Rat CnC Exfil
- [ ] ET MALWARE MSIL/Crimson CnC Server Command (info) M3
- [x] ET MALWARE Matrix Max Stealer Exfiltration Observed
- [ ] ET MALWARE Observed Blackguard_v3.5 Domain (ritmflow .online) in TLS SNI
- [x] ET MALWARE Observed Zingo/GinzoStealer CnC Domain (nominally .ru in TLS SNI)
- [x] ET MALWARE Zingo/GinzoStealer Downloading Additional Payloads
- [ ] ET MALWARE Suspected TA404 APT Related Activity M2
- [x] ET MALWARE DPRK APT Related Domain in DNS Lookup (tokenais .com)
- [x] ET MALWARE DPRK APT Related Domain in DNS Lookup (alticgo .com)
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (vasepinay .com)
- [x] ET MALWARE Win32/TrojanDownloader.Agent.RFS Variant Checkin
- [ ] ET MALWARE DPRK APT Related Domain in DNS Lookup (beastmodser .club)
- [x] ET MALWARE Win32/STEALBIT Data Exfiltration Tool Activity (PUT)
- [ ] ET MALWARE Cobalt Strike X-Client Header (notevil)
- [x] ET MALWARE MSIL/Crimson Receiving Command (folders list)
- [x] ET MALWARE MSIL/Crimson Receiving Command (getavs)
- [ ] ET MALWARE Win32/Shuckworm CnC Exfil M1
- [x] ET MALWARE MSIL/Crimson CnC Server Command (info) M1
- [x] ET MALWARE Vidar/Arkei/Megumin Stealer Keywords Retrieved
- [x] ET MALWARE Scarab APT - HeaderTip CnC Domain in DNS Lookup (mert .my03 .com)
- [ ] ET MALWARE Cobalt Strike Related Activity (GET)
- [ ] ET MALWARE TransparentTribe APT Related Activity (POST)
- [ ] ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (wicommerece .com)
- [ ] ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (netpixelds .com)
- [ ] ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (ananoka .com)
- [ ] ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (msfbckupsc .com)
- [ ] ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (informaxima .org)
- [ ] ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (liongracem .com)
- [ ] ET MALWARE DeathStalker/EvilNum Delivery Domain in DNS Lookup (am-reader .com)
- [x] ET MALWARE Fodcha Bot CnC Client Heartbeat
- [x] ET MALWARE Observed DNS Query to Fodcha Bot Domain
- [ ] ET MALWARE Observed DNS Query to VBS/Agent.PUK Domain
- [x] ET MALWARE VBS/Agent.PUK Data Exfiltration Request M1
- [x] ET MALWARE Lyceum Golang HTTP Backdoor Connectivity Check
- [x] ET MALWARE Lyceum Golang HTTP Backdoor Requesting Commands
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [x] ET MALWARE EvilNominatus Ransomware Related Domain in DNS Lookup
- [x] ET MALWARE Possible Gamaredon APT Related Malicious Shortcut Activity (GET)
- [x] ET MALWARE Observed DNS Query to ShadowPad Domain (greatsong .soundcast .me)
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [ ] ET MALWARE Observed DNS Query to Hilal RAT Domain (signin .dedyn .io)
- [ ] ET MALWARE Observed DNS Query to Hilal RAT Domain (market .vinam .me)
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (hojimizeg .com)
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (rewujisaf .com)
- [x] ET MALWARE MSIL/Crimson Rat CnC Server Response
- [ ] ET MALWARE MSIL/Crimson Client Command Response (info)
- [x] ET MALWARE Zingo/GinzoStealer Stealer Exfiltration Observed
- [ ] ET MALWARE Blackguard_v3.5 Domain in DNS Lookup (ritmflow .online)
- [x] ET MALWARE Zingo/GinzoStealer Data Exfiltration M2
- [ ] ET MALWARE Suspected TA404 APT Related Activity M1
- [x] ET MALWARE DPRK APT Related Domain in DNS Lookup (dafom .dev)
- [x] ET MALWARE DPRK APT Related Domain in DNS Lookup (cryptais .com)
- [x] ET MALWARE DPRK APT Related Domain in DNS Lookup (esilet .com)
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (dixavokij .com)
- [x] ET MALWARE DPRK APT Related Maldoc Activity (POST)
- [x] ET MALWARE DPRK APT Related Maldoc Activity (POST) M2
- [ ] ET MALWARE Win64/CobaltStrike.Beacon.J CnC Checkin
- [x] ET MALWARE MSIL/Crimson Receiving Command (dirs list)
- [x] ET MALWARE MSIL/Crimson Receiving Command (files list)
- [x] ET MALWARE MSIL/CrimsonRAT Activity (POST)
- [ ] ET MALWARE Win32/Shuckworm CnC Exfil M2

- [ ] ET MALWARE Win32/Pterodo CnC VNC Connect Request
- [ ] ET MALWARE Win32/ChromeBack CnC Checkin
- [ ] ET MALWARE Win32/ChromeBack Browser Hijacker Sync
- [x] ET MALWARE Win32/ChromeBack Browser Hijacker (getAd)
- [x] ET MALWARE 000Stealer CnC Checkin
- [x] ET MALWARE Win32/Blacktech Plead CnC Activity (GET)
- [x] ET MALWARE BlackCat Ransomware Related Domain in TLS SNI (updatedaemon .com)
- [x] ET MALWARE Observed BlackCat Ransomware Related SSL Cert (updatedaemon .com)
- [x] ET MALWARE Arkei/Vidar/Mars Stealer Variant
- [x] ET MALWARE Win32/TrojanDownloader.Agent.APBB Checkin
- [ ] ET MALWARE Observed DNS Query to Certishell Domain (forummanazera .sk)
- [ ] ET MALWARE Observed DNS Query to Certishell Domain (msrousinov .cz)
- [x] ET MALWARE Observed DNS Query to Certishell Domain (profiit .fiit .stuba .sk)
- [x] ET MALWARE Observed DNS Query to Certishell Domain (sivpici .php5 .sk)
- [x] ET MALWARE Observed DNS Query to Certishell Domain (limousine-service .cz)
- [x] ET MALWARE Observed DNS Query to Certishell Domain (vavave .xf .cz)
- [x] ET MALWARE Win32/Filecoder.STOP Variant Request for Public Key
- [ ] ET MALWARE Win32/Agent.VAZ Bot CnC Checkin (StatusTime)
- [ ] ET MALWARE Win32/Agent.VAZ Bot CnC Checkin (Checkupdate)
- [x] ET MALWARE Observed Malicious SSL Cert for IRS Credential Phish Domain (supportmicrohere .com)
- [x] ET MALWARE Innostealer Domain in DNS Lookup (windows11-upgrade .com)
- [ ] ET MALWARE Innostealer Domain in DNS Lookup (windows11-infoserver .com)
- [ ] ET MALWARE Innostealer Domain (windows-11info .com) in TLS SNI
- [ ] ET MALWARE GOLDBACKDOOR Domain in DNS Lookup (main .dailynk .us)
- [ ] ET MALWARE GOLDBACKDOOR Domain (main .dailynk .us) in TLS SNI
- [ ] ET MALWARE Innostealer Domain in DNS Lookup (seventyfor .site)
- [ ] ET MALWARE Innostealer Domain (windows-server031 .com) in TLS SNI
- [x] ET MALWARE Common RAT Connectivity Check Observed
- [x] ET MALWARE TA410 APT FlowCloud Dependency Download M2
- [x] ET MALWARE TA410 APT FlowCloud Dependency Download M4
- [ ] ET MALWARE DPRK APT Related Maldoc Activity (POST)
- [ ] ET MALWARE TraderTraitor CnC Domain (alticgo .com) in DNS Lookup
- [ ] ET MALWARE TraderTraitor CnC Domain (tokenais .com) in DNS Lookup
- [ ] ET MALWARE TraderTraitor CnC Domain (www .esilet .com) in DNS Lookup
- [x] ET MALWARE TraderTraitor CnC Domain (dafom .dev) in DNS Lookup
- [ ] ET MALWARE Observed TraderTraitor Domain (cryptais .com) in TLS SNI
- [ ] ET MALWARE Observed TraderTraitor Domain (aideck .net) in TLS SNI
- [ ] ET MALWARE Observed TraderTraitor Domain (creaideck .com) in TLS SNI
- [x] ET MALWARE TraderTraitor dafom CnC Checkin M1 (POST)
- [x] ET MALWARE TraderTraitor AlticGO CnC Checkin (POST)
- [x] ET MALWARE TA410 APT LookBack Client HTTP Activity (POST)
- [x] ET MALWARE DDoS Win32/Nitol.A Checkin
- [x] ET MALWARE Nobelium APT Related Activity (GET)
- [ ] ET MALWARE Win32/ChromeBack Extention Payload Fetch
- [ ] ET MALWARE Win32/ChromeBack Browser Hijacker Query Redirection
- [x] ET MALWARE Win32/ChromeBack Browser Hijacker Home Beacon
- [x] ET MALWARE Kratos Silent Miner Checkin via Discord
- [x] ET MALWARE 000Stealer Data Exfiltration M1
- [ ] ET MALWARE BlackTech FlagPro Dropper Activity (GET)
- [x] ET MALWARE BlackCat Ransomware Related Domain in DNS Lookup (updatedaemon .com)
- [x] ET MALWARE Win32/Blacktech Plead CnC Activity (POST)
- [x] ET MALWARE Zingo/GinzoStealer Data Command List Fetch
- [x] ET MALWARE 000Stealer Data Exfiltration M2
- [ ] ET MALWARE Observed DNS Query to Certishell Domain (reality .skarabeus .sk)
- [x] ET MALWARE Observed DNS Query to Certishell Domain (googleprovider .ru)
- [x] ET MALWARE Observed DNS Query to Certishell Domain (freetips .php5 .sk)
- [x] ET MALWARE Observed DNS Query to Certishell Domain (hotel-boss .eu)
- [x] ET MALWARE Observed DNS Query to Certishell Domain (ms .rousinov .cz)
- [x] ET MALWARE Win32/Vodkagats Loader Requesting Payload
- [x] ET MALWARE Win32/Filecoder.STOP Variant Public Key Download
- [ ] ET MALWARE Win32/Agent.VAZ Bot CnC Checkin (Comands)
- [ ] ET MALWARE Win32/Agent.VAZ Bot CnC Checkin M1
- [x] ET MALWARE Observed Malicious SSL Cert IRS Credential Phish Domain (jbdelmarket .com)
- [ ] ET MALWARE Innostealer Domain in DNS Lookup (windows-11info .com)
- [ ] ET MALWARE Innostealer Domain (windows11-upgrade .com) in TLS SNI
- [ ] ET MALWARE Innostealer Domain (windows11-infoserver .com) in TLS SNI
- [ ] ET MALWARE GOLDBACKDOOR Domain in DNS Lookup (lit-peak-25706 .herokuapp .com)
- [ ] ET MALWARE GOLDBACKDOOR Domain (lit-peak-25706 .herokuapp .com) in TLS SNI
- [ ] ET MALWARE Innostealer Domain in DNS Lookup windows-server031 .com)
- [ ] ET MALWARE Innostealer Domain (seventyfor .site) in TLS SNI
- [x] ET MALWARE TA410 APT FlowCloud Dependency Download M1
- [x] ET MALWARE TA410 APT FlowCloud Dependency Download M3
- [x] ET MALWARE Possible TA410 APT FlowCloud Dependency Download
- [x] ET MALWARE TA410 APT FlowCloud Hardcoded Request (POST)
- [ ] ET MALWARE TraderTraitor CnC Domain (cryptais .com) in DNS Lookup
- [ ] ET MALWARE TraderTraitor CnC Domain (aideck .net) in DNS Lookup
- [ ] ET MALWARE TraderTraitor CnC Domain (creaideck .com) in DNS Lookup
- [x] ET MALWARE Observed TraderTraitor Domain (alticgo .com) in TLS SNI
- [ ] ET MALWARE Observed TraderTraitor Domain (tokenais .com) in TLS SNI
- [ ] ET MALWARE Observed TraderTraitor Domain (www .esilet .com) in TLS SNI
- [ ] ET MALWARE Observed TraderTraitor Domain (dafom .dev) in TLS SNI
- [x] ET MALWARE TraderTraitor dafom CnC Checkin M2 (POST)
- [x] ET MALWARE MoneroOcean Installer Batch Script Inbound
- [x] ET MALWARE [ESET] TA410 APT LookBack HTTP Server Response
- [x] ET MALWARE Win32.ServStart.D Checkin
- [x] ET MALWARE China Based APT Related Domain in DNS Lookup (p1 .offline-microsoft .com)

- [x] ET MALWARE China Based APT Related Domain in DNS Lookup (portal .super-encrypt .com)
- [x] ET MALWARE Nerbian RAT Data Exfiltration
- [x] ET MALWARE Likely Mirai Related Outbound Shell Request
- [x] ET MALWARE Lazarus APT Related Domain in DNS Lookup (onlinestockwatch .net)
- [x] ET MALWARE Maldoc Retrieving Remote Template (GET)
- [ ] ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (daji8 .me)
- [ ] ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (11i .me)
- [ ] ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (googie .ph)
- [ ] ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (rootkit .tools)
- [ ] ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (mircrosoftscoulds .com)
- [ ] ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (adobe .name)
- [ ] ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (adobe-flash .wiki)
- [x] ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (flash .wy886066 .com)
- [ ] ET MALWARE Earth Berberoka CnC Domain in DNS Lookup
- [ ] ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (linux .wy01 .com)
- [ ] ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (agph .ivi66 .net)
- [x] ET MALWARE Win32/PlugX Variant CnC Activity
- [x] ET MALWARE UsefulTyphon CnC Activity M2
- [x] ET MALWARE JS/Cryxos Stealer Variant Sending Data to Telegram (POST)
- [ ] ET MALWARE PoshC2 - Observed Default URI Structure M1
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M3
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M5
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M7
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M9
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M11
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M13
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M16
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M18
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M20
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M22
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M24
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M26
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M28
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M30
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M32
- [x] ET MALWARE Eternity Stealer Data Exfiltration Activity
- [x] ET MALWARE Stonefly APT Related Domain in DNS Lookup (semiconductboard .com)
- [x] ET MALWARE Win32/SilentBreak Related Domain in DNS Lookup (eleed .cloud)
- [x] ET MALWARE Win32/SilentBreak Related Domain in DNS Lookup
- [x] ET MALWARE TA452 Related Domain in DNS Lookup
- [x] ET MALWARE Win32/Wacatac.B Loader CnC Checkin
- [ ] ET MALWARE Win32/Throwback CnC Activity (POST)
- [x] ET MALWARE Malicious ELF Activity
- [x] ET MALWARE PennyWise Stealer Data Exfil M1
- [x] ET MALWARE IceApple User-Agent observed
- [ ] ET MALWARE Restylink Domain in DNS Lookup (mbusabc .com)
- [x] ET MALWARE Restylink Domain in DNS Lookup (officehoster .com)
- [x] ET MALWARE Restylink Domain in DNS Lookup (sseekk .xyz)
- [x] ET MALWARE BlueShtorm Infostealer Data Exfiltration
- [x] ET MALWARE Win32/NetDooka Framework Related Activity (POST)
- [x] ET MALWARE Nerbian RAT CnC Checkin
- [x] ET MALWARE Win32/Farfli.BAL CnC Activity
- [ ] ET MALWARE TeamTNT Related Domain in DNS Lookup (chimaera .cc)
- [x] ET MALWARE DeathStalker APT Related Maldoc Activity (GET)
- [ ] ET MALWARE PoshC2 Downloader Activity (GET)
- [ ] ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (fbi .am)
- [ ] ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (shopingchina .net)
- [ ] ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (daj8 .me)
- [ ] ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (github .wiki)
- [ ] ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (whoamis .info)
- [ ] ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (dajuw .com)
- [ ] ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (update .adobe .wiki)
- [ ] ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (linux .wy01 .vip)
- [ ] ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (exmail .googie .com .ph)
- [ ] ET MALWARE Earth Berberoka CnC Domain in DNS Lookup (mmimdown .oss-cn-hongkong .aliyuncs .com)
- [ ] ET MALWARE Earth Berberoka CnC Domain in DNS Lookup
- [x] ET MALWARE UsefulTyphon CnC Activity M1
- [x] ET MALWARE PhantomNet/Smanager Related Domain in DNS Lookup
- [ ] ET MALWARE Kimsuky APT PebbleDash Related Activity (GET)
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M2
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M4
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M6
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M8
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M10
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M12
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M15
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M17
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M19
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M21
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M23
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M25
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M27
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M29
- [x] ET MALWARE PoshC2 - Observed Default URI Structure M31
- [x] ET MALWARE Eternity Stealer Screen Capture Activity
- [ ] ET MALWARE Eternity Stealer CnC Domain in DNS Lookup (wasabiwallet .online)
- [x] ET MALWARE Stonefly APT Related Domain in DNS Lookup (tecnojournals .com)
- [x] ET MALWARE Win32/SilentBreak Related Domain in DNS Lookup (eleed .online)
- [x] ET MALWARE TA452 Related Domain in DNS Lookup
- [x] ET MALWARE TA452 Related Domain in DNS Lookup
- [x] ET MALWARE Win32/Wacatac.B Payload Download
- [x] ET MALWARE Win32/Throwback Server Response (Incoming)
- [x] ET MALWARE Win32/Borr Stealer Variant Sending System Information
- [x] ET MALWARE Win32/SiMay RAT Activity (GET)
- [ ] ET MALWARE Restylink Domain in DNS Lookup (differentfor .com)
- [x] ET MALWARE Restylink Domain in DNS Lookup (disknxt .com)
- [x] ET MALWARE Restylink Domain in DNS Lookup (spffusa .org)
- [x] ET MALWARE Restylink Domain in DNS Lookup (youmiuri .com)
- [ ] ET MALWARE Win32/NetDooka Framework RAT CnC Activity
- [x] ET MALWARE Win32/NetDooka Framework RAT Sending Session ID

- [x] ET MALWARE Win32/NetDooka Framework RAT Sending System Information M1
- [x] ET MALWARE Win32/NetDooka Framework RAT Sending System Information M2
- [x] ET MALWARE Observed PowerShell/CustomRAT Domain (kleinm .de) in TLS SNI
- [x] ET MALWARE Credit Card Scraper Domain in DNS Lookup (authorizen .net)
- [x] ET MALWARE Transparent Tribe APT Related Domain in DNS Lookup
- [x] ET MALWARE DCRat Related CnC Domain in DNS Lookup
- [x] ET MALWARE Observed Malicious SSL Cert (DCRat)
- [x] ET MALWARE oRAT Related CnC Domain in DNS Lookup
- [x] ET MALWARE Bitter APT Related Domain in DNS Lookup (huandocimama .com)
- [x] ET MALWARE Bitter APT Related Activity (GET)
- [x] ET MALWARE J-Spy JSP webshell response
- [x] ET MALWARE Win32/ArtraDownloader CnC Activity (GET)
- [x] ET MALWARE Win32/Vidar Variant/Mars Stealer Resources Download
- [x] ET MALWARE TWISTEDPANDA CnC Domain in DNS Lookup (www .miniboxmail .com)
- [x] ET MALWARE TWISTEDPANDA CnC Domain in DNS Lookup (www .minzdravros .com)
- [x] ET MALWARE Observed TWISTEDPANDA Domain in TLS SNI (www .microtreely .com)
- [x] ET MALWARE Observed TWISTEDPANDA Domain in TLS SNI (img .elliotterusties .com)
- [x] ET MALWARE Win32/Vidar Variant/Mars CnC Activity (GET)
- [x] ET MALWARE Observed Python CTX Library Backdoor Domain (anti-theft-web .herokuapp .com) in TLS SNI
- [x] ET MALWARE Cobalt Strike Related Activity (GET)
- [x] ET MALWARE Cobalt Strike Related Activity (GET)
- [x] ET MALWARE Win32/SiMay RAT Activity M2 (GET)
- [x] ET MALWARE Downloader/Win.MalXll.R466354 Payload Request
- [x] ET MALWARE Patchwork APT Related Activity (POST)
- [ ] ET MALWARE SocGholish Related Domain in DNS Lookup (irsbusinessaudit .net)
- [x] ET MALWARE MSIL/Spy.Agent.CVT CnC Exfil
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (paknavy .comsats .xyz)
- [x] ET MALWARE Tandem Espionage CnC Domain (zpuxmwmwdxxk .ru) in DNS Lookup
- [x] ET MALWARE Tandem Espionage CnC Domain (rwwmefkauiaa .ru) in DNS Lookup
- [x] ET MALWARE Tandem Espionage CnC Domain (sinelnikovd .ru) in DNS Lookup
- [x] ET MALWARE Tandem Espionage CnC Domain (zyzkikpfewuf .ru) in DNS Lookup
- [x] ET MALWARE Tandem Espionage CnC Domain (dwrfqitgvmqn .ru) in DNS Lookup
- [x] ET MALWARE Tandem Espionage CnC Domain (dvizhdom .ru) in DNS Lookup
- [x] ET MALWARE Nim Based Downloader Activity (GET)
- [x] ET MALWARE Ave Maria/Warzone RAT Encrypted CnC Checkin (Inbound)
- [x] ET MALWARE APT SideWinder CnC Domain in DNS Lookup (cdn-in. net)
- [ ] ET MALWARE Suspected BPFDoor UDP Magic Packet (Inbound)
- [ ] ET MALWARE Suspected BPFDoor ICMP Magic Packet (Inbound)
- [x] ET MALWARE Mustang Panda APT PlugX Related Domain in DNS Lookup (hilifimyanmar .com)
- [x] ET MALWARE TA457 Related Activity M2 (POST)
- [x] ET MALWARE Win32/NetDooka Framework RAT Sending File
- [x] ET MALWARE Powershell/CustomRAT CnC Domain in DNS Lookup (kleinm .de)
- [x] ET MALWARE PowerShell/CustomRAT CnC Traffic
- [x] ET MALWARE Cobalt Strike Related Activity (GET)
- [x] ET MALWARE ReVBShell Command Response
- [x] ET MALWARE DCRat Related CnC Domain in DNS Lookup
- [x] ET MALWARE Observed DCRat Related Domain (crystalfiles .ru in TLS SNI)
- [x] ET MALWARE Bitter APT Related Domain in DNS Lookup (emshedulersvc .com)
- [x] ET MALWARE Bitter APT Related Domain in DNS Lookup (diyefosterfeeds .com)
- [x] ET MALWARE Bitter APT Related Activity (GET)
- [x] ET MALWARE J-Spy JSP webshell request
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup
- [x] ET MALWARE TWISTEDPANDA CnC Domain in DNS Lookup (img .elliotterusties .com)
- [x] ET MALWARE TWISTEDPANDA CnC Domain in DNS Lookup (www .microtreely .com)
- [x] ET MALWARE Observed TWISTEDPANDA Domain in TLS SNI (www .miniboxmail .com)
- [x] ET MALWARE Observed TWISTEDPANDA Domain in TLS SNI (www .minzdravros .com)
- [x] ET MALWARE Malicious Rust Crate Related Domain in DNS Lookup (api .kakn .li)
- [x] ET MALWARE Python CTX Library Backdoor Domain in DNS Lookup (anti-theft-web .herokuapp .com)
- [x] ET MALWARE GuLoader Domain in DNS Lookup (zoneofzenith .com)
- [x] ET MALWARE Cobalt Strike Related Activity (GET)
- [x] ET MALWARE Cobalt Strike Related Activity (GET)
- [x] ET MALWARE Patchwork APT Related Domain in DNS Lookup (dayspringdesk .xyz)
- [x] ET MALWARE Gamaredon APT Maldoc Related Activity (GET)
- [x] ET MALWARE Patchwork APT Related Activity M2 (POST)
- [ ] ET MALWARE SocGholish Related Domain in DNS Lookup (irsgetwell .net)
- [x] ET MALWARE Observed DNS Query to bablosoft Domain (downloads .bablosoft .com)
- [x] ET MALWARE Tandem Espionage CnC Domain (cugdwpnykghx .ru) in DNS Lookup
- [x] ET MALWARE Tandem Espionage CnC Domain (rhjebiuujydv .ru) in DNS Lookup
- [x] ET MALWARE Tandem Espionage CnC Domain (sanlygeljek .ru) in DNS Lookup
- [x] ET MALWARE Tandem Espionage CnC Domain (wzqyuwtdxyee .ru) in DNS Lookup
- [x] ET MALWARE Tandem Espionage CnC Domain (ckrddvcveumq .ru) in DNS Lookup
- [x] ET MALWARE Tandem Espionage CnC Domain (aztkiryhetxx .ru) in DNS Lookup
- [x] ET MALWARE Grandoreiro Banking Trojan DGA Domain in DNS Lookup (freedynamicdns. org)
- [x] ET MALWARE Ave Maria/Warzone RAT Encrypted CnC Checkin
- [x] ET MALWARE Pandorahvnc/Pikolo RAT Checkin Activity
- [x] ET MALWARE APT SideWinder CnC Domain in DNS Lookup (cdn-dl. cn)
- [ ] ET MALWARE Suspected BPFDoor TCP Magic Packet (Inbound)
- [x] ET MALWARE Mustang Panda APT PlugX Related Domain in DNS Lookup (myanmarnewsonline .org)
- [x] ET MALWARE TA457 Related Activity (POST)
- [x] ET MALWARE TA457 Related Activity M3 (POST)

- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (chrom3 .net)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (aspbin .net)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (s3-cdn .net)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (tin-url .com)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (gov-pok .net)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (d01fa .net)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (cdn-aws .net)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (cdn-src .net)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (cdn-pak .net)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (ap1-port .net)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (sd1-bin .net)
- [x] ET MALWARE SideWinder APT antibot script
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (docuserve .ltd)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (cvix .live)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (paknvay-pk .net)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (ppinewsagency .live)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (iugur .live)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (mod-pk .com)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (ksew .org)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (bbcnew .cn)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (pakgov .org)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (fdn-trace .net)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (pkrepublic .org)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (int-secure .org)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (gov-mail .net)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (pak-web .com)
- [x] ET MALWARE DOUBLEBACK CnC Activity
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [ ] ET MALWARE Polonium CreepyDrive Upload Request
- [ ] ET MALWARE Polonium CreepyDrive Client CnC Response
- [x] ET MALWARE Observed Malicious SSL Cert (Darkme CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (Darkme CnC)
- [x] ET MALWARE Win32/Darkme Trojan Checkin M2
- [x] ET MALWARE Win32/Darkme CnC Domain in DNS Lookup (pallomnareraebrazo .com)
- [x] ET MALWARE Win32/Darkme CnC Domain in DNS Lookup (8as1s2 .com)
- [x] ET MALWARE Win32/Darkme CnC Domain in DNS Lookup (kalpoipolpmi .net)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (pakgov .net)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (cdn-edu .net)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (bitlyy .me)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (nrots .net)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (govpk-mail .net)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (kdf-mail .com)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (cdn-top .net)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (filesrvr .net)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (dawnpk .org)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (vpn-secure .co)
- [x] ET MALWARE Suspected Sidewinder APT Phishing Activity - Landing Page URI Pattern
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (paf-gov .net)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (fileserve .work)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (edu-cx .org)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (ministry-pk .net)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (cr20g .org)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (moma-pk .org)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (cloud-apt .net)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (bahariafoundation .org)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (pak-gov .com)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (csd-pk .co)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (pakmarines .com)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (pafwa .info)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (kpt-pk .net)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (krlwin .org)
- [x] ET MALWARE Observed DOUBLEBACK CnC Domain (bestcake .ca in TLS SNI)
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [ ] ET MALWARE Polonium CreepyDrive Implant Request
- [x] ET MALWARE Polonium CreepyDrive Download Request
- [x] ET MALWARE TA401 Arid Viper CnC Domain in DNS Lookup (sknzy-mysl .vip)
- [x] ET MALWARE Observed Malicious SSL Cert (Darkme CnC)
- [x] ET MALWARE Win32/Darkme Trojan Checkin M1
- [x] ET MALWARE Win32/Darkme CnC Domain in DNS Lookup (muasaashshaj .com)
- [x] ET MALWARE Win32/Darkme CnC Domain in DNS Lookup (aka7newmalp23 .com)
- [x] ET MALWARE Win32/Darkme CnC Domain in DNS Lookup (938jss .com)
- [x] ET MALWARE Win32/Darkme CnC Domain in DNS Lookup (cspapop110 .com)

- [x] ET MALWARE Win32/Darkme CnC Domain in DNS Lookup (csmmmsp099q .com)
- [x] ET MALWARE Deathstalker/Evilnum Delivery Domain in DNS Lookup (puccino .altervista .org)
- [x] ET MALWARE Deathstalker/Evilnum Delivery Domain in DNS Lookup (storangefilecloud .vip)
- [x] ET MALWARE Deathstalker/Evilnum Delivery Domain (puccino .altervista .org) in TLS SNI
- [x] ET MALWARE WatchDog Coinminer Payload Delivery Domain in DNS Lookup (oracle .zzhreceive .top)
- [x] ET MALWARE Win32/SVCReady Loader CnC Activity
- [x] ET MALWARE PlugX CnC Beacon
- [x] ET MALWARE Gh0st RAT Backdoor Checkin
- [x] ET MALWARE Win32/SVCReady Loader - Logs
- [x] ET MALWARE Win32/SVCReady Loader - SysInfo M2
- [x] ET MALWARE Transparent Tribe APT Related Backdoor Receiving Command (Inbound)
- [x] ET MALWARE Earth Berberoka Domain in DNS Lookup
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [x] ET MALWARE Generic Stealer Config Download Request
- [x] ET MALWARE Observed Malicious SSL/TLS Certificate (APT-C-55/ BabyShark Staging Domain)
- [x] ET MALWARE Observed Malicious SSL/TLS Certificate (APT-C-55/ BabyShark Staging Domain)
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE TA401 Arid Viper Related Activity (POST)
- [x] ET MALWARE njRAT v65.0 CnC Checkin
- [x] ET MALWARE APT-Q-37/Manling Flower Payload - CnC Checkin
- [x] ET MALWARE Kinsing Botnet Related Domain in DNS Lookup (blacknurse .lib)
- [x] ET MALWARE Kinsing Botnet Related Domain in DNS Lookup (babaroga .lib)
- [x] ET MALWARE Suspected APT-Q-37 Related Activity (Outbound)
- [x] ET MALWARE Symbiote CnC Domain in DNS Lookup (assets .fans)
- [x] ET MALWARE Symbiote CnC Domain in DNS Lookup (bancodobrasil .dev)
- [x] ET MALWARE Symbiote CnC Domain in DNS Lookup (caixa .wf)
- [x] ET MALWARE Win32/Gomorrah Stealer Data Exfiltration
- [ ] ET MALWARE Win32.Stealer CnC Domain in DNS Lookup (kealkun .16mb .com)
- [x] ET MALWARE Trojan-PSW.Win32.Stealer.sb CnC
- [x] ET MALWARE MegalodonHTTP/LuciferHTTP/Gomorrah Client Action M2
- [ ] ET MALWARE Aoqin Dragon APT Related Activity (GET)
- [x] ET MALWARE PingPull Related Activity (POST)
- [x] ET MALWARE Gallium APT Related Domain in DNS Lookup (micfkbeljacob .com)
- [x] ET MALWARE PingPull ICMP Activity M2 (Outbound)
- [x] ET MALWARE Loxes/Mongall Related CnC Beacon (GET)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (navy-mil-bd .jmicc .xyz)
- [x] ET MALWARE Deathstalker/Evilnum Delivery Domain in DNS Lookup (bukjut11 .com)
- [ ] ET MALWARE Deathstalker/Evilnum Delivery Domain in DNS Lookup (1b)
- [x] ET MALWARE Deathstalker/Evilnum Delivery Domain (bukjut11 .com) in TLS SNI
- [x] ET MALWARE Deathstalker/Evilnum Delivery Domain (storangefilecloud .vip) in TLS SNI
- [x] ET MALWARE Observed Win32/SVCReady Loader User-Agent
- [x] ET MALWARE Win32/SVCReady Loader Requesting Payload
- [x] ET MALWARE W32/Quasar 1.3/Venom RAT Connectivity Check 2
- [x] ET MALWARE Win32/SVCReady Loader CnC Activity M2
- [x] ET MALWARE Win32/SVCReady Loader - SysInfo M1
- [x] ET MALWARE Win32/SVCReady Loader - Screenshot
- [x] ET MALWARE Transparent Tribe APT Related Backdoor Sending System Information
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (nod-update .it)
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [x] ET MALWARE Generic Stealer Config from Server
- [x] ET MALWARE Observed Malicious SSL/TLS Certificate (APT-C-55/ BabyShark Staging Domain)
- [x] ET MALWARE Observed Malicious SSL/TLS Certificate (APT-C-55/ BabyShark Staging Domain)
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE Observed DNS Query to TA455 Domain
- [x] ET MALWARE GoLang Popping Eagle Trojan Related Activity (POST)
- [x] ET MALWARE Win32/RecordBreaker CnC Checkin M1
- [x] ET MALWARE ELF/Mirai Variant Activity (Outbound)
- [x] ET MALWARE Kinsing Botnet Related Domain in DNS Lookup (dragon .lib)
- [x] ET MALWARE Kinsing Botnet Related Domain in DNS Lookup (tempest .lib)
- [x] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [x] ET MALWARE Symbiote CnC Domain in DNS Lookup (dpf .fm)
- [x] ET MALWARE Symbiote CnC Domain in DNS Lookup (caixa .cx)
- [x] ET MALWARE Win32/RecordBreaker CnC Checkin - Server Response
- [x] ET MALWARE Win32/Agent.Fish Data Exfiltration
- [ ] ET MALWARE Win32.Stealer CnC Domain in DNS Lookup (ping .otwalkun .16mb .com)
- [x] ET MALWARE Win32.Agent.kawe SMTP Stealer
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (bahriafoundation .live)
- [x] ET MALWARE PingPull ICMP Activity (Outbound)
- [x] ET MALWARE Gallium APT Related Domain in DNS Lookup (hinitial .com)
- [x] ET MALWARE PingPull Related Activity (Outbound)
- [ ] ET MALWARE Aoqin Dragon APT Related Activity (GET)
- [x] ET MALWARE Loxes/Mongall Related CnC Beacon M2 (GET)
- [ ] ET MALWARE Loxes/Mongall Related CnC Beacon M3 (GET)

- [x] ET MALWARE MalDoc Retrieving Qbot Payload 2022-06-14
- [ ] ET MALWARE Observed DNS Query to Maldoc Domain (sportpony .ch)
- [ ] ET MALWARE Observed DNS Query to Maldoc Domain (procoach .jp)
- [ ] ET MALWARE Observed DNS Query to Maldoc Domain (regenerationcongo .com)
- [x] ET MALWARE Suspected Gamaredon APT Related Activity (GET)
- [x] ET MALWARE APT/Bitter CnC Exfiltration via TCP
- [x] ET MALWARE Maldoc Retrieving Payload 2022-06-15
- [ ] ET MALWARE Maldoc Retrieving Payload 2022-06-15
- [x] ET MALWARE Win32/Tiggre!rfn Zipped Exfil
- [x] ET MALWARE Base64 Encoded Windows Command Prompt (Outbound)
- [x] ET MALWARE Suspected Cobalt Strike Beacon User-Agent String
- [x] ET MALWARE Win32/Criminal RAT CnC Checkin
- [ ] ET MALWARE Win32.Banker Trojan CnC Checkin
- [x] ET MALWARE CopperStealer - Remote Desktop - CnC Server Request via Pastebin
- [x] ET MALWARE CopperStealer - Remote Desktop - Initial Checkin
- [x] ET MALWARE Win32/TrojanDownloader.Agent.FLZ CnC Activity
- [x] ET MALWARE Unknown CN Related APT Activity (GET)
- [x] ET MALWARE Win32/IceXLoader Sending Initial Checkin (POST)
- [x] ET MALWARE Win32/IceXLoader Sending System Information (POST)
- [x] ET MALWARE Win64/Agent.BP System Info Exfil
- [x] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [x] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [x] ET MALWARE CN Based APT Related Domain in DNS Lookup (open .zerdeopen .top)
- [x] ET MALWARE TA459 Related Activity (Inbound)
- [x] ET MALWARE Win32/Unknown Stealer Command (filegrab) (Outbound)
- [x] ET MALWARE Win32/Unknown Stealer Command (domaindetect) (Outbound)
- [x] ET MALWARE Win32/Unknown Stealer CnC Log Exfil
- [x] ET MALWARE Win32/APT28 Host Fingerprint Exfiltration via IMAP
- [x] ET MALWARE SharpPanda APT Activity (GET)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (mailh .alit .live)
- [x] ET MALWARE Win32/Matanbuchus Loader Related Domain in DNS Lookup (collectiontelemetrysystem .com)
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (extic .icu)
- [x] ET MALWARE Win32/Delf.TJJ CnC Checkin M2
- [x] ET MALWARE Win32/Delf.TJJ CnC Domain in DNS Lookup (udo .jxwan .com)
- [x] ET MALWARE Win32/Delf.TJJ CnC Domain in DNS Lookup (wx .go890 .com)
- [x] ET MALWARE Win32/Delf.TJJ CnC Domain in DNS Lookup (bk .957wan .com)
- [x] ET MALWARE Win32/Delf.TJJ CnC Domain in DNS Lookup (cnwx .58ad .cn)
- [x] ET MALWARE Win32/Delf.TJJ CnC Domain in DNS Lookup (cmps .58sky .com)
- [x] ET MALWARE ToddyCat Ninja Backdoor CnC
- [x] ET MALWARE DonotGroup APT Related Domain in DNS Lookup (who .worksolution .buzz)
- [x] ET MALWARE Win32/Wacatac Ransomware Variant Retrieving File (GET)
- [x] ET MALWARE DarkCrystal Rat Stealer Data Exfiltration Activity
- [x] ET MALWARE Win32/Ymacco.AA60 Checkin
- [x] ET MALWARE ZuoRAT send_http_msg_php Call to ssid.php
- [x] ET MALWARE ZuoRAT send_http_msg_php Call to arp.php
- [x] ET MALWARE ZuoRAT CBeacon CnC
- [x] ET MALWARE Observed DNS Query to Maldoc Domain (webnar .info)
- [ ] ET MALWARE Observed DNS Query to Maldoc Domain (spprospekt .com .br)
- [ ] ET MALWARE Observed DNS Query to Maldoc Domain (suidi .com)
- [x] ET MALWARE Win32/Upgilf CnC Beacon
- [x] ET MALWARE Loxes/Mongall Related CnC Beacon M4 (GET)
- [ ] ET MALWARE Panchan Mining Rig CnC Activity (Inbound)
- [ ] ET MALWARE Maldoc Retrieving Payload 2022-06-15
- [x] ET MALWARE Win32/Grandoreiro Loader Checkin Activity (POST)
- [x] ET MALWARE TA457 Backdoor CnC Response
- [x] ET MALWARE TA457 Backdoor CnC Activity
- [x] ET MALWARE Win32/MassLogger FTP Data Exfiltration
- [x] ET MALWARE Win32.Zegost CnC Checkin
- [x] ET MALWARE CopperStealer - Browser Stealer Exfil via Telegram
- [x] ET MALWARE CopperStealer - Remote Desktop - CnC Server Response via Pastebin
- [x] ET MALWARE CopperStealer - Remote Desktop - Task Request
- [x] ET MALWARE Unknown CN Related APT Domain in DNS Lookup (upportteam .lingrevelat .com)
- [x] ET MALWARE System Information Being Sent in User-Agent
- [x] ET MALWARE Win32/IceXLoader Sending Command Acknowledgement (POST)
- [x] ET MALWARE Win64/Agent.BP Checkin
- [x] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [x] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [x] ET MALWARE CN Based APT Related Activity (POST)
- [x] ET MALWARE CN Based APT Related Domain in DNS Lookup (sign .sanaqsign .org)
- [x] ET MALWARE Konni APT MalDoc Activity (GET)
- [x] ET MALWARE Win32/Unknown Stealer Command (loader) (Outbound)
- [x] ET MALWARE Win32/Unknown Stealer Command (geoblock) (Outbound)
- [x] ET MALWARE Win32/Unknown Stealer Command Response (filegrab) (Inbound)
- [x] ET MALWARE [Akamai] Panchan Miner Botnet Checkin
- [x] ET MALWARE Cobalt Strike Malleable C2 Amazon Profile Variant (GET)
- [x] ET MALWARE Win32/Agent.RDE Checkin
- [x] ET MALWARE Win32/Matanbuchus Loader Related Domain in DNS Lookup (telemetrysystemcollection .com)
- [x] ET MALWARE Win32/Delf.TJJ CnC Checkin M1
- [x] ET MALWARE Win32/Delf.TJJ CnC Domain in DNS Lookup (ysl .jxwan .com)
- [x] ET MALWARE Win32/Delf.TJJ CnC Domain in DNS Lookup (dsk .5636 .com)
- [x] ET MALWARE Win32/Delf.TJJ CnC Domain in DNS Lookup (cfg .jipinwan .com)
- [x] ET MALWARE Win32/Delf.TJJ CnC Domain in DNS Lookup (www .58sky .com)
- [x] ET MALWARE Win32/Delf.TJJ CnC Domain in DNS Lookup (gc .wb51 .com)
- [x] ET MALWARE ToddyCat Ninja Backdoor CnC Domain in DNS Lookup (eohsdnsaaojrhnqo .windowshost .us)
- [ ] ET MALWARE DonotGroup Maldoc Activity (GET)
- [x] ET MALWARE DonotGroup APT Related Domain in DNS Lookup (rus .feedpolicy .xyz)
- [ ] ET MALWARE Observed DNS Query to DarkCrystal Rat Domain (datagroup .ddns .net) (2022-06-27)
- [x] ET MALWARE Observed DNS Query to Win32/TrojanDropper.Agent.SLC Domain
- [x] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [x] ET MALWARE ZuoRAT send_http_msg_php Call to dns.php
- [x] ET MALWARE ZuoRAT Windows Loader Shellcode Retrieval
- [x] ET MALWARE ZuoRAT GoBeacon CnC

- [x] ET MALWARE Win32/CHAOS RAT/AlfaC2 Checkin
- [x] ET MALWARE EvilNum APT Related Domain in DNS Lookup (bookaustriavisit .com)
- [x] ET MALWARE EvilNum APT Related Domain in DNS Lookup (pcamanalytics .com)
- [x] ET MALWARE EvilNum APT Related Domain in DNS Lookup (imageztun .com)
- [x] ET MALWARE Cobalt Strike Malleable C2 JQuery Custom Profile M6
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (MageCart Payload CnC)
- [x] ET MALWARE LinPEAS Privilege Escalation Script Response (With Banner)
- [x] ET MALWARE SilentLibrarian Domain in DNS Lookup (login .cardiff .acuk .me)
- [x] ET MALWARE Troj_Yahoya Variant CnC Checkin
- [x] ET MALWARE Win32/Wacatac.B!ml CnC Checkin
- [x] ET MALWARE MSIL/PSW.Agent.SUD Zipped Data Exfil (set)
- [x] ET MALWARE Golang/Kaos/YamaBot CnC Activity
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [x] ET MALWARE Win32/Remcos RAT Checkin 809
- [x] ET MALWARE Golang/Kaos/YamaBot CnC Activity M2 (POST)
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [x] ET MALWARE Win32/RecordBreaker Checkin M2
- [x] ET MALWARE Lazarus APT Related VSingle Backdoor Activity (GET)
- [x] ET MALWARE Observed Malicious SSL Cert (Microsoft Security localhost)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (bitsbfree .com)
- [x] ET MALWARE TA471/UNC2589 Related Domain in DNS Lookup (skreatortemp .site)
- [x] ET MALWARE Bitter APT AlmondRAT CnC Checkin
- [x] ET MALWARE Bitter APT Domain in DNS Lookup (huandocimama .com)
- [x] ET MALWARE CN Based APT Related Domain in DNS Lookup (supportteam .lingrevelat .com)
- [x] ET MALWARE CN Based APT Related Domain in DNS Lookup (instructor .giize .com)
- [x] ET MALWARE MSIL/Spy.Agent.AES Zipped Exfil
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [x] ET MALWARE HiveRAT CnC Activity M2
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (syriahr .eu)
- [x] ET MALWARE NoMercy Data Exfiltration M1
- [x] ET MALWARE X-Files Stealer CnC Exfil Activity M2
- [x] ET MALWARE MSIL/PSW.Discord.AIY CnC Exfil
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [x] ET MALWARE Win32/HackTool.Agent.CS SMTP activity
- [x] ET MALWARE Possible Raspberry Robin Activity (GET)
- [x] ET MALWARE Win32/H0lyGh0st Ransomware CnC Activity (GET Public Key)
- [x] ET MALWARE Win32/H0lyGh0st Ransomware CnC Response
- [x] ET MALWARE Possible Compromised Host AnubisNetworks Sinkhole Cookie Value btst
- [x] ET MALWARE Win32/Wacapew CnC Checkin
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [x] ET MALWARE PlugX Related Domain in DNS Lookup (wpsup .daj8 .me)
- [x] ET MALWARE Win32/Sality.NBA CnC Checkin
- [x] ET MALWARE ChromeLoader Activity (GET)
- [ ] ET MALWARE APT29/CloakedUrsa Related Domain in DNS Lookup (crossfity .com)
- [x] ET MALWARE Win32/Wacapew.C!ml Checkin
- [x] ET MALWARE EvilNum APT Related Domain in DNS Lookup (msdllopt .com)
- [x] ET MALWARE EvilNum APT Related Domain in DNS Lookup (estimefm .org)
- [x] ET MALWARE ShadowPad Backdoor Related Domain in DNS Lookup (grandfoodtony .com)
- [x] ET MALWARE Win32/a310Logger Variant Data Exfil via SMTP
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (MageCart Payload CnC)
- [x] ET MALWARE LinPEAS Privilege Escalation Script Response (Without Banner)
- [x] ET MALWARE Observed Malicious SSL Cert (SilentLibrarian)
- [x] ET MALWARE Win32/Fynloski.AA CnC Checkin
- [x] ET MALWARE Win32/Wacatac.B!ml Data Exfiltration
- [x] ET MALWARE MSIL/PSW.Agent.SUD Zipped Data Exfil
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [x] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [x] ET MALWARE Win32/Remcos RAT Checkin 810
- [x] ET MALWARE Generic CMD Remote Shell
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [x] ET MALWARE BluStealer - SysInfo Exfil via Telegram M2
- [x] ET MALWARE Lazarus APT Related Valefor/VSingle CnC Beacon
- [x] ET MALWARE Lazarus APT Related Domain in DNS Lookup (ougreen .com)
- [x] ET MALWARE Suspected Brute Ratel CnC Activity (POST)
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [x] ET MALWARE Win32/TrojanDownloader.AutoHK.MT CnC Checkin
- [x] ET MALWARE Bitter APT ZxxZ Downloader CnC Checkin
- [x] ET MALWARE TontoTeam APT Related Bisonal CnC Activity
- [x] ET MALWARE CN Based APT Related Domain in DNS Lookup (news .wooordhunts .com)
- [x] ET MALWARE MSIL/PSW.Agent.RXP Checkin
- [x] ET MALWARE MSIL/Spy.Agent.DYS Exfil
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [x] ET MALWARE NoMercy Stealer CnC Checkin
- [x] ET MALWARE NoMercy Data Exfiltration M2
- [x] ET MALWARE Cobalt Strike Related Activity (GET)
- [x] ET MALWARE MSIL/Agent.CTK Checkin
- [x] ET MALWARE Win32/HackTool.Agent.CS SMTP Scanner CnC Checkin
- [x] ET MALWARE Win64/Agent.qwiakk CnC Checkin
- [x] ET MALWARE Unknown APT Related Domain in DNS Lookup
- [x] ET MALWARE Win32/H0lyGh0st Ransomware Exfil Activity (POST)
- [x] ET MALWARE JS/TrojanDropper.Agent.OHE CnC Checkin
- [x] ET MALWARE Win32/H0lyGh0st CnC Activity
- [x] ET MALWARE Win32/Wacapew.C!ml CnC Checkin
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [x] ET MALWARE PlugX Related Domain in DNS Lookup (wps .daj8 .me)
- [ ] ET MALWARE JS.SocGholish CnC Activity (POST)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (ksew .kpt-gov .org)
- [ ] ET MALWARE APT29/CloakedUrsa Related Domain in DNS Lookup (techspaceinfo .com)

- [x] ET MALWARE APT29/CloakedUrsa Google Drive Authentication (POST)
- [x] ET MALWARE Win32/MSIL.Heracles Checkin
- [x] ET MALWARE Ave Maria/Warzone RAT Encrypted CnC Checkin (Inbound)
- [x] ET MALWARE TA444 Related Domain in DNS Lookup (fclouddown .co)
- [x] ET MALWARE Win32/Shrine.A CnC Checkin
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [x] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (paf-gov .org)
- [x] ET MALWARE MSIL/Spy.Agent.CSS Exfil
- [x] ET MALWARE Win32/Loli Stealer CnC Activity
- [ ] ET MALWARE 8220 Gang Related Domain in DNS Lookup (letmaker .top)
- [x] ET MALWARE VBS/Agent.6B29!tr CnC Checkin
- [x] ET MALWARE Win32/Kryptik.GSKY CnC Checkin
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [x] ET MALWARE Gamaredon APT Related Activity (GET)
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [x] ET MALWARE Win32/VB.NBI CnC Checkin
- [x] ET MALWARE Win32/SuperBOT CnC Checkin
- [x] ET MALWARE W32.DarkVNC Variant Checkin
- [x] ET MALWARE Observed Cobalt Strike Domain (zuyonijobo .com) in TLS SNI
- [x] ET MALWARE IIS Backdoor CnC Command Inbound
- [x] ET MALWARE Win32/SystemHijack.gen CnC Checkin
- [x] ET MALWARE RKO Remote File Upload Attempt
- [x] ET MALWARE Win32/VBS.Sload Activity (GET)
- [x] ET MALWARE TA444 Related Domain in DNS Lookup (inst .shconstmarket .com)
- [x] ET MALWARE TA444 Related Domain in DNS Lookup (wordonline .cloud)
- [x] ET MALWARE W32/CoinMiner.ESJ!tr CnC Domain (ui .0x0x0x0x0 .xyz) in DNS Lookup
- [x] ET MALWARE W32/CoinMiner.ESJ!tr CnC Domain (aj .0x0x0x0x0 .best) in DNS Lookup
- [x] ET MALWARE W32/CoinMiner.ESJ!tr CnC Domain (qb .1c1c1c1c .best) in DNS Lookup
- [x] ET MALWARE Win32/Agent.TWI CnC Checkin
- [x] ET MALWARE Observed DNS Query to Known Knotweed/SubZero Domain
- [x] ET MALWARE Observed DNS Query to Known Knotweed/SubZero Domain
- [x] ET MALWARE Observed DNS Query to Known Knotweed/SubZero Domain
- [x] ET MALWARE Ave Maria/Warzone RAT Credential Exfil
- [x] ET MALWARE ENV Variable Data Exfiltration Domain (ovz1 .j19544519 .pr46m .vps .myjino .ru) in DNS Lookup
- [x] ET MALWARE RedGuard Framework Related Request Activity
- [x] ET MALWARE SSL/TLS Certificate Observed (Link Implant Default)
- [x] ET MALWARE Lazarus APT Related Domain in DNS Lookup (mktrending .com)
- [x] ET MALWARE Woody RAT CnC Domain (oakrussia .ru) in DNS Lookup
- [x] ET MALWARE Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup
- [x] ET MALWARE Woody RAT Payload Delivery Domain (garmandesar .duckdns .org) in DNS Lookup
- [x] ET MALWARE Woody RAT CnC Checkin
- [x] ET MALWARE CHIMNEYSWEEP Backdoor CnC Domain (windowsupadates .com) in DNS Lookup
- [ ] ET MALWARE HTML/TrojanDropper.Agent.T Payload Inbound
- [x] ET MALWARE Win32/Stealerium Stealer Checkin via Discord
- [x] ET MALWARE TA444 Related Domain in DNS Lookup (documentworkspace .io)
- [x] ET MALWARE TA444 Related Domain in DNS Lookup (googlesheet .info)
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [x] ET MALWARE Bitter APT Payload Request
- [x] ET MALWARE Downloaded .PNG With Embedded File (.sh)
- [x] ET MALWARE Loli Stealer CnC Domain in DNS Lookup (webstealer .ru)
- [ ] ET MALWARE 8220 Gang Related Domain in DNS Lookup (onlypirate .top)
- [ ] ET MALWARE 8220 Gang Related Domain in DNS Lookup (oracleservice .top)
- [x] ET MALWARE Unknown Maldoc CnC Activity (2022-07-25)
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [ ] ET MALWARE Observed Malicious SSL/TLS Certificate (SilentLibrarian)
- [x] ET MALWARE Gamaredon APT Related Activity (GET)
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [x] ET MALWARE Win32/VB.QPK CnC Checkin
- [x] ET MALWARE Win32/Sabsik.TE.B!ml CnC Checkin
- [x] ET MALWARE Win32/Unknown VBScript Backdoor Activity (GET)
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (zuyonijobo .com)
- [x] ET MALWARE Cobalt Strike Malleable C2 Beacon (Custom)
- [x] ET MALWARE MSIL/Filecoder.EK CnC Checkin
- [x] ET MALWARE Trojan.Dropper.HTML.Agent Payload
- [x] ET MALWARE Win32/Small.NMZ CnC Checkin
- [x] ET MALWARE Gamaredon APT Related Activity (GET)
- [x] ET MALWARE TA444 Related Domain in DNS Lookup (web .shconstmarket .com)
- [x] ET MALWARE Manjusaka CnC Server Response
- [x] ET MALWARE W32/CoinMiner.ESJ!tr CnC Domain (rp .oiwcvbnc2e .stream) in DNS Lookup
- [x] ET MALWARE W32/CoinMiner.ESJ!tr CnC Domain (xs .0x0x0x0x0 .club) in DNS Lookup
- [x] ET MALWARE W32/CoinMinerESJ!tr CnC Domain (ox .mygoodluck .best) in DNS Lookup
- [x] ET MALWARE Observed Malicious SSL/TLS Certificate (Knotweed/SubZero)
- [x] ET MALWARE Observed Malicious SSL/TLS Certificate (Knotweed/SubZero)
- [x] ET MALWARE Observed Malicious SSL/TLS Certificate (Knotweed/SubZero)
- [x] ET MALWARE Suspected BTC Swapper Activity (GET)
- [x] ET MALWARE Possible T-RAT Encrypted Zip Request M2
- [x] ET MALWARE ENV Variable Data Exfiltration Attempt (HTTP POST)
- [x] ET MALWARE Observed Malicious SSL Cert (RedGuard Framework)
- [x] ET MALWARE Link Implant CnC Activity (POST)
- [x] ET MALWARE Woody RAT CnC Domain (microsoft-telemetry .ru) in DNS Lookup
- [x] ET MALWARE Woody RAT CnC Domain (kurmakata .duckdns .org) in DNS Lookup
- [x] ET MALWARE Woody RAT CnC Domain (fns77 .ru) in DNS Lookup
- [x] ET MALWARE Woody RAT Payload Delivery Domain (fcloud .nciinform .ru) in DNS Lookup
- [x] ET MALWARE CHIMNEYSWEEP Backdoor CnC Domain (pgp .eu .com) in DNS Lookup
- [x] ET MALWARE CHIMNEYSWEEP Backdoor CnC Domain (skype .se .net) in DNS Lookup

- [x] ET MALWARE CHIMNEYSWEEP Backdoor CnC Domain (telegram-update .com) in DNS Lookup
- [x] ET MALWARE CHIMNEYSWEEP Backdoor CnC Domain (server-avira .com) in DNS Lookup
- [x] ET MALWARE CHIMNEYSWEEP Backdoor CnC Domain (uk2privat .com) in DNS Lookup
- [x] ET MALWARE CHIMNEYSWEEP Backdoor CnC Domain (update-real .com) in DNS Lookup
- [x] ET MALWARE Win64/Spy.Agent.EU CnC Checkin
- [x] ET MALWARE SHARPEXT CnC Domain in DNS Lookup (gonamod .com)
- [x] ET MALWARE Lazarus APT Related Activity (GET)
- [x] ET MALWARE ELF/RapperBot CnC Checkin M2
- [x] ET MALWARE CosmicStrand Rootkit Related Domain in DNS Lookup (update .bokts .com)
- [x] ET MALWARE Win32/ErbiumStealer Panel CnC Checkin
- [x] ET MALWARE Win32/RA-based.NCX CnC Checkin
- [x] ET MALWARE Win32/RecordBreaker - Observed UA M2
- [x] ET MALWARE Observed DNS Query to ROMCOM RAT Domain (combinedresidency .org)
- [x] ET MALWARE Win32/Korplug.HQ CnC Activity
- [x] ET MALWARE Win32/Lilith Stealer registerBot CnC Checkin
- [x] ET MALWARE Win32/Lilith Stealer uploadFile Data Exfiltration Attempt
- [x] ET MALWARE Win.Backdoor.Kolobko-9950676-0 Retrieving CnC Commands
- [x] ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (ciscovpn2 .com)
- [x] ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (cisco-helpdesk .cf)
- [x] ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (mycisco .cf)
- [x] ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (devcisco .com)
- [x] ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (cisco-help .cf)
- [x] ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (helpzonecisco .com)
- [x] ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (kazaboldu .net)
- [x] ET MALWARE Arkei/Vidar/Mars Stealer Variant DLL GET Request
- [ ] ET MALWARE Win32/CopperStealer CnC Domain (ec083aa56dc0449a .com) in DNS Lookup
- [x] ET MALWARE Shuckworm CnC Domain (leonardis .ru) in DNS Lookup
- [x] ET MALWARE Shuckworm/Gamaredon CnC Domain (heato .ru) in DNS Lookup
- [x] ET MALWARE Shuckworm CnC Domain (a0698649 .xsph .ru) in DNS Lookup
- [x] ET MALWARE RShell Backdoor Keepalive
- [x] ET MALWARE RShell CnC Domain (time .ntp-server .asia) in DNS Lookup
- [x] ET MALWARE RShell Backdoor Initial CnC Checkin
- [x] ET MALWARE Observed DNS Query to TA444 Domain (cooporatestock .com)
- [x] ET MALWARE Observed DNS Query to TA444 Domain (1drvmicrosoft .com)
- [x] ET MALWARE Observed DNS Query to TA444 Domain (globiscapital .co)
- [ ] ET MALWARE Win32/GRAT2 Client Data Exfil
- [x] ET MALWARE Observed DNS Query to UNC3890 Domain (naturaldolls .store)
- [x] ET MALWARE Observed DNS Query to UNC3890 Domain (xxx-doll .com)
- [x] ET MALWARE Observed DNS Query to UNC3890 Domain (office365update .live)
- [x] ET MALWARE CargoBay User-Agent
- [x] ET MALWARE CHIMNEYSWEEP Backdoor CnC Domain (update-pgp .com) in DNS Lookup
- [x] ET MALWARE CHIMNEYSWEEP Backdoor CnC Domain (avira .ltd) in DNS Lookup
- [x] ET MALWARE CHIMNEYSWEEP Backdoor CnC Domain (cloud-avira .com) in DNS Lookup
- [x] ET MALWARE Win32/Agent.UOI CnC Checkin
- [x] ET MALWARE Win32.ClipBanker.uhn Exfil
- [x] ET MALWARE SHARPEXT CnC Domain in DNS Lookup (siekis .com)
- [x] ET MALWARE ELF/RapperBot CnC Checkin M1
- [ ] ET MALWARE Patchwork APT Related Activity M3 (POST)
- [x] ET MALWARE Observed DNS Query to ErbiumStealer Domain (erbium .ml)
- [x] ET MALWARE Win32/ErbiumStealer CnC Activity (GetBuild)
- [x] ET MALWARE Win32/RecordBreaker - Observed UA M1
- [x] ET MALWARE Win32/RecordBreaker - Library Request
- [x] ET MALWARE Observed DNS Query to ROMCOM RAT Domain (optasko .com)
- [x] ET MALWARE Win32/Lilith Stealer getFile Command
- [x] ET MALWARE Win32/Lilith Stealer getCommands Command
- [x] ET MALWARE Win32/Packed.BlackMoon.A CnC Checkin
- [x] ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (mycisco-helpdesk .ml)
- [x] ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (primecisco .com)
- [x] ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (ciscovpn1 .com)
- [x] ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (pwresetcisco .com)
- [x] ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (ciscovpn3 .com)
- [x] ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (mycisco .gq)
- [x] ET MALWARE Observed DNS Query to Win.Backdoor.Kolobko Domain in DNS Lookup (devciscoprograms .com)
- [x] ET MALWARE Arkei/Vidar/Mars Stealer Variant CnC checkin commands
- [x] ET MALWARE Arkei/Vidar/Mars Stealer Variant Data Exfiltration Attempt
- [x] ET MALWARE Win32/VB.QTV CnC Checkin
- [x] ET MALWARE Shuckworm CnC Domain (destroy .asierdo .ru) in DNS Lookup
- [x] ET MALWARE Shuckworm/Gamaredon CnC Domain (motoristo .ru) in DNS Lookup
- [x] ET MALWARE Shuckworm/Gamaredon CnC Domain (pasamart .ru) in DNS Lookup
- [x] ET MALWARE RShell CnC Domain (linux .updatelive-oline .com) in DNS Lookup
- [x] ET MALWARE RShell CnC Domain (center .veryssl .org) in DNS Lookup
- [ ] ET MALWARE Win32/GRAT2 Client CnC Checkin
- [x] ET MALWARE Observed DNS Query to TA444 Domain (finxiio .com)
- [x] ET MALWARE Observed DNS Query to TA444 Domain (ledger-cloud .com)
- [x] ET MALWARE Observed DNS Query to TA444 Domain (wpsonline .co)
- [x] ET MALWARE Observed DNS Query to UNC3890 Domain (pfizerpoll .com)
- [x] ET MALWARE Observed DNS Query to UNC3890 Domain (rnfacebook .com)
- [x] ET MALWARE Observed DNS Query to UNC3890 Domain (celebritylife .news)
- [x] ET MALWARE Observed DNS Query to UNC3890 Domain (fileupload .shop)
- [x] ET MALWARE Shuckworm Backdoor Screenshot Upload Attempt

- [x] ET MALWARE JSSLoader CnC Domain (essentialsmassageanddayspa .com) in DNS Lookup
- [x] ET MALWARE JSSLoader Initial Checkin
- [x] ET MALWARE Successful CargoBay Exfil
- [ ] ET MALWARE DonotGroup APT Related Domain in DNS Lookup (clipboardgames .xyz)
- [ ] ET MALWARE DonotGroup APT Related Domain in DNS Lookup (globalseasurfer .xyz)
- [ ] ET MALWARE DonotGroup APT Related Domain in DNS Lookup (doctorstrange .buzz)
- [x] ET MALWARE DonotGroup APT Related Domain in DNS Lookup (beetelson .xyz)
- [x] ET MALWARE DonotGroup APT Related Domain in DNS Lookup (kotlinn .xyz)
- [x] ET MALWARE Suspected VileRAT Related Request Activity (GET)
- [x] ET MALWARE TA453/CharmingKitten HYPERSCRAPE Tool Identity Check Activity (GET)
- [x] ET MALWARE Trojan:Win32/WinLNK.APA!MTB Payload Request
- [x] ET MALWARE Confucious APT Related Domain in DNS Lookup (viterwin .club)
- [x] ET MALWARE HTTPRevShell Initial CnC Checkin
- [x] ET MALWARE Possible OSX/SHLAYER Checkin M2
- [x] ET MALWARE Win32/Grandoreiro Sending System Information (POST)
- [x] ET MALWARE Win32/Filecoder.GC CnC Credentials Exfil
- [x] ET MALWARE PyPI Phishing/Malware Data Exfiltration Domain (linkedopports .com) in DNS Lookup
- [x] ET MALWARE PyPI Malicious Library Payload Delivery Domain (python-release .com) in DNS Lookup
- [x] ET MALWARE Win32/Unknown CnC Activity
- [x] ET MALWARE Win32/Caypnamer.A RAT CnC Keepalive
- [x] ET MALWARE Win32/Meimaii Checkin
- [x] ET MALWARE VBS/Kimsuky UA Observed
- [x] ET MALWARE Win32/Nitrokod CnC Domain (Intelserviceupdate .com) in DNS Lookup
- [x] ET MALWARE Win32/Nitrokod Domain (intelserviceupdate .com) in TLS SNI
- [x] ET MALWARE Win32/Nitrokod Domain (nvidiacenter .com) in TLS SNI
- [x] ET MALWARE PureCrypter Requesting Injector M1
- [x] ET MALWARE PureCrypter Requesting Injector - Known Campaign ID M1
- [x] ET MALWARE PureCrypter Requesting Injector - Known Campaign ID M3
- [x] ET MALWARE PureCrypter Requesting Injector - Known Campaign ID M5
- [x] ET MALWARE Win32/Orchard Botnet Activity M2
- [ ] ET MALWARE Observed DNS Query to TA444 Domain (documentshare .info)
- [ ] ET MALWARE Observed DNS Query to TA444 Domain (cloud .globiscapital .co)
- [x] ET MALWARE Observed DNS Query to TA444 Domain (stablehouses .info)
- [ ] ET MALWARE Observed DNS Query to TA444 Domain (bankofamerica .us .org)
- [x] ET MALWARE Observed DNS Query to TA444 Domain (cloud .jbic .us)
- [ ] ET MALWARE Observed DNS Query to TA444 Domain (vote .anobaka .info)
- [x] ET MALWARE ErbiumStealer Variant CnC Activity (getstub)
- [x] ET MALWARE Malicious SSL Certificate detected (BoratRat)
- [x] ET MALWARE Win32/Orchard Botnet Activity
- [x] ET MALWARE Win32.Stealer.alwu Data Exfiltration Attempt
- [x] ET MALWARE Observed JSSLoader Domain (essentialsmassageanddayspa .com) in TLS SNI
- [x] ET MALWARE Win32/Atomsilo Ransomware Activity (POST)
- [x] ET MALWARE CargoBay CnC Activity
- [x] ET MALWARE DonotGroup APT Related Domain in DNS Lookup (esr .suppservices .xyz)
- [ ] ET MALWARE DonotGroup APT Related Domain in DNS Lookup (worldpro .buzz)
- [ ] ET MALWARE DonotGroup APT Related Domain in DNS Lookup (fitnesscheck .xyz)
- [x] ET MALWARE DonotGroup APT Related Domain in DNS Lookup (ser .dermlogged .xyz)
- [x] ET MALWARE VileRAT Related Domain in DNS Lookup (hubflash .co)
- [x] ET MALWARE TA453/CharmingKitten HYPERSCRAPE Tool Check-in Activity (GET)
- [x] ET MALWARE TA453/CharmingKitten HYPERSCRAPE Tool Sending System Information (POST)
- [x] ET MALWARE Confucious APT Related Domain in DNS Lookup (bonimoni .xyz)
- [x] ET MALWARE Win32/RecordBreaker CnC Exfil (Cookies)
- [x] ET MALWARE OSX/SHLAYER CnC Activity M2
- [x] ET MALWARE Win32/Matanbuchus Loader Activity (POST)
- [x] ET MALWARE Win32/Grandoreiro Related Activity (GET)
- [x] ET MALWARE PyPI Malicious Library Update Payload Checkin
- [x] ET MALWARE Observed PyPI Phishing/Malicious Library Data Exfiltration Domain (linkedopports .com) in TLS SNI
- [ ] ET MALWARE Observed PyPI Malicious Library Payload Delivery Domain (python-release .com) in TLS SNI
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (telecomly .info)
- [x] ET MALWARE Win32/Caypnamer.A RAT CnC Initial Checkin
- [x] ET MALWARE VBS/Kimsuky.O Host Fingerprint Exfil
- [x] ET MALWARE Win32/Nitrokod CnC Domain (nitrokod .com) in DNS Lookup
- [x] ET MALWARE Win32/Nitrokod CnC Domain (nvidiacenter .com) in DNS Lookup
- [x] ET MALWARE Win32/Nitrokod Domain (nitrokod .com) in TLS SNI
- [x] ET MALWARE Win32/Sabsik.FL.B!ml Exfil
- [x] ET MALWARE PureCrypter Requesting Injector M2
- [x] ET MALWARE PureCrypter Requesting Injector - Known Campaign ID M2
- [x] ET MALWARE PureCrypter Requesting Injector - Known Campaign ID M4
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (fuvataren .com)
- [ ] ET MALWARE Observed DNS Query to TA444 Domain (wps .wpsonline .co)
- [ ] ET MALWARE Observed DNS Query to TA444 Domain (unchained-capital .co)
- [ ] ET MALWARE Observed DNS Query to TA444 Domain (shconstmarket .com)
- [ ] ET MALWARE Observed DNS Query to TA444 Domain (edit .wpsonline .co)
- [x] ET MALWARE Observed DNS Query to TA444 Domain (salt1ending .com)
- [ ] ET MALWARE Observed DNS Query to TA444 Domain (share .anobaka .info)
- [ ] ET MALWARE Observed DNS Query to TA444 Domain (cloud .wpic .ink)
- [x] ET MALWARE ErbiumStealer Domain (erbium .ml) in TLS SNI
- [x] ET MALWARE Win32/VictoryGate/Orchard Botnet CnC Checkin
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (dofixifa .co)
- [x] ET MALWARE Win32/Sabsik.EN.D!ml CnC Checkin

- [x] ET MALWARE Evilnum APT Related Domain in DNS Lookup (image .jamespage .net)
- [x] ET MALWARE ErbiumStealer Response From Panel
- [ ] ET MALWARE ErbiumStealer CnC Domain (ozaron .beget .tech) in DNS Lookup
- [ ] ET MALWARE ErbiumStealer CnC Domain (a0715952 .xsph .ru) in DNS Lookup
- [x] ET MALWARE Suspected Chinese Based APT Malware Retrieving File (GET)
- [x] ET MALWARE Observed Chinese APT Related Domain (ramblercloud .com in TLS SNI)
- [ ] ET MALWARE Observed DNS Query to EvilProxy Domain (msdnmail .net)
- [ ] ET MALWARE Observed DNS Query to EvilProxy Domain (rproxy .io)
- [ ] ET MALWARE Observed DNS Query to EvilProxy Domain (top-cyber .club)
- [x] ET MALWARE Observed DNS Query to TA444 Domain (mufg .tokyo)
- [x] ET MALWARE Win32/MagicRAT CnC Checkin M1
- [x] ET MALWARE Win32/MagicRAT Additional Payload URI M1
- [x] ET MALWARE Win32/MagicRAT Additional Payload URI M3
- [x] ET MALWARE MagicRAT CnC Domain (gendoraduragonkgp126 .com) in DNS Lookup
- [x] ET MALWARE Bitter APT Related Domain in DNS Lookup (signal-premium-app .org)
- [x] ET MALWARE Bitter APT Related Domain in DNS Lookup (youtubepremiumapp .com)
- [x] ET MALWARE Gamaredon APT Related Activity (GET)
- [x] ET MALWARE Win32/MagicRAT CnC Activity M1
- [x] ET MALWARE Observed DNS Query to TA444 Domain (bankofamerica .nyc)
- [x] ET MALWARE Observed TA444 Domain (azure-protection .cloud in TLS SNI)
- [x] ET MALWARE Observed TA444 Domain (azure-protect .online in TLS SNI)
- [x] ET MALWARE Win32/Wacapew.C!ml CnC Checkin
- [x] ET MALWARE Win64/Spy.Agent.EU CnC Checkin
- [x] ET MALWARE Sidecopy APT Related Backdoor Activity
- [x] ET MALWARE PowerShell/PowHeartBeat CnC Domain (airplane .travel-commercials .agency) in DNS Lookup
- [x] ET MALWARE Gamaredon Related Maldoc Activity (GET)
- [x] ET MALWARE Gamaredon Related Maldoc Activity (GET)
- [x] ET MALWARE Gamaredon Related Maldoc Activity (GET)
- [x] ET MALWARE Gamaredon Related Maldoc Activity (GET)
- [x] ET MALWARE Gamaredon Related Maldoc Activity (GET)
- [x] ET MALWARE Powershell/PowHeartBeat CnC Checkin - ICMP
- [x] ET MALWARE Observed DNS Query to Reverse Shell Payload Domain (opentunnel .quest)
- [x] ET MALWARE Observed Reverse Shell Payload Delivery Domain (opentunnel .quest) in TLS SNI
- [ ] ET MALWARE OSX/XCSSET Related Domain in DNS Lookup (appledocs .ru)
- [ ] ET MALWARE OSX/XCSSET Related Domain in DNS Lookup (kinksdoc .ru)
- [ ] ET MALWARE OSX/XCSSET Related Domain in DNS Lookup (cosmodron .com)
- [ ] ET MALWARE OSX/XCSSET Related Domain in DNS Lookup (melindas .ru)
- [ ] ET MALWARE Observed DNS Query to Default Brute Ratel C2 Domain (evasionlabs .com)
- [x] ET MALWARE Brute Ratel CnC Activity (xml-c2) M1
- [x] ET MALWARE Brute Ratel CnC Activity (json-c2) M1
- [x] ET MALWARE Suspected Win32/TinyNode Activity (Outbound)
- [x] ET MALWARE ErbiumStealer Response From CnC
- [ ] ET MALWARE Observed ErbiumStealer Domain (ozaron .beget .tech) in TLS SNI
- [x] ET MALWARE Trojan.Proxy.Small.Z CnC Checkin
- [x] ET MALWARE Chinese Based APT Related Domain in DNS Lookup (ramblercloud .com)
- [ ] ET MALWARE Observed DNS Query to Temporary File Hosting Domain (temp .sh)
- [ ] ET MALWARE Observed DNS Query to EvilProxy Domain (evilproxy .pro)
- [ ] ET MALWARE Observed DNS Query to EvilProxy Domain (pua75npooc4ekrkkppdglaleftn5mi2hxsunz5uuup6uxqmen4deepyd .onion)
- [x] ET MALWARE Observed DNS Query to TA444 Domain (careersbankofamerica .us)
- [x] ET MALWARE Observed DNS Query to TA444 Domain (azure-protect .online)
- [x] ET MALWARE Win32/MagicRAT CnC Checkin M2
- [x] ET MALWARE Win32/MagicRAT Additional Payload URI M2
- [x] ET MALWARE Win32/MagicRAT Additional Payload URI M4
- [ ] ET MALWARE Chinese Based APT Related Malware Sending System Information (POST)
- [x] ET MALWARE Bitter APT Related Domain in DNS Lookup (signalpremium .com)
- [x] ET MALWARE Win32/Qbot CnC Activity M3 (POST)
- [x] ET MALWARE Win32/Zegost!ml CnC Checkin
- [x] ET MALWARE Observed DNS Query to TA444 Domain (azure-protection .cloud)
- [x] ET MALWARE Observed TA444 Domain (bankofamerica .nyc in TLS SNI)
- [x] ET MALWARE Observed TA444 Domain (careersbankofamerica .us in TLS SNI)
- [x] ET MALWARE Observed TA444 Domain (mufg .tokyo in TLS SNI)
- [ ] ET MALWARE MSIL/TrojanDownloader.Agent.ITY Screenshot Upload Attempt
- [x] ET MALWARE Win32/MagicRAT CnC Activity M2
- [x] ET MALWARE PowerShell/PowHeartBeat CnC Domain (central .suhypercloud .org) in DNS Lookup
- [x] ET MALWARE Win32/TrojanDownloader.VB.RTN Payload Delivery Request
- [x] ET MALWARE Gamaredon Related Maldoc Activity (GET)
- [x] ET MALWARE Gamaredon Related Maldoc Activity (GET)
- [x] ET MALWARE Gamaredon Related Maldoc Activity (GET)
- [x] ET MALWARE Gamaredon Related Maldoc Activity (GET)
- [x] ET MALWARE Gamaredon Related Maldoc Activity (GET)
- [x] ET MALWARE Bitter APT CHM CnC Activity (GET) M1
- [x] ET MALWARE Observed DNS Query to Malicious Powershell Payload domain (onerecovery .click)
- [x] ET MALWARE Observed Malicious Powershell Payload Delivery Domain (onerecovery .click) in TLS SNI
- [x] ET MALWARE Powershell/PowHeartBeat CnC Checkin - HTTPS
- [ ] ET MALWARE OSX/XCSSET Related Domain in DNS Lookup (gurumades .ru)
- [ ] ET MALWARE OSX/XCSSET Related Domain in DNS Lookup (superdocs .ru)
- [ ] ET MALWARE OSX/XCSSET Related Domain in DNS Lookup (gismolow .com)
- [ ] ET MALWARE OSX/XCSSET Related Domain in DNS Lookup (adobefile .ru)
- [x] ET MALWARE Brute Ratel Fake User-Agent
- [x] ET MALWARE Brute Ratel CnC Activity (xml-c2) M2
- [x] ET MALWARE Brute Ratel CnC Activity (json-c2) M2

- [x] ET MALWARE Observed DNS Query to TA444 Domain (cloud .tptf .ltd)
- [x] ET MALWARE Observed DNS Query to TA444 Domain (careers .bankofamerica .nyc)
- [x] ET MALWARE Observed DNS Query to TA444 Domain (bankofamerica .offerings .cloud)
- [x] ET MALWARE Observed DNS Query to TA444 Domain (bankofamerica .tel)
- [x] ET MALWARE Observed DNS Query to TA444 Domain (cloud .mufg .uk)
- [x] ET MALWARE Observed TA444 Domain (cloud .tptf .ltd in TLS SNI)
- [x] ET MALWARE Observed TA444 Domain (bankofamerica .tel in TLS SNI)
- [x] ET MALWARE Observed TA444 Domain (cloud .mufg .uk in TLS SNI)
- [x] ET MALWARE Observed TA444 Domain (bankofamerica .offerings .cloud in TLS SNI)
- [x] ET MALWARE Observed TA444 Domain (careers .bankofamerica .nyc in TLS SNI)
- [x] ET MALWARE Windows/OriginLogger CnC Domain (originpro .me) in DNS Lookup
- [x] ET MALWARE Windows/OriginLogger CnC Domain (originproducts .xyz) in DNS Lookup
- [x] ET MALWARE Windows/OriginLogger CnC Domain (originlogger .com) in DNS Lookup
- [x] ET MALWARE Windows/OriginLogger CnC Domain (originproducts .pw) in DNS Lookup
- [x] ET MALWARE Win64/Spy.Agent.EE CnC Checkin Server Response
- [ ] ET MALWARE Sidewinder APT Related Domain in DNS Lookup (ptcl-gov .com)
- [x] ET MALWARE Win32.Agent.Y!c CnC Checkin
- [x] ET MALWARE Mercury APT Related Domain in DNS Lookup (sygateway .com)
- [x] ET MALWARE Warzone RAT Response (Inbound)
- [x] ET MALWARE Golang/Webbfustator DNS Tunneling Activity
- [x] ET MALWARE Win32/Agent.XXZ Checkin
- [x] ET MALWARE Win32/Covagent Checkin
- [x] ET MALWARE Win32/QQPass Checkin
- [x] ET MALWARE Gamaredon Information Stealer Data Exfiltration Attempt
- [x] ET MALWARE Gamaredon CnC Domain (kuckuduk .ru) in DNS Lookup
- [x] ET MALWARE Gamaredon CnC Domain (celticso .ru) in DNS Lookup
- [x] ET MALWARE DonotGroup Activity (GET)
- [ ] ET MALWARE DonotGroup Related Domain in DNS Lookup (furnish .spacequery .live)
- [x] ET MALWARE Observed DonotGroup Related Domain (furnish .spacequery .live in TLS SNI)
- [x] ET MALWARE Win32/RecordBreaker - Observed UA M3 (TakeMyPainBack)
- [x] ET MALWARE Win32/RecordBreaker CnC Checkin - Server Response M2
- [x] ET MALWARE Win32/Cryptbotv2 CnC Activity (POST) M1
- [x] ET MALWARE Observed DNS Query to TA444 Domain (docuprivacy .com)
- [ ] ET MALWARE Observed DNS Query to TA444 Domain (share .anobaka .info)
- [x] ET MALWARE Observed DNS Query to TA444 Domain (privacysign .org)
- [x] ET MALWARE Observed DNS Query to TA444 Domain (ms .onlineshares .cloud)
- [x] ET MALWARE Observed DNS Query to TA444 Domain (team .msteam .biz)
- [x] ET MALWARE Observed DNS Query to TA444 Domain (mizuhogroup .us)
- [x] ET MALWARE Observed DNS Query to TA444 Domain (docs .azurehosting .co)
- [x] ET MALWARE Observed DNS Query to TA444 Domain (tptf .fund)
- [x] ET MALWARE Observed DNS Query to TA444 Domain (perseus .bond)
- [x] ET MALWARE Observed DNS Query to TA444 Domain (smbcgroup .us)
- [x] ET MALWARE Observed DNS Query to TA444 Domain (tptf .cloud)
- [x] ET MALWARE Observed TA444 Domain (tptf .fund in TLS SNI)
- [x] ET MALWARE Observed TA444 Domain (docs .azurehosting .co in TLS SNI)
- [x] ET MALWARE Observed TA444 Domain (team .msteam .biz in TLS SNI)
- [x] ET MALWARE Observed TA444 Domain (share .anobaka .info in TLS SNI)
- [x] ET MALWARE Observed TA444 Domain (smbcgroup .us in TLS SNI)
- [x] ET MALWARE Observed TA444 Domain (perseus .bond in TLS SNI)
- [x] ET MALWARE Observed TA444 Domain (docuprivacy .com in TLS SNI)
- [x] ET MALWARE Observed TA444 Domain (privacysign .org in TLS SNI)
- [x] ET MALWARE Observed TA444 Domain (mizuhogroup .us in TLS SNI)
- [x] ET MALWARE Observed TA444 Domain (ms .onlineshares .cloud in TLS SNI)
- [x] ET MALWARE Observed TA444 Domain (tptf .cloud in TLS SNI)
- [x] ET MALWARE Win32/Cryptbot V2 Data Exfiltration Attempt
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (casting .faeryfox .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (predator .foxscalesjewelry .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (amplifier .myjesusloves .me)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (loans .mistakenumberone .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (restructuring .breatheinnew .life)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (prompt .zonashoppers .academy)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (hair .2topost .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (custom .usmuchmedia .com)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (moments .abledity .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (notes .fumcpittsburg .org)
- [x] ET MALWARE APT28/FancyBear Related Activity (POST)
- [x] ET MALWARE Metador CnC Domain (networkselfhelp .com) in DNS Lookup
- [x] ET MALWARE dYdX NPM Package Backdoor Exfiltration Domain (api .circle-cdn .com) in DNS Lookup
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (tutorials .girandolashutkindconstruction .com)
- [x] ET MALWARE Gamaredon APT Backdoor Related Activity
- [x] ET MALWARE OSX/SHLAYER CnC Domain in DNS Lookup
- [x] ET MALWARE OSX/SHLAYER CnC Domain in DNS Lookup
- [x] ET MALWARE OSX/SHLAYER CnC Domain in DNS Lookup
- [x] ET MALWARE OSX/SHLAYER CnC Domain in DNS Lookup
- [x] ET MALWARE OSX/SHLAYER CnC Domain in DNS Lookup
- [x] ET MALWARE OSX/SHLAYER CnC Domain in DNS Lookup
- [x] ET MALWARE OSX/SHLAYER CnC Domain in DNS Lookup
- [x] ET MALWARE OSX/SHLAYER CnC Domain in DNS Lookup

- [x] ET MALWARE Golang/Webbfustator Related Domain in DNS Lookup (xmlschemeformat .com)
- [x] ET MALWARE Golang/Webbfustator Related Domain in DNS Lookup (updatesagent .com)
- [x] ET MALWARE Lazarus APT Related Domain in DNS Lookup (digiboxes .us)
- [x] ET MALWARE TA444 Related Domain in DNS Lookup (onlinecloud .cloud)
- [x] ET MALWARE Lockbit Ransomware Related Domain in DNS Lookup (lockbitapt)
- [ ] ET MALWARE Lockbit Ransomware Related Domain in DNS Lookup (ppaauuaa11232 .cc)
- [x] ET MALWARE Win32/Logger RAT CnC Checkin
- [x] ET MALWARE Win32/Spy.Delf.QTL Data Exfiltration Attempt
- [x] ET MALWARE Maldoc CnC Checkin
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (jobs .registermegod .online)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (logistics .socialtrendsmanagement .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (football .4tosocial .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (memorial .4tosocialprofessional .com)
- [x] ET MALWARE ErbiumStealer CnC Domain (mamamiya137 .ru) in DNS Lookup
- [x] ET MALWARE ErbiumStealer CnC Domain (www .f0679086 .xsph .ru) in DNS Lookup
- [x] ET MALWARE Win32/SaintStealer Data Exfiltration Attempt M1
- [x] ET MALWARE Win32/SaintStealer CnC Response
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (people .zonashoppers .com)
- [x] ET MALWARE LazyScripter Related Domain in DNS Lookup (hpsj .firewall-gateway .net)
- [x] ET MALWARE LazyScripter Related Activity (GET)
- [x] ET MALWARE Lazyscripter Related Activity (Inbound)
- [x] ET MALWARE Win32/Sephora Related Domain in DNS Lookup (sephus .me)
- [x] ET MALWARE Win32/Sephora Related Activity (GET)
- [x] ET MALWARE Win32/Sephora Related Activity (POST)
- [x] ET MALWARE Win32/Variant.Babar.74963 CnC Exfil
- [x] ET MALWARE Win32/SaintStealer Data Exfiltration Attempt M2
- [x] ET MALWARE Maldoc Domain (word2022 .c1 .biz) in DNS Lookup
- [x] ET MALWARE TigerHunter DOTM CnC Checkin
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (soendorg .top)
- [ ] ET MALWARE TA569 Domain in DNS Lookup (luxury-limousine .com)
- [ ] ET MALWARE TA569 sczriptzzbn JavaScript Inject
- [ ] ET MALWARE TA569 Fake Captcha Download
- [ ] ET MALWARE TA569 Domain in DNS Lookup (skambio-porte .com)
- [ ] ET MALWARE TA569 Fake Browser Update
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (training .c1ypsilanti .org)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (engine .discoveryhypnosis .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (fundraising .mystylingmylife .xyz)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (resale .adkelly .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (auction .wonderwomanquilts .com)
- [x] ET MALWARE Win32/NetDooka Framework Related Activity (POST) M2
- [x] ET MALWARE Observed Malicious SSL Cert (Go/Chaos Botnet)
- [x] ET MALWARE Gamaredon APT Related Activity (GET)
- [x] ET MALWARE Win32/Coldstealer Sending System Information (POST)
- [x] ET MALWARE TA444 Domain in DNS Lookup
- [x] ET MALWARE TA444 Domain in DNS Lookup
- [x] ET MALWARE Observed TA444 Domain (mufg .ink in TLS SNI)
- [x] ET MALWARE Observed TA444 Domain (mufg .us .org in TLS SNI)
- [x] ET MALWARE Chaos Botnet CnC Domain (ars1 .wemix .cc) in DNS Lookup
- [x] ET MALWARE Chaos Botnet CnC Domain (quanquandd .top) in DNS Lookup
- [x] ET MALWARE Chaos Botnet CnC Domain (tomca1 .com) in DNS Lookup
- [ ] ET MALWARE Chaos Botnet CnC Domain (a .nqb001 .com) in DNS Lookup
- [ ] ET MALWARE Chaos Botnet CnC Domain (js .wanpay1 .cn) in DNS Lookup
- [ ] ET MALWARE Chaos Botnet CnC Domain (tf .xiaozhuddos .co) in DNS Lookup
- [ ] ET MALWARE Chaos Botnet CnC Domain (abc .cfed .cc) in DNS Lookup
- [x] ET MALWARE Chaos Botnet CnC Domain (ai .nqb001 .com) in DNS Lookup
- [ ] ET MALWARE Chaos Botnet CnC Domain (x .xlg360 .xyz) in DNS Lookup
- [ ] ET MALWARE Chaos Botnet CnC Domain (kivspace .xyz) in DNS Lookup
- [ ] ET MALWARE Chaos Botnet CnC Domain (bitantcoins .pro) in DNS Lookup
- [ ] ET MALWARE Chaos Botnet CnC Domain (botnet .ddoswow .site) in DNS Lookup
- [x] ET MALWARE Chaos Botnet CnC Domain (skyeda .vip) in DNS Lookup
- [x] ET MALWARE Chaos Botnet CnC Domain (linuxddos .net) in DNS Lookup
- [ ] ET MALWARE Chaos Botnet CnC Domain (xiaomai233 .f3322 .net) in DNS Lookup
- [ ] ET MALWARE Chaos Botnet CnC Domain (bb .hash3688 .com) in DNS Lookup
- [ ] ET MALWARE Chaos Botnet CnC Domain (are .nishabig .pro) in DNS Lookup
- [ ] ET MALWARE Lazarus APT Related CnC Domain in DNS Lookup (market .contradecapital .com)
- [x] ET MALWARE Observed Lazarus Domain (market .contradecapital .com in TLS SNI)
- [x] ET MALWARE Havoc Framework CnC Request
- [x] ET MALWARE Havoc Framework CnC Response
- [x] ET MALWARE TA404/Zinc Trojanized KiTTY CnC Checkin
- [x] ET MALWARE TA404/Zinc Trojanized muPDF/Subliminal CnC Checkin
- [x] ET MALWARE WP CharCode Inject
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (premiere .4tosocialbeginners .com)
- [ ] ET MALWARE TA569 Obfuscated sczriptzzb JavaScript Inject
- [x] ET MALWARE DonotGroup Pult Downloader Activity (POST) M2
- [x] ET MALWARE Observed DNS Query to Comm100 Trojan Domain (amazonawsreplay .com)
- [ ] ET MALWARE Observed DNS Query to Comm100 Trojan Domain (microsoftfileapis .com)
- [ ] ET MALWARE Observed DNS Query to Comm100 Trojan Domain (windowstearns .com)
- [x] ET MALWARE JS/Comm100 Trojan Backdoor Inbound
- [x] ET MALWARE JS/Comm100 Trojan CnC Payload Inbound
- [ ] ET MALWARE TA569 Domain in DNS Lookup (googletag .com)
- [ ] ET MALWARE TA569 Domain in DNS Lookup (brocode3s .com)
- [ ] ET MALWARE Malicious Browser Installer Domain in DNS Lookup (torbrowser .io)

- [ ] ET MALWARE Malicious Browser Installer Domain in DNS Lookup (tor-browser .io)
- [ ] ET MALWARE Observed DNS Query to XWorm RAT Domain (system6458 .ddns .net)
- [x] ET MALWARE AllcomeClipper CnC Checkin
- [ ] ET MALWARE TA569 Fake Browser Update Domain in DNS Lookup (profi-stom .com)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (faristo .site)
- [ ] ET MALWARE WinGo/Go-rod moz_cookies Failed Data Exfiltration attempt
- [x] ET MALWARE TrueBot/Silence.Downlaoder Screenshot Post M1
- [x] ET MALWARE Win32/RM3Loader Activity (set)
- [x] ET MALWARE Win32/RM3Loader Server Response
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (family .1ablecommunity .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (ecar .allsunstates .com)
- [x] ET MALWARE Polonium APT CREEPYSNAIL Backdoor Related Activity (GET)
- [x] ET MALWARE Arid Viper APT Related Domain in DNS Lookup (zakaria-chotzen .info)
- [x] ET MALWARE HTML/Qbot Dropper (.zip)
- [x] ET MALWARE Observed Malicious SSL/TLS Certificate (QakBot)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (demand .sageyogatherapies .com)
- [x] ET MALWARE Arid Viper APT Related Activity (POST)
- [ ] ET MALWARE Mekotio Banking Trojan CnC Domain (zautoservice .eu) in DNS Lookup
- [ ] ET MALWARE MSSQL maggie backdoor Accessall Query Observed
- [x] ET MALWARE MSSQL maggie backdoor ls Query Observed
- [x] ET MALWARE MSSQL maggie backdoor whoami Query Observed
- [x] ET MALWARE VBA/Agent.AAV CnC Checkin
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (ktwods .lflink .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (relationship .epac .to)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (ftp .hinet .dns-dns .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (RdAccount .dns1 .us)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (Facebook .ddns .ms)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (zbAction .dynssl .COM)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (big .qpoe .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (bnhxalex .organiccrap .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (kilomier .2waky .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (american .ddns .us)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (zcrd .twgogo .org)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (oop .gov .minecraftr .us)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (most .gov .allowed .org)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (accountinfo .ssl443 .org)
- [x] ET MALWARE Malicious Browser Installer Checkin (POST)
- [ ] ET MALWARE AllcomeClipper CnC Domain (dba692117be7b6d3480fe5220fdd58b38bf .xyz) in DNS Lookup
- [ ] ET MALWARE TA569 Domain in DNS Lookup (pastukhova .com)
- [x] ET MALWARE Suspected Smokeloader Activity (POST)
- [x] ET MALWARE WinGo/Go-rod signInUrls Failed Data Exfiltration attempt
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (internal .blessedfoodshalalmeat .com)
- [x] ET MALWARE TrueBot/Silence.Downlaoder Screenshot Post M2
- [ ] ET MALWARE Observed DNS Query to DonotGroup Domain (stokpro .buzz)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (repo .allgoodsnservices .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (resort .reliablecommunityservices .com)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (houses .in-vermont .com)
- [x] ET MALWARE Polonium APT PAPACREEP Backdoor Related Activity
- [x] ET MALWARE Observed Arid Viper APT Related Domain (zakaria-chotzen .info in TLS SNI)
- [ ] ET MALWARE Observed DNS Query to Cobalt Strike Domain 2022-10-11 (pigahinilu .com)
- [x] ET MALWARE Observed Malicious SSL/TLS Certificate (QakBot)
- [x] ET MALWARE Observed Malicious SSL/TLS Certificate (QakBot)
- [x] ET MALWARE Magecart Related Domain in DNS Lookup (cdn-mediahub .com)
- [x] ET MALWARE Win32/Spy.Mekotio.EY Payload Request
- [x] ET MALWARE MSSQL maggie backdoor ListIP Query Observed
- [x] ET MALWARE MSSQL maggie backdoor sysinfo Query Observed
- [x] ET MALWARE MSSQL maggie backdoor sp_addextendedproc Command Observed
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (happy .MyNetAV .ORG)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (centers .allowed .org)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (common .taiwan .twilightparadox .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (dirco .jetos .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (cart .skyseaweb .org)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (sacstartapples .mohwfreshman1 .otzo .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (web .stonekiki .freeddns .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (oop .ddns .us)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (asia .publiccosplay .org)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (article .phdfa .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (Kaccount .moneyhome .biz)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (duth .ahfree .net)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (ftp .wlksbb .MrsLove .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (kgoogfsd .freetcp .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (mofa .ignorelist .com)

- ET MALWARE Observed DNS Query to Budminer Domain (thesizeofearth .ourhobby .com)
- ET MALWARE Observed DNS Query to Budminer Domain (taitra .fartit .com)
- ET MALWARE Observed DNS Query to Budminer Domain (bing .ikwb .com)
- ET MALWARE Observed DNS Query to Budminer Domain (ey .acaro .org)
- ET MALWARE Observed DNS Query to Budminer Domain (fsc-kd .ns01 .info)
- ET MALWARE Observed DNS Query to Budminer Domain (whlu .congci .info)
- ET MALWARE Observed DNS Query to Budminer Domain (av .phdfa .com)
- ET MALWARE Observed DNS Query to Budminer Domain (youtobeother .twbbs .org)
- ET MALWARE Observed DNS Query to Budminer Domain (kcg2 .gov .tw .allowed .org)
- ET MALWARE Observed DNS Query to Budminer Domain (loginlived .com)
- ET MALWARE Observed DNS Query to Budminer Domain (prefers .kboyda .net)
- ET MALWARE Observed DNS Query to Budminer Domain (saitama .map-shinai .com)
- ET MALWARE Observed DNS Query to Budminer Domain (liveupdate .Jkub .com)
- ET MALWARE Observed DNS Query to Budminer Domain (Liveupdate .jkub .com)
- ET MALWARE Observed DNS Query to Budminer Domain (iphone .site .web .fbs .ezua .com)
- ET MALWARE Observed DNS Query to Budminer Domain (mitac_com .dns05 .com)
- ET MALWARE Observed DNS Query to Budminer Domain (soft .update .cloudns .info)
- ET MALWARE Observed DNS Query to Budminer Domain (gpu .wikaba .com)
- ET MALWARE Observed DNS Query to Budminer Domain (name .itsaol .com)
- ET MALWARE Observed DNS Query to Budminer Domain (infor .nttcom .tk)
- ET MALWARE Observed DNS Query to Budminer Domain (healths .jumpingcrab .com)
- ET MALWARE Observed DNS Query to Budminer Domain (gmailgroup .mooo .com)
- ET MALWARE Observed DNS Query to Budminer Domain (bigbank .cnkk .org)
- ET MALWARE Observed DNS Query to Budminer Domain (madicity .org)
- ET MALWARE Observed DNS Query to Budminer Domain (rt .skymeto .com)
- ET MALWARE Observed DNS Query to Budminer Domain (nscnet .tk)
- ET MALWARE Observed DNS Query to Budminer Domain (pic-yahoo .ddns .us)
- ET MALWARE Observed DNS Query to Budminer Domain (mosec .twgogo .org)
- ET MALWARE Observed DNS Query to Budminer Domain (yahoo .serveuser .com)
- ET MALWARE Observed DNS Query to Budminer Domain (TheoreticalModel .onmypc .us)
- ET MALWARE Observed DNS Query to Budminer Domain (family .mobwork .net)
- ET MALWARE Observed DNS Query to Budminer Domain (bigbang .ddns .ms)
- ET MALWARE Observed DNS Query to Budminer Domain (wmdshr .3322 .org)
- ET MALWARE Observed DNS Query to Budminer Domain (ftp .newmc .dns-dns .com)
- ET MALWARE Observed DNS Query to Budminer Domain (ftp .yahoo-inc .DSMTP .COM)
- ET MALWARE Observed DNS Query to Budminer Domain (zoneprenuin .crabdance .com)
- ET MALWARE Observed DNS Query to Budminer Domain (rfvg .karlosb .com)
- ET MALWARE Observed DNS Query to Budminer Domain (aolmail .ddns .info)
- ET MALWARE Observed DNS Query to Budminer Domain (pe .publiccosplay .org)
- ET MALWARE Observed DNS Query to Budminer Domain (google .ddns .name)
- ET MALWARE Observed DNS Query to Budminer Domain (kuangdao .serveftp .com)
- ET MALWARE Observed DNS Query to Budminer Domain (oop .crabdance .com)
- ET MALWARE Observed DNS Query to Budminer Domain (stonekiki .freeddns .com)
- ET MALWARE Observed DNS Query to Budminer Domain (smtpgov .eSMTP .biz)
- ET MALWARE Observed DNS Query to Budminer Domain (info .lsASecret .com)
- ET MALWARE Observed DNS Query to Budminer Domain (Kmember .wikaba .com)
- ET MALWARE Observed DNS Query to Budminer Domain (bigbang .myddns .com)
- ET MALWARE Observed DNS Query to Budminer Domain (ftp .twnic .almostmy .com)
- ET MALWARE Observed DNS Query to Budminer Domain (video .itsaol .com)
- ET MALWARE Observed DNS Query to Budminer Domain (wlksbb .MrsLove .com)
- ET MALWARE Observed DNS Query to Budminer Domain (tipo .dns-dns .com)
- ET MALWARE Observed DNS Query to Budminer Domain (global .smart-house .ga)
- ET MALWARE Observed DNS Query to Budminer Domain (exchanger-online-thalesgroup .zyns .com)
- ET MALWARE Observed DNS Query to Budminer Domain (ftp .lily .onmypc .net)
- ET MALWARE Observed DNS Query to Budminer Domain (cier .edu .tw .us .to)
- ET MALWARE Observed DNS Query to Budminer Domain (moea .jumpingcrab .com)
- ET MALWARE Observed DNS Query to Budminer Domain (kaspersky .apchnetinfo .com)
- ET MALWARE Observed DNS Query to Budminer Domain (nditd .top)
- ET MALWARE Observed DNS Query to Budminer Domain (mysweetpig .news .minecraftnoob .com)
- ET MALWARE Observed DNS Query to Budminer Domain (ftp .kingdom .myddns .com)
- ET MALWARE Observed DNS Query to Budminer Domain (moeaidb .ro .lt)
- ET MALWARE Observed DNS Query to Budminer Domain (bigbigbig .servehttp .com)
- ET MALWARE Observed DNS Query to Budminer Domain (tdns .verydvcd .com)
- ET MALWARE Observed DNS Query to Budminer Domain (airlinesflightleaving .thesizeofearth .ourhobby .com)
- ET MALWARE Observed DNS Query to Budminer Domain (wlks .ServeUsers .com)
- ET MALWARE Observed DNS Query to Budminer Domain (bulk .indonet .org)
- ET MALWARE Observed DNS Query to Budminer Domain (skype .mrbonus .com)
- ET MALWARE Observed DNS Query to Budminer Domain (toolbar .qpoe .com)

- ☐ ET MALWARE Observed DNS Query to Budminer Domain (micro .security .services .rebatesrule .net)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (sci .dns1 .us)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (twmis .twgogo .org)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (emailfromsm .mpsdtupdsda .ezua .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (google_service .ns01 .us)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (youtobebig .cnkk .org)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (moea .toythieves .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (hinet .dns-stuff .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (photostw .twgogo .org)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (oop .govtw .servernux .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (google .apchnetinfo .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (oop .uk .to)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (sceyf .ibmmt .net)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (symantecAnti .ItemDB .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (economy .ServeUser .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (privilegecom .theesponsibility .crabdance .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (dns .dymantic .service .fbs .ocry .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (oop .itsaol .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (intweb .mobwork .net)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (yahoo .ddns .name)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (moea .dsmtp .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (jjj .ns02 .us)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (expiration .toythieves .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (ftp .boonty .Got-Game .org)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (obicsystem .ntt-nexia .tk)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (rocky3288 .changeip .org)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (tpp .otzo .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (skyfd .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (news .rockspace .wang)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (taiwanmail .org .ignorelist .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (update .madicity .org)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (enjoyit .longmusic .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (music .apchnetinfo .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (googlemailinforma .orge .pl)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (k1fsc .ax .lt)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (manated .dynamic-dns .net)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (update .mefound .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (bigkszb .twgogo .org)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (newsda .opsdatus .greatfinder .org)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (google .dynssl .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (gov .toh .info)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (msnlive .25u .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (moeaidb .tk)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (iPhone .linkWebSock .ZoneID .uk .to)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (kdbb .ourhobby .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (faqtos .ignorelist .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (info .chemoimmunity .top)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (getadobe .dns-dns .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (specas .OurHobby .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (mbank .moneyhome .biz)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (kuangd .new .privatedns .org)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (moeaidb .dns-dns .tw)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (bitcom .polaczyk .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (biz .pcanywhere .NET)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (trends .crabdance .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (backupcoa .serveftp .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (ey .uk .to)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (common .taiwaninfoma .uk .to)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (itunes .toythieves .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (bidsd .justdied .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (mails .grousp .allowed .org)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (lily .onmypc .net)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (cca .us .to)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (pqsl .servernux .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (mains .tainoetnde .bgphome .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (members .viaopen .net)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (customs .bot .nu)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (bbwlkszb .organiccrap .com)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (news .onmypc .org)
- ☐ ET MALWARE Observed DNS Query to Budminer Domain (fareastone .my03 .com)

- [ ] ET MALWARE Observed DNS Query to Budminer Domain (news .mynews .photo-frame .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (trace .leecantu .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (googledrivercould .serveuser .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (blizzard .apchnetinfo .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (money .terelation .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (kuangd .new .hack-inter .net)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (voicetube .citytalk .crabdance .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (jgx .explorermaker .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (moeaidb .qhigh .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (post .ourhobby .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (yahoo .mailweb .sxn .us)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (gov .organiccrap .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (update .madacity .top)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (wephone .us .to)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (renders .maninta .anichgroup .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (qtwlkszb .dynamicdns .org .uk)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (H0TMAIL .ddns .info)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (Artor .terelation .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (mofir .twgg .org)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (find .usdc .ignorelist .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (software .acmetoy .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (lookup .ns02 .us)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (mpsdtupdsda .ezua .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (mptudp .pw)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (toolbar .DSMTP .COM)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (ftp .ourfriends .sexxxy .biz)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (iphone-ex .info .tm)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (1122334 .zyns .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (ourfriends .sexxxy .biz)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (offerings .love4lifewellness .com)
- [x] ET MALWARE Win32/TrojanDropper.Agent.SSQ Checkin
- [ ] ET MALWARE Win32/Lumma Stealer Data Exfiltration Attempt M1
- [x] ET MALWARE Win32/Lumma Stealer CnC Domain (765mm .xyz) in DNS Lookup
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (festival .robingaster .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (aimimi .xxuz .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (kelsdc .compress .to)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (idb .dns-dns .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (widcards .abousts .fabioabreu .net)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (yahoonews .twgg .org)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (ktwords .lflink .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (moea .strangled .net)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (ofa .fartit .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (kingpsng .twgogo .org)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (sososb .twbbs .org)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (yahoofacebook .345 .pl)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (download .longmusic .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (trademoea .onmypc .net)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (tw .americanunfinished .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (dayan .onedumb .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (workstation .mypop3 .org)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (kingdom .myddns .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (kdmm .t28 .net)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (list .googlebook .mrbonus .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (sorry .iownyour .biz)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (symantec .apchnetinfo .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (mofamail .acmetoy .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (mimimi .VizVaz .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (bestcom .dns2 .us)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (security .MyNetAV .ORG)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (mybb .dns-dns .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (airbus .zyns .com)
- [ ] ET MALWARE Observed DNS Query to Budminer Domain (mobiles .chickenkiller .com)
- [x] ET MALWARE MSSQL maggie backdoor Query Observed (other functions)
- [x] ET MALWARE Win32/TrojanDropper.Agent.SRM Exfil via Discord
- [ ] ET MALWARE Observed DNS Query to Cryptojacking Domain (a-dog .top)
- [ ] ET MALWARE Win32/Lumma Stealer CnC Domain (evetesttech .net) in DNS Lookup
- [x] ET MALWARE Win32/Lumma Stealer CnC Domain (safe-car .ru) in DNS Lookup
- [x] ET MALWARE WinGo/YT Stealer CnC Domain in DNS Lookup

- [x] ET MALWARE WinGo/YT Stealer CnC Checkin
- [ ] ET MALWARE SocGholish Domain in DNS Lookup
- [x] ET MALWARE Suspected POLONIUM CnC Domain (consulting-ukraine .tk) in DNS Lookup
- [x] ET MALWARE Suspected Polonium CnC Initial Checkin M1
- [x] ET MALWARE Suspected Polonium CnC Checkin (get_cmd)
- [x] ET MALWARE Suspected Polonium CnC Checkin (result.php - process list) M2
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (chess .north-atlantic .com)
- [x] ET MALWARE TA452 Related Backdoor Activity (GET)
- [x] ET MALWARE TA452 Related Backdoor Activity (POST)
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (ellechina .online)
- [x] ET MALWARE Observed DNS Query to ROMCOM RAT Domain (notfiled .com)
- [ ] ET MALWARE Observed DNS Query to ROMCOM RAT Domain (advanced-ip-scaner .com)
- [x] ET MALWARE Observed DNS Query to ROMCOM RAT Domain (www .get .adobe .com .aspx .io)
- [x] ET MALWARE Win32/WarHawk Activity (ping)
- [x] ET MALWARE Win32/WarHawk Activity (cmd)
- [x] ET MALWARE Win32/WarHawk Activity (filemgr) M2
- [x] ET MALWARE Win32/WarHawk Activity (task_done)
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup
- [x] ET MALWARE Sidewinder APT Related Malware Activity M2 (GET)
- [x] ET MALWARE Observed Malicious SSL/TLS Certificate (QakBot)
- [x] ET MALWARE Win32/Injector.BBYK Checkin
- [x] ET MALWARE Potential Juniper Phar Deserialization RCE Attempt (CVE-2022-22241)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (portraits .studio-94-photography .com)
- [x] ET MALWARE Potential Juniper Path Traversal RCE Attempt (CVE-2022-22245)
- [x] ET MALWARE Manjusaka C2 Client Heartbeat
- [ ] ET MALWARE JS/AlterSave Skimmer Payload Inbound M1
- [x] ET MALWARE Malicious Doc CnC Domain (e-demarches .kodeo .ch) in DNS Lookup
- [x] ET MALWARE Win32/Agent.AETZ CnC Checkin
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (myfood .silverspringfoodproject .org)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (podcasts .momsgrabcoffee .com)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (lionnik .xyz)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (astope .xyz)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (pinki .cyou)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (kidup .xyz)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (minotos .xyz)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (dodstep .cyou)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (higmon .cyou)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (fineg .xyz)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (prises .cyou)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (gigeram .com)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (gigimas .xyz)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (dodsman .com)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (reaso .xyz)
- [x] ET MALWARE Observed Ursnif Domain in TLS SNI (lionnik .xyz)
- [x] ET MALWARE Observed Ursnif Domain in TLS SNI (astope .xyz)
- [x] ET MALWARE Observed Ursnif Domain in TLS SNI (pinki .cyou)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (consultant .meredithklemmblog .com)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup
- [x] ET MALWARE Suspected POLONIUM CnC Domain (ukrsupport .info) in DNS Lookup
- [x] ET MALWARE Suspected Polonium CnC Initial Checkin M2
- [x] ET MALWARE Suspected Polonium CnC Checkin (result.php - process list) M1
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (discover .jsfconnections .com)
- [x] ET MALWARE MSIL/InfoStealer Variant Activity (POST)
- [x] ET MALWARE TA452 Related Backdoor Activity (POST)
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (pedaily .online)
- [x] ET MALWARE Observed DNS Query to ROMCOM RAT Domain (gov .mil .ua .aspx .io)
- [ ] ET MALWARE Observed DNS Query to ROMCOM RAT Domain (advanced-ip-scanners .com)
- [ ] ET MALWARE Observed DNS Query to ROMCOM RAT Domain (4qzm .com)
- [x] ET MALWARE Win32/WarHawk Checkin Activity
- [x] ET MALWARE Win32/WarHawk Activity (task)
- [x] ET MALWARE Win32/WarHawk Activity (filemgr)
- [x] ET MALWARE Win32/WarHawk Activity (fileupload)
- [x] ET MALWARE Win32/WarHawk Sending Windows System Information (POST)
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup
- [x] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [x] ET MALWARE Observed Malicious SSL/TLS Certificate (QakBot)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (shipwrecks .ggentile .com)
- [x] ET MALWARE Potential Juniper XPATH Injection Attempt (CVE-2022-22244)
- [x] ET MALWARE Potential Juniper Reflected XSS Attempt (CVE-2022-22242)
- [x] ET MALWARE Potential Juniper PHP Local File Inclusion Attempt (CVE-2022-22246)
- [x] ET MALWARE Manjusaka C2 Heartbeat Response
- [ ] ET MALWARE JS/AlterSave Skimmer Payload Inbound M2
- [x] ET MALWARE Win32.Agent.OSCF CnC Checkin
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (squad .incumetrics .com)
- [ ] ET MALWARE Python Library Backdoor Domain (wasp .plague .fun) in DNS Lookup
- [x] ET MALWARE Emotet Style Request Activity (GET)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (fishenddog .xyz)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (mamount .cyou)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (daydayvin .xyz)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (damnater .com)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (isteros .com)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (logotep .xyz)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (gigiman .xyz)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (pipap .xyz)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (binchfog .xyz)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (mainwog .xyz)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (tornton .xyz)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (rorfog .com)
- [x] ET MALWARE Observed DNS Query to Ursnif Domain (giantos .xyz)
- [x] ET MALWARE Observed Ursnif Domain in TLS SNI (fishenddog .xyz)
- [x] ET MALWARE Observed Ursnif Domain in TLS SNI (mamount .cyou)
- [x] ET MALWARE Observed Ursnif Domain in TLS SNI (daydayvin .xyz)

☑ ET MALWARE Observed Ursnif Domain in TLS SNI (kidup .xyz)
☑ ET MALWARE Observed Ursnif Domain in TLS SNI (damnater .com)
☑ ET MALWARE Observed Ursnif Domain in TLS SNI (minotos .xyz)
☑ ET MALWARE Observed Ursnif Domain in TLS SNI (isteros .com)
☑ ET MALWARE Observed Ursnif Domain in TLS SNI (dodstep .cyou)
☑ ET MALWARE Observed Ursnif Domain in TLS SNI (logotep .xyz)
☑ ET MALWARE Observed Ursnif Domain in TLS SNI (higmon .cyou)
☑ ET MALWARE Observed Ursnif Domain in TLS SNI (vavilgo .xyz)
☑ ET MALWARE Observed Ursnif Domain in TLS SNI (gigiman .xyz)
☑ ET MALWARE Observed Ursnif Domain in TLS SNI (fineg .xyz)
☑ ET MALWARE Observed Ursnif Domain in TLS SNI (pipap .xyz)
☑ ET MALWARE Observed Ursnif Domain in TLS SNI (prises .cyou)
☑ ET MALWARE Observed Ursnif Domain in TLS SNI (binchfog .xyz)
☑ ET MALWARE Observed Ursnif Domain in TLS SNI (gigeram .com)
☑ ET MALWARE Observed Ursnif Domain in TLS SNI (mainwog .xyz)
☑ ET MALWARE Observed Ursnif Domain in TLS SNI (gigimas .xyz)
☑ ET MALWARE Observed Ursnif Domain in TLS SNI (fingerpin .cyou)
☑ ET MALWARE Observed Ursnif Domain in TLS SNI (tornton .xyz)
☑ ET MALWARE Observed Ursnif Domain in TLS SNI (dodsman .com)
☑ ET MALWARE Observed Ursnif Domain in TLS SNI (rorfog .com)
☑ ET MALWARE Observed Ursnif Domain in TLS SNI (reaso .xyz)
☑ ET MALWARE Observed Ursnif Domain in TLS SNI (giantos .xyz)
☑ ET MALWARE Win32/Ursnif LDR4 Beacon (POST)
☑ ET MALWARE EICAR File Sent With X-Powered By Kaspersky Labs 2022-11-03
☑ ET MALWARE Win32/FlyStudio.OJJ CnC Checkin
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
☑ ET MALWARE Observed DNS Query to Hyperion Obfuscator Domain (plague .fun)
☑ ET MALWARE Hyperion Obfuscator Payload Inbound
☑ ET MALWARE Win32/DataStealer.P CnC Checkin
☑ ET MALWARE Win32/Delf.UUW CnC Keep-Alive
☐ ET MALWARE Win32\Cryptbot CnC Domain (kyrsti44 .top) in DNS Lookup
☑ ET MALWARE Win32\Cryptbot CnC Domain (okwnyw02 .top) in DNS Lookup
☑ ET MALWARE Win32\Cryptbot CnC Domain (okwydg05 .top) in DNS Lookup
☐ ET MALWARE Win32\Cryptbot CnC Domain (towcqx32 .top) in DNS Lookup
☐ ET MALWARE Win32\Cryptbot CnC Domain (okwerh01 .top) in DNS Lookup
☐ ET MALWARE Win32\Cryptbot CnC Domain (suqzyt03 .top) in DNS Lookup
☐ ET MALWARE Win32\Cryptbot CnC Domain (suqyjb01 .top) in DNS Lookup
☐ ET MALWARE Win32\Cryptbot CnC Domain (okwyeg04 .top) in DNS Lookup
☐ ET MALWARE Win32\Cryptbot CnC Domain (pefjfw62 .top) in DNS Lookup
☑ ET MALWARE Win32\Cryptbot CnC Domain (suqpvu08 .top) in DNS Lookup
☑ ET MALWARE Win32\Cryptbot CnC Domain (towhfs22 .top) in DNS Lookup
☐ ET MALWARE Win32\Cryptbot CnC Domain (suqosk04 .top) in DNS Lookup
☐ ET MALWARE Win32\Cryptbot CnC Domain (suqyqu10 .top) in DNS Lookup
☐ ET MALWARE Win32\Cryptbot CnC Domain (kyrjwt45 .top) in DNS Lookup
☐ ET MALWARE Win32\Cryptbot CnC Domain (suqzpe02 .top) in DNS Lookup
☐ ET MALWARE Win32\Cryptbot CnC Domain (suqycd05 .top) in DNS Lookup
☐ ET MALWARE Win32\Cryptbot CnC Domain (suqoyw07 .top) in DNS Lookup
☐ ET MALWARE Win32\Cryptbot CnC Domain (towspd42 .top) in DNS Lookup
☐ ET MALWARE ROMCOM RAT CnC Domain (you-supported .com) in DNS Lookup
☐ ET MALWARE ROMCOM RAT Campaign Domain (wveeam .com) in DNS Lookup
☐ ET MALWARE ROMCOM RAT Campaign Domain (keepas .org) in DNS Lookup
☐ ET MALWARE Kutaki Stealer CnC Domain (terebinnahicc .club) in DNS Lookup
☐ ET MALWARE Kutaki Stealer CnC Domain (treysbeatend .com) in DNS Lookup
☑ ET MALWARE ChromeLoader CnC Domain (istakechau .autos) in DNS Lookup
☐ ET MALWARE ChromeLoader CnC Domain (imenttogethe .xyz) in DNS Lookup
☑ ET MALWARE ChromeLoader CnC Checkin M1
☑ ET MALWARE ChromeLoader CnC Error
☑ ET MALWARE ChromeLoader CnC Checkin M2
☑ ET MALWARE WinGO\Monitor.go CnC Checkin
☐ ET MALWARE APT36/TransparentTribe CnC Domain (richa-sharma .ddns .net) in DNS Lookup
☐ ET MALWARE SocGholish Domain in DNS Lookup (course .netpickstrading .com)
☐ ET MALWARE SocGholish CnC Domain in DNS Lookup (campaign .tworiversboat .com)
☐ ET MALWARE SocGholish Domain in DNS Lookup (automatic .tworiversboats .com)
☑ ET MALWARE JS/Cloud9 Domain (download .loginserv .net) in DNS Lookup
☑ ET MALWARE JS/Cloud9 Domain (cloud-miner .de) in DNS Lookup
☑ ET MALWARE JS/Cloud9 Domain (zmsp .top) in DNS Lookup
☑ ET MALWARE JS/Cloud9 Domain (download .agency) in DNS Lookup
☑ ET MALWARE JS/Cloud9 Cookie Exfiltration Attempt
☑ ET MALWARE JS/Cloud9 Clipboard Exfiltration Attempt
☑ ET MALWARE DeimosC2 TCP Agent Heartbeat

- [x] ET MALWARE VBA/Agent.ADT Checkin
- [x] ET MALWARE APT41 CnC Domain (www .affice366 .com) in DNS Lookup
- [x] ET MALWARE APT41 CnC Domain (www .vietsovspeedtest .com) in DNS Lookup
- [ ] ET MALWARE IceXLoader CnC Domain (www .filifilm .com .br) in DNS Lookup
- [x] ET MALWARE Laplas Clipper CnC Domain (clipper .guru) in DNS Lookup
- [x] ET MALWARE Laplas Clipper - SetOnline CnC Checkin
- [x] ET MALWARE GO/Titan Stealer Data Exfiltration Attempt
- [ ] ET MALWARE TA569 Domain in DNS Lookup (friscomusicgroup .com)
- [x] ET MALWARE Win32/TyphonReborn Telegram CnC Checkin
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (collapse .tradingiswar .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (travel .dianatokaji .com)
- [x] ET MALWARE Observed Malicious SSL/TLS Certificate (CobaltStrike C2)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (factors .djbel .com)
- [x] ET MALWARE Suspected Bitter APT Related Activity
- [x] ET MALWARE Kimsuky CnC Domain (jojoa .mypressonline .com) Observed in DNS Query
- [ ] ET MALWARE Maldoc Related Domain in DNS Lookup
- [x] ET MALWARE Maldoc Retrieving Remote Template (GET)
- [x] ET MALWARE Observed TA444 Domain (gdocshare .one in TLS SNI)
- [x] ET MALWARE Golang Aurora Stealer Exfil Activity
- [x] ET MALWARE TA453 Domain in DNS Lookup (washingtonlnstitute .org)
- [x] ET MALWARE TA444 Domain in DNS Lookup (sharedrive .ink)
- [x] ET MALWARE Observed TA444 Domain (sharedrive .ink in TLS SNI)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (dashboard .skybacherslocker .com)
- [x] ET MALWARE Win32/Gh0st RAT Variant CnC Checkin response
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (subscribe .3gbling .com)
- [x] ET MALWARE Win32/ViperSoftX Stealer Activity M3 (POST)
- [ ] ET MALWARE Backdoored MSI Afterburner Payload Delivery Domain (git .git .skblxin .matrizauto .net) in DNS Lookup
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (wiki .clotheslane .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (mask .covidturf .com)
- [ ] ET MALWARE Observed DNS Query to W32/Filecoder.KY!tr.ransom Domain (e4c0660414bf .eu .ngrok .io)
- [ ] ET MALWARE Qakbot/Cobalt Strike Domain (jesofidiwi .com) in DNS Lookup
- [ ] ET MALWARE Qakbot/Cobalt Strike Domain (vopaxafi .com) in DNS Lookup
- [ ] ET MALWARE DonotGroup Related Domain in DNS Lookup (grapehister .buzz)
- [ ] ET MALWARE DonotGroup Related Domain in DNS Lookup (orangeholister .buzz)
- [ ] ET MALWARE TA453 Related Domain in DNS Lookup (mailer-daemon .me)
- [ ] ET MALWARE TA453 Related Domain in DNS Lookup (mailer-daemon .net)
- [x] ET MALWARE TA453 Related Domain in DNS Lookup (de-ma .online)
- [x] ET MALWARE TA453 Related Domain in DNS Lookup (mailer-daemon .online)
- [ ] ET MALWARE Python PyPi Typo Squatting Package Payload Delivery Domain (anarchydev .com) in DNS Request
- [x] ET MALWARE DonotGroup Maldoc Activity (GET)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (rate .coinangel .online)
- [x] ET MALWARE APT41 CnC Domain (c .ymvh8w5 .xyz) in DNS Lookup
- [ ] ET MALWARE IceXLoader CnC Domain (stealthelite .one) in DNS Lookup
- [ ] ET MALWARE CloudAtlas Related Domain in DNS Lookup (protocol-list .com)
- [x] ET MALWARE Laplas Clipper - Regex CnC Request
- [x] ET MALWARE Laplas Clipper - GetAddress CnC Checkin
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (community .backpacktrader .com)
- [x] ET MALWARE Fodcha Botnet Style DNS Server Lookup
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (casting .austinonline .shop)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (founder .carflower .pics)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (diary .lojjh .com)
- [x] ET MALWARE Win32/VB.PNU CnC Checkin
- [x] ET MALWARE Win32/Corrempa/HZRAT CnC Checkin
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [x] ET MALWARE Kimsuky CnC Domain (okihs .mypressonline .com) Observed in DNS Query
- [ ] ET MALWARE Maldoc Related Domain in DNS Lookup
- [x] ET MALWARE TA444 Domain in DNS Lookup (gdocshare .one)
- [x] ET MALWARE Win32/Filecoder.OJC CnC Checkin
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (mini .ptipexcel .com)
- [x] ET MALWARE Observed TA453 Domain (washingtonlnstitute .org in TLS SNI)
- [x] ET MALWARE TA444 Domain in DNS Lookup (dnx .capital)
- [x] ET MALWARE Observed TA444 Domain (dnx .capital in TLS SNI)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (montage .travelguidediva .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (hook .adieh .com)
- [x] ET MALWARE Mustang Panda APT TONESHELL Related Activity
- [ ] ET MALWARE Vidar Stealer Payload Delivery Domain (audacitya .org) in DNS Lookup
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (pastor .cntcog .org)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (perspective .cdsignner .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (progress .cashdigger .com)
- [ ] ET MALWARE Observed DNS Query to W32/Filecoder.KY!tr.ransom Domain (ec2-3-125-223-134 .eu-central-1 .compute .amazonaws .com)
- [ ] ET MALWARE Qakbot/Cobalt Strike Domain (tevokaxol .com) in DNS Lookup
- [ ] ET MALWARE Qakbot/Cobalt Strike Domain (dimingol .com) in DNS Lookup
- [x] ET MALWARE DonotGroup Backdoor Activity (POST)
- [ ] ET MALWARE Observed DonotGroup Related Domain (orangeholister .buzz in TLS SNI)
- [ ] ET MALWARE TA453 Related Domain in DNS Lookup (mailer-daemon .live)
- [x] ET MALWARE TA453 Related Domain in DNS Lookup (tinyurl .ink)
- [x] ET MALWARE TA453 Related Domain in DNS Lookup (litby .us)
- [x] ET MALWARE TA453 Related Domain in DNS Lookup (mailer-daemon .org)
- [ ] ET MALWARE Octopus Energy Themed Trojan CnC Domain (docusign-octopus-energy .com) in DNS Lookup
- [x] ET MALWARE Blackmagic Ransomware Checkin Activity (GET)

- [ ] ET MALWARE Magecart Skimmer Domain in DNS Lookup (cdn-jsnode-call .com)
- [ ] ET MALWARE Win32/DuckLogs Malware Related Domain in DNS Lookup (ducklogs .com)
- [ ] ET MALWARE Observed Win32/DuckLogs Malware Domain (ducklogs .com in TLS SNI)
- [x] ET MALWARE Possible Heliconia Noise Landing Page Response
- [x] ET MALWARE Observed DNS Query to AppleJeus Domain (telloo .io)
- [x] ET MALWARE Observed DNS Query to AppleJeus Domain (rebelthumb .net)
- [x] ET MALWARE Observed DNS Query to AppleJeus Domain (bloxholder .com)
- [x] ET MALWARE JS/Batloader Payload Request (GET)
- [ ] ET MALWARE Bitter APT CnC Domain (updnangelgroup .com) in DNS Lookup
- [ ] ET MALWARE Observed DNS Query to XWORM RAT Domain (esteticamarbai .es)
- [x] ET MALWARE Win32/RecordBreaker - Observed UA M4 (20112211)
- [x] ET MALWARE Observed DNS Query to ElectronBot Domain (11k .online)
- [x] ET MALWARE JS.ElectronBot Payload Inbound
- [ ] ET MALWARE TA569 Domain in DNS Lookup (ergpractice .com)
- [x] ET MALWARE GCleaner Downloader Activity M8
- [x] ET MALWARE Observed Pirate Stealer Domain in DNS Lookup (wearenotbbystealer .nl)
- [ ] ET MALWARE Confucious APT CnC Domain (microsoftonedriver .com) in DNS Lookup
- [ ] ET MALWARE Maldoc Related Domain in DNS Lookup (ms-office .services)
- [x] ET MALWARE Win32/Irafau Backdoor CnC Activity (POST)
- [x] ET MALWARE Observed DNS Query to Impersoni-fake-ator (uc .ejalase .org)
- [x] ET MALWARE Observed DNS Query to Impersoni-fake-ator (cloud .crmdev .org)
- [x] ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (cloud .skypecloud .net)
- [x] ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (plastic .delldrivers .in)
- [x] ET MALWARE Playful Taurus CnC Domain (proxy .oracleapps .org)
- [x] ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (news .alberto2011 .com)
- [x] ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (picture .efanshion .com)
- [x] ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (api .vmwareapi .net)
- [x] ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (info .fazlollah .net)
- [x] ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (mci .ejalase .org)
- [x] ET MALWARE Win32/ModernLoader Activity (POST)
- [x] ET MALWARE Win32/Eternity Stealer Activity (POST)
- [x] ET MALWARE Win32/BlackMagic Ransomware Payload Request (GET)
- [ ] ET MALWARE Observed BatLoader Domain (installationupgrade6 .com) in TLS SNI
- [ ] ET MALWARE Observed BatLoader Domain (tableau-cloud .com) in TLS SNI
- [x] ET MALWARE Observed BatLoader Domain (logmeincloudss .com) in TLS SNI
- [ ] ET MALWARE Confucious APT Related Domain in DNS Lookup (info-updates .ddns .net)
- [x] ET MALWARE Win32/DuckLogs Malware Activity (GET)
- [x] ET MALWARE ZINC APT Related Backdoor Activity (POST)
- [x] ET MALWARE Observed DNS Query to AppleJeus Domain (strainservice .com)
- [x] ET MALWARE Observed DNS Query to AppleJeus Domain (wirexpro .com)
- [x] ET MALWARE Observed DNS Query to AppleJeus Domain (oilycargo .com)
- [x] ET MALWARE Win32/AppleJeus CnC Checkin (POST)
- [ ] ET MALWARE Bitter APT CnC Domain (mobisharestock .com) in DNS Lookup
- [x] ET MALWARE Bitter APT CHM Activity (GET) M3
- [ ] ET MALWARE Observed DNS Query to XWORM RAT Domain (pujakumari .duckdns .org)
- [x] ET MALWARE Observed DNS Query to ElectronBot Domain (Electron-Bot .s3 .eu-central-1 .amazonaws .com)
- [x] ET MALWARE JS.ElectronBot.B.F7A4D930 Downloader (GET)
- [x] ET MALWARE Win32/XFILES Stealer Data Exfiltration Attempt
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .fate .truelance .com)
- [x] ET MALWARE Observed DNS Query to Pirate Stealer Domain (mdvksublbpczqluqvvbytfprxdwakuke .nl)
- [x] ET MALWARE Confucious APT CnC Checkin
- [ ] ET MALWARE Maldoc Related Domain in DNS Lookup (ms-offices .com)
- [ ] ET MALWARE Maldoc Related Domain in DNS Lookup (template-openxml .com)
- [x] ET MALWARE Observed DNS Query to Impersoni-fake-ator (cloud .fastpaymentser-vice .com)
- [x] ET MALWARE Observed DNS Query to Impersoni-fake-ator (cloud .microsoftshop .org)
- [x] ET MALWARE Observed DNS Query to Impersoni-fake-ator (fcanet .microsoftshop .org)
- [x] ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (iranwatch .tech)
- [x] ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (iransec .services)
- [x] ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (iredugov .wiki)
- [x] ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (info .payamradio .com)
- [x] ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (srv .fazlollah .net)
- [x] ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (mail .irir .org)
- [x] ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (soap .crmdev .org)
- [x] ET MALWARE Observd DNS Query to Impersoni-fake-ator Domain (srv .payamradio .com)
- [x] ET MALWARE Impersoni-fake-ator backdoor CnC Checkin
- [x] ET MALWARE Win32/Eternity Ransomware Retrieving Image (GET)
- [ ] ET MALWARE Observed BatLoader Domain (cloudsteamview .com) in TLS SNI
- [ ] ET MALWARE Observed BatLoader Domain (installationsoftware1 .com) in TLS SNI
- [x] ET MALWARE Observed BatLoader Domain (internalchecksssso .com) in TLS SNI
- [x] ET MALWARE Observed BatLoader Domain (105105105015 .com) in TLS SNI

- [x] ET MALWARE BatLoader CnC Domain (cloudsteamview .com) in DNS Lookup
- [ ] ET MALWARE BatLoader CnC Domain (installationsoftware1 .com) in DNS Lookup
- [ ] ET MALWARE BatLoader CnC Domain (internalchecksssso .com) in DNS Lookup
- [ ] ET MALWARE BatLoader CnC Domain (105105105015 .com) in DNS Lookup
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (aloyadakmashin .com)
- [x] ET MALWARE Cobalt Strike Related Activity (GET)
- [x] ET MALWARE JS/GootLoader CnC Exfil
- [ ] ET MALWARE Observed TA444/Lazarus Domain (one .microshare .cloud) in TLS SNI
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (docs-view .cloud)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (mufg .college)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (prosec .ink)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (angelbridge .capital)
- [ ] ET MALWARE DangerousPassword APT Related Domain in DNS Lookup (thecloudnet .org)
- [x] ET MALWARE DangerousPassword APT Style Request (GET)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (dwn-files .shop in TLS SNI)
- [x] ET MALWARE Win32/Valyria Maldoc Payload Request M2
- [x] ET MALWARE 7ev3n Ransomware Related Activity (GET)
- [x] ET MALWARE PSRansom File Exfiltration (POST)
- [x] ET MALWARE Win32/SocksTroy Session Initiation Attempt M1
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (modernism .designpaw .com)
- [x] ET MALWARE Filez Downloader Checkin
- [x] ET MALWARE Cobalt Strike Related Activity (GET)
- [x] ET MALWARE PS/PSRansom Client Checkin (GET)
- [x] ET MALWARE Win32/Khaosz.A!MTB Checkin - Command Retrieval
- [x] ET MALWARE RedditC2 Related Activity M2 (POST)
- [x] ET MALWARE Phonk Trojan CnC Checkin (POST)
- [x] ET MALWARE Win32/Goofy Guineapig CnC Activity (GET) M1
- [ ] ET MALWARE CIA Ransomware Domain (cia .cookie-coin .xyz) in DNS Lookup
- [x] ET MALWARE GoLinux/GoTrim CnC Checkin
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (deposit .coveprice .com)
- [x] ET MALWARE Observed Malicious Mustang Panda APT Related SSL Cert (File Transfer Service)
- [x] ET MALWARE TrueBot/Silence.Downloader CnC Checkin 3
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (cloud .prosec .ink)
- [x] ET MALWARE TA453 Related Domain in DNS Lookup (universityofmhealth .biz)
- [x] ET MALWARE Win32/Vulturi CnC Activity (GET)
- [x] ET MALWARE Gamaredon APT Related Activity (GET)
- [ ] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (vasimgo .shop)
- [ ] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (files-dwn .shop)
- [x] ET MALWARE Win32/RisePro CnC Command Outbound (get_loaders)
- [x] ET MALWARE Win32/RisePro CnC Command Outbound (freezeStats)
- [x] ET MALWARE Win32/RisePro CnC Command Outbound (pingmap)
- [x] ET MALWARE Win32/RisePro CnC Server Response M1
- [x] ET MALWARE Win32/RisePro CnC Server Response M3
- [ ] ET MALWARE BatLoader CnC Domain (installationupgrade6 .com) in DNS Lookup
- [ ] ET MALWARE BatLoader CnC Domain (tableau-cloud .com) in DNS Lookup
- [ ] ET MALWARE BatLoader CnC Domain (logmeincloudss .com) in DNS Lookup
- [x] ET MALWARE Win32/Packed.Themida.AAL Checkin
- [x] ET MALWARE Cobalt Strike Related Domain in DNS Lookup (pejapezey .com)
- [x] ET MALWARE Win32/DolphinCape Activity (POST)
- [x] ET MALWARE Observed Pirate Stealer Domain in DNS Lookup (socket .bby .gg)
- [ ] ET MALWARE TA444/Lazarus Related Domain in DNS Lookup (microshare .cloud)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (microshare .cloud)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (auto-protection .cloud)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (smbc-vc .com)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (meeting .work .gd)
- [x] ET MALWARE Observed DangerousPassword Related Domain (www .thecloudnet .org in TLS SNI)
- [ ] ET MALWARE Gamaredon APT Related Domain in DNS Lookup
- [x] ET MALWARE Win32/Valyria Maldoc Payload Request M1
- [ ] ET MALWARE Villain C2 Framework HTTP Command Response
- [x] ET MALWARE DOC/TrojanDownloader.Agent.ARJ Payload Request
- [x] ET MALWARE Villain C2 Framework HTTP Server Response
- [x] ET MALWARE Win32/SocksTroy Session Initiation Attempt M2
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (library .covebooks .com)
- [x] ET MALWARE RedditC2 Related Activity (POST)
- [x] ET MALWARE Cobalt Strike Related Activity (GET)
- [x] ET MALWARE PS/PSRansom Server Status Check (GET)
- [x] ET MALWARE Win32/Sality.NBA Exfil
- [x] ET MALWARE Suspected Golang/Zerobot Websocket Activity (GET)
- [x] ET MALWARE Win32/Goofy Guineapig CnC Activity (GET) M2
- [ ] ET MALWARE Observed DNS Query to Goofy Guineapig Domain (static .tcplog .com)
- [x] ET MALWARE CIA Ransomware - wallpaper/readme retrieval attempt
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (fittingroom .gibbsjewelry .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (brooklands .harteverything .com)
- [x] ET MALWARE Win32/PSW.LdPinch CnC Checkin
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (cloudprotect .us .org)
- [x] ET MALWARE Win32/Phoenix Grabber Sending System Information (POST)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (navyseal .bezmail .com)
- [x] ET MALWARE Charming Kitten APT Related DNS Activity
- [x] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [ ] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (admin-dpsu .org)
- [x] ET MALWARE Win32/RisePro CnC Command Outbound (set_file)
- [x] ET MALWARE Win32/RisePro CnC Command Outbound (get_marks)
- [x] ET MALWARE Win32/RisePro CnC Command Outbound (get_grabbers)
- [x] ET MALWARE Win32/RisePro CnC Activity (GET)
- [x] ET MALWARE Win32/RisePro CnC Server Response M2
- [x] ET MALWARE Win32/Generik.BUTNSNA Checkin

- [ ] ET MALWARE SocGholish Domain in DNS Lookup (governing .beautynic .com)
- [x] ET MALWARE Gamaredon APT Related Activity (POST)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (group5 .corralphacap .com)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .shrubs .emptyisland .pics)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (perspective .abcbarbecue .xyz)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (extcourse .zurvio .com)
- [x] ET MALWARE Antinum WebSockets Start
- [x] ET MALWARE Win32/Drokbk Checkin Activity (GET)
- [ ] ET MALWARE CloudAtlas APT Related Domain in DNS Lookup
- [ ] ET MALWARE Observed DNS Query to Alibaba2044 Domain (service-fatturecloud .de)
- [ ] ET MALWARE Observed DNS Query to Alibaba2044 Domain (downloadpdf-fattura .de)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (taxes .rpacx .com)
- [x] ET MALWARE Observed Glupteba CnC Domain (cdneurops .buzz in TLS SNI)
- [x] ET MALWARE Observed Glupteba CnC Domain (cdneurops .pics in TLS SNI)
- [ ] ET MALWARE Observed Glupteba CnC Domain (getyourgift .life in TLS SNI)
- [ ] ET MALWARE Observed Glupteba CnC Domain (tmetres .com in TLS SNI)
- [ ] ET MALWARE Observed Glupteba CnC Domain (limeprime .com in TLS SNI)
- [x] ET MALWARE Observed Glupteba CnC Domain (cdneurop .cloud in TLS SNI)
- [x] ET MALWARE Observed Glupteba CnC Domain (checkpos .net in TLS SNI)
- [ ] ET MALWARE Observed Glupteba CnC Domain (mastiakele .icu in TLS SNI)
- [ ] ET MALWARE Observed Glupteba CnC Domain (mastiakele .xyz in TLS SNI)
- [x] ET MALWARE Observed Glupteba CnC Domain (cdneurops .shop in TLS SNI)
- [ ] ET MALWARE Observed Glupteba CnC Domain (duniadekho .bar in TLS SNI)
- [x] ET MALWARE Win32/RisePro CnC Command Outbound (get_settings)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (torggissoft .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (hero-files .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (files-rate .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (xx1-files .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (pin-files .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (get-24files .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (m-rise .pro)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (my-rise .cc)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (fvp-files .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (get-files24 .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (greatsofteasy .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (upxlead .com)
- [x] ET MALWARE Gamaredon APT Related Activity (GET)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (office .cdsigner .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (navyseal .digijump .online)
- [x] ET MALWARE Win32/RecordBreaker - Observed UA M5 (23591)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (exclusive .milonopensky .store)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (internship .ojul .com)
- [x] ET MALWARE Antinum HTTP Checkin
- [ ] ET MALWARE CloudAtlas APT Related Domain in DNS Lookup
- [x] ET MALWARE Aurora Stealer Admin Console In HTTP Response
- [ ] ET MALWARE Observed DNS Query to Alibaba2044 Domain (utente .service-fatturecloud .de)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (people .fl2wealth .com)
- [x] ET MALWARE Observed Glupteba CnC Domain (greenphoenix .xyz in TLS SNI)
- [x] ET MALWARE Observed Glupteba CnC Domain (mastiakele .ae .org in TLS SNI)
- [x] ET MALWARE Observed Glupteba CnC Domain (zaoshang .ooo in TLS SNI)
- [x] ET MALWARE Observed Glupteba CnC Domain (zaoshang .ru in TLS SNI)
- [x] ET MALWARE Observed Glupteba CnC Domain (revouninstaller .homes in TLS SNI)
- [ ] ET MALWARE Observed Glupteba CnC Domain (zaoshanghao .su in TLS SNI)
- [x] ET MALWARE Observed Glupteba CnC Domain (zaoshanghaoz .net in TLS SNI)
- [x] ET MALWARE Observed Glupteba CnC Domain (zaoshang .moscow in TLS SNI)
- [x] ET MALWARE Observed Glupteba CnC Domain (cdntokiog .studio in TLS SNI)
- [x] ET MALWARE Observed Glupteba CnC Domain (cdneurops .health in TLS SNI)
- [ ] ET MALWARE Observed Glupteba CnC Domain (mastiakele .cyou in TLS SNI)
- [ ] ET MALWARE Lazarus APT Related Domain in DNS Lookup (professiondesc .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (first-mirror .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (myrise .pro)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (uc-files .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (rate-files .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (webproduct25 .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (best24-files .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (neo-files .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (pickofiles .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (my-rise .pro)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (gg-download .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (vi-files .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (qd-file .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (jojo-files .com)

- [x] ET MALWARE Observed DNS Query to RisePro Domain (vip-space .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (elite-hacks .ru)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (softs-portal .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (gs24softeasy .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (boost-files .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (uni-files .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (pu-file .com)
- [x] ET MALWARE Win32/RisePro CnC Server Response M3
- [x] ET MALWARE Win32/RisePro CnC Server Response M5
- [ ] ET MALWARE TA569 Domain in DNS Lookup (luxurycompare .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (fairu-schnellvpn .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (wmail-service .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (fairu-blog .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (bideo-blog .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (wmail-chat .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (wmail-schnellvpn .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (wmail-cdn .xyz)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (bideo-endpoint .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (fairu-cdn .xyz)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (privatproxy-schnellvpn .xyz)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (privatproxy-chat .xyz)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (bideo-blog .xyz)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (privatproxy-blog .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (bideo-endpoint .xyz)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (wmail-cdn .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (ahoravideo-endpoint .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (ahoravideo-blog .xyz)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (ahoravideo-blog .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (wmail-endpoint .xyz)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (bideo-schnellvpn .xyz)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (fairu-chat .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (fairu-chat .xyz)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (bideo-cdn .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (bideo-chat .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (ahoravideo-chat .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (ahoravideo-chat .xyz)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (files-sender .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (gg-loader .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (factor1right .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (teleportsoft .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (testitsoft .com)
- [x] ET MALWARE Observed DNS Query to RisePro Domain (fixgroupfactor .com)
- [x] ET MALWARE Possible PrivateLoader Payload Request (GET)
- [x] ET MALWARE Win32/RisePro CnC Server Response M4
- [x] ET MALWARE Win32/Uwamson.A!ml CnC Checkin
- [x] ET MALWARE Compromised Chat Application Related User-Agent (Chrorne)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (ahoravideo-schnellvpn .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (privatproxy-blog .xyz)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (bideo-chat .xyz)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (wmail-blog .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (fairu-schnellvpn .xyz)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (ahoravideo-endpoint .xyz)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (wmail-blog .xyz)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (bideo-cdn .xyz)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (fairu-endpoint .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (ahoravideo-schnellvpn .xyz)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (ahoravideo-cdn .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (bideo-schnellvpn .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (privatproxy-endpoint .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (fairu-endpoint .xyz)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (ahoravideo-cdn .xyz)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (privatproxy-chat .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (wmail-endpoint .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (privatproxy-cdn .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (fairu-cdn .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (wmail-chat .xyz)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (fairu-blog .xyz)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (privatproxy-endpoint .xyz)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (privatproxy-schnellvpn .com)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (privatproxy-cdn .xyz)
- [x] ET MALWARE ViperSoftX CnC Domain in DNS Lookup (wmail-schnellvpn .xyz)
- [x] ET MALWARE ViperSoftX HTTP CnC Activity

- [x] ET MALWARE TA444 Domain in DNS Lookup (hoststudio .org)
- [x] ET MALWARE TA444 Related Activity (POST)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (canonical .fmunews .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (passphrase .singinganewsong .com)
- [x] ET MALWARE ActionLoader CnC Domain in DNS Lookup (mejito .ru)
- [x] ET MALWARE ActionLoader CnC Domain in DNS Lookup (cloud-documents .com)
- [x] ET MALWARE ActionLoader CnC Domain in DNS Lookup (azure-tech .pro)
- [x] ET MALWARE ActionLoader CnC Domain in DNS Lookup (ekb .tanzedrom .ru)
- [ ] ET MALWARE linux.backdoor.wordpressexploit.1 CnC Domain (transadforward .icu) in DNS Lookup
- [x] ET MALWARE Observed linux.backdoor.wordpressexploit.1 Domain (gabriellalovecats .com) in TLS SNI
- [x] ET MALWARE Observed linux.backdoor.wordpressexploit.1 Domain (tommyforgreendream .icu) in TLS SNI
- [ ] ET MALWARE linux.backdoor.wordpressexploit.2 CnC Domain (letsmakeparty3 .ga) in DNS Lookup
- [ ] ET MALWARE linux.backdoor.wordpressexploit.2 CnC Domain (lobbydesires .com) in DNS Lookup
- [x] ET MALWARE Observed linux.backdoor.wordpressexploit.2 Domain (clon .collectfasttracks .com) in TLS SNI
- [x] ET MALWARE Observed linux.backdoor.wordpressexploit.2 Domain (count .trackstatisticsss .com) in TLS SNI
- [x] ET MALWARE Observed linux.backdoor.wordpressexploit.2 Domain (deliverygoodstrategies .com) in TLS SNI
- [x] ET MALWARE linux.backdoor.wordpressexploit.1 JS backdoor retrieval
- [x] ET MALWARE linux.backdoor.wordpressexploit.2 JS backdoor retrieval
- [x] ET MALWARE Win32/Aurora Stealer WORK Command
- [x] ET MALWARE Win32/Aurora Stealer Thanks Command
- [x] ET MALWARE Win32/Aurora Stealer Sending System Information
- [x] ET MALWARE Observed PyPI Malicious Library Payload Delivery Domain (h4ck .cfd in TLS SNI)
- [x] ET MALWARE Donot APT Related Domain in DNS Lookup (soundvista .club)
- [x] ET MALWARE Donot APT Related Domain in DNS Lookup (biteupdates .live)
- [x] ET MALWARE Donot APT Related Domain in DNS Lookup (printerupdates .online)
- [x] ET MALWARE Donot APT Related Domain in DNS Lookup (tplinkupdates .space)
- [x] ET MALWARE Donot APT Related Domain in DNS Lookup (lovingallupdates .life)
- [x] ET MALWARE Golang/Sandcat Plugin Activity (POST)
- [x] ET MALWARE Win32/DarkCloud Exfil Over SMTP (Body)
- [x] ET MALWARE MintStealer Discord Activity (GET)
- [x] ET MALWARE MintStealer CnC Activity (GET)
- [ ] ET MALWARE Downloader/Linux.Agent CnC Domain (wget .hostname .help) in DNS Lookup
- [x] ET MALWARE Win32/Youtube Bot - CnC Checkin
- [x] ET MALWARE Turla JS/Kopiluwak Sending Information (POST)
- [x] ET MALWARE Win32/Generik.NWVMNHQ Variant Exfil (POST)
- [x] ET MALWARE Remote Utility Access Tool Key SMTP Exfil
- [x] ET MALWARE Win32/Screenshotter Backdoor CnC Activity (GET)
- [x] ET MALWARE Observed DNS Query to IcedID Domain (dogotungtam .com)
- [x] ET MALWARE Observed DNS Query to IcedID Domain (baherlakerl .online)
- [x] ET MALWARE WinPwn PenTesting Activity
- [x] ET MALWARE NetSupport RAT Domain (tradinghuy .duckdns .org) in DNS Lookup
- [x] ET MALWARE TA444 Domain in DNS Lookup (updatezone .org)
- [x] ET MALWARE TA444 Related CnC Payload Request
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (kinematics .starmidwest .com)
- [x] ET MALWARE ViperSoftX HTTP CnC Activity
- [x] ET MALWARE ActionLoader CnC Domain in DNS Lookup (roskazna .net)
- [x] ET MALWARE ActionLoader CnC Domain in DNS Lookup (kc-3 .ru)
- [x] ET MALWARE ActionLoader CnC Domain in DNS Lookup (xlssmooth .xyz)
- [ ] ET MALWARE linux.backdoor.wordpressexploit.1 CnC Domain (gabriellalovecats .com) in DNS Lookup
- [ ] ET MALWARE linux.backdoor.wordpressexploit.1 CnC Domain (tommyforgreendream .icu) in DNS Lookup
- [x] ET MALWARE Observed linux.backdoor.wordpressexploit.1 Domain (transadforward .icu) in TLS SNI
- [ ] ET MALWARE linux.backdoor.wordpressexploit.2 CnC Domain (clon .collectfasttracks .com) in DNS Lookup
- [ ] ET MALWARE linux.backdoor.wordpressexploit.2 CnC Domain (count .trackstatisticsss .com) in DNS Lookup
- [ ] ET MALWARE linux.backdoor.wordpressexploit.2 CnC Domain (deliverygoodstrategies .com) in DNS Lookup
- [x] ET MALWARE Observed linux.backdoor.wordpressexploit.2 Domain (letsmakeparty3 .ga) in TLS SNI
- [x] ET MALWARE Observed linux.backdoor.wordpressexploit.2 Domain (lobbydesires .com) in TLS SNI
- [x] ET MALWARE linux.backdoor.wordpressexploit.1 CnC Checkin
- [x] ET MALWARE linux.backdoor.wordpressexploit.2 CnC Checkin
- [x] ET MALWARE linux.backdoor.wordpressexploit file upload test
- [x] ET MALWARE Win32/Aurora Stealer Accept Command
- [x] ET MALWARE Rhadamanthys Stealer - Payload Download Request
- [x] ET MALWARE Observed PyPI Malicious Library Payload Delivery Domain (h4ck .cfd) Domain in DNS Lookup
- [x] ET MALWARE Win32/Lumma Stealer Data Exfiltration Attempt M2
- [x] ET MALWARE Donot APT Related Domain in DNS Lookup (resolverequest .live)
- [x] ET MALWARE Donot APT Related Domain in DNS Lookup (biteupdates .site)
- [x] ET MALWARE Donot APT Related Domain in DNS Lookup (printersolutions .live)
- [x] ET MALWARE Donot APT Related Domain in DNS Lookup (packetbite .live)
- [x] ET MALWARE AHK Bot Domain Profiler CnC Activity
- [x] ET MALWARE Win32/DarkCloud Exfil Over SMTP (Subject)
- [x] ET MALWARE MintStealer Discord Activity (GET)
- [x] ET MALWARE MintStealer CnC Activity (GET)
- [x] ET MALWARE MintStealer CnC Activity (POST)
- [ ] ET MALWARE Downloader/Linux.Agent CnC Domain (pateu .freevar .com) in DNS Lookup
- [x] ET MALWARE Redline Stealer TCP CnC Activity
- [x] ET MALWARE Redline Stealer TCP CnC - Id1Response
- [x] ET MALWARE O97M/Sadoca.C!ml Checkin
- [x] ET MALWARE WasabiSeed Backdoor Payload Request (GET)
- [x] ET MALWARE DNS Query to Fake TeamViewer Domain (coldcreekranch .com)
- [x] ET MALWARE Observed DNS Query to IcedID Domain (acehphonnajaya .com)
- [x] ET MALWARE Observed DNS Query to IcedID Domain (ajerlakerl .online)
- [ ] ET MALWARE Vidar Stealer IP Address in DNS Query Response
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .asset .tradingvein .xyz)

- [x] ET MALWARE BLINDEAGLE CnC Domain (laminascol .linkpc .net) in DNS Lookup
- [x] ET MALWARE BLINDEAGLE CnC Domain (systemwin .linkpc .net) in DNS Lookup
- [ ] ET MALWARE IcedID CnC Domain in DNS Lookup
- [ ] ET MALWARE IcedID CnC Domain in DNS Lookup
- [ ] ET MALWARE IcedID CnC Domain in DNS Lookup
- [ ] ET MALWARE IcedID CnC Domain in DNS Lookup
- [x] ET MALWARE Observed IcedID Domain in DNS Lookup (spkdeutshnewsupp .com)
- [x] ET MALWARE Win32/Nitol.A CnC Checkin M3
- [x] ET MALWARE TA444 Related Domain (updatezone .org) in DNS Lookup
- [x] ET MALWARE TA444 Related Domain (autoprotect .gb .net) in DNS Lookup
- [x] ET MALWARE TA444 Related Domain (azure-security .site) in DNS Lookup
- [x] ET MALWARE TA444 Related Domain (thecloudnet .org) in DNS Lookup
- [x] ET MALWARE VectorStealer Data Exfil via Telegram
- [x] ET MALWARE Observed Various Malware Staging Domain (direct-trojan .com in TLS SNI)
- [x] ET MALWARE Magecart Loader Domain in DNS Lookup (2xdepp .com)
- [x] ET MALWARE Magecart Skimmer Domain in DNS Lookup (elon2xmusk .com)
- [x] ET MALWARE Win32/Gamaredon CnC Activity
- [x] ET MALWARE Cobalt Strike Domain in DNS Lookup (fepopeguc .com)
- [x] ET MALWARE Win32/Spy.KeyLogger.RJA Checkin
- [x] ET MALWARE Observed DNS Query to CnC Domain (StrongPity)
- [x] ET MALWARE Win32/Emotet CnC Activity M12 (POST)
- [x] ET MALWARE Magecart Loader Javascript
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (pkusamain .cloud)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (pahtafinlund .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (nigaragusoups .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (needzolapa .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (avoymratax .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (marmelokpa .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (trinazhkoma .club)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (apretakert .com)
- [x] ET MALWARE Win32/Qakbot CnC Activity (POST)
- [x] ET MALWARE BatLoader CnC Domain (grammarlycheck2 .com) in DNS Lookup
- [x] ET MALWARE BatLoader CnC Domain (updateclientssoftware .com) in DNS Lookup
- [x] ET MALWARE BatLoader CnC Domain (24xpixeladvertising .com) in DNS Lookup
- [x] ET MALWARE BatLoader CnC Domain (updatecloudservice1 .com) in DNS Lookup
- [x] ET MALWARE BatLoader CnC Domain (cloudupdatesss .com) in DNS Lookup
- [x] ET MALWARE Observed BatLoader Domain (updatea1 .com) in TLS SNI
- [x] ET MALWARE Observed BatLoader Domain (t1pixel .com) in TLS SNI
- [x] ET MALWARE Observed BatLoader Domain (clodtechnology .com) in TLS SNI
- [x] ET MALWARE Observed BatLoader Domain (externalchecksso .com) in TLS SNI
- [x] ET MALWARE Playful Taurus Malicious SSL Certificate Observed
- [x] ET MALWARE Playful Taurus Observe malicious SSL Cert (self-signed www .netgate .com)
- [x] ET MALWARE BLINDEAGLE CnC Domain (upxsystems .com) in DNS Lookup
- [x] ET MALWARE XDR33 CnC Server SSL Certificate Observed
- [ ] ET MALWARE IcedID CnC Domain in DNS Lookup
- [ ] ET MALWARE IcedID CnC Domain in DNS Lookup
- [ ] ET MALWARE IcedID CnC Domain in DNS Lookup
- [ ] ET MALWARE IcedID CnC Domain in DNS Lookup
- [ ] ET MALWARE Observed IcedID Domain in DNS Lookup (bayernbadabum .com)
- [ ] ET MALWARE Observed DNS Query to TA444/Lazarus Domain (concrecapital .com)
- [x] ET MALWARE TA444 Related Domain (autoprotect .com .de) in DNS Lookup
- [x] ET MALWARE TA444 Related Domain (azure-security .online) in DNS Lookup
- [x] ET MALWARE TA444 Related Domain (hoststudio .org) in DNS Lookup
- [x] ET MALWARE DCRAT Checkin via Telegram
- [ ] ET MALWARE ZeroBot/ZeroStresser Botnet Related Domain in DNS Lookup (zero .sudolite .ml)
- [x] ET MALWARE Various Malware Staging Domain in DNS Lookup (direct-trojan .com)
- [x] ET MALWARE Magecart CnC Domain in DNS Lookup (saylor2xbtc .com)
- [ ] ET MALWARE Observed DNS Query to Xworm Domain (su1d .nerdpol .ovh)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup
- [x] ET MALWARE Cobalt Strike Domain (fepopeguc .com) in TLS SNI
- [x] ET MALWARE Observed DNS Query to CnC Domain (StrongPity)
- [ ] ET MALWARE Magecart Skimmer Domain in DNS Lookup (magento-cdn .net)
- [x] ET MALWARE Observed DNS Query to Mirai Domain (miraistealer .xyz)
- [x] ET MALWARE Magecart Skimmer CSS
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (brakudafear .pics)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (owisportlittle .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (tonikantos .one)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (wendypior .ink)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (stillprunnert .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (likasertik .shop)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (skafiparod .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (wcollopracket .com)
- [x] ET MALWARE Possible Vidar Stealer C2 Config In Steam Profile
- [x] ET MALWARE BatLoader CnC Domain (updatea1 .com) in DNS Lookup
- [x] ET MALWARE BatLoader CnC Domain (t1pixel .com) in DNS Lookup
- [x] ET MALWARE BatLoader CnC Domain (clodtechnology .com) in DNS Lookup
- [x] ET MALWARE BatLoader CnC Domain (externalchecksso .com) in DNS Lookup
- [x] ET MALWARE Observed BatLoader Domain (grammarlycheck2 .com) in TLS SNI
- [x] ET MALWARE Observed BatLoader Domain (updateclientssoftware .com) in TLS SNI
- [x] ET MALWARE Observed BatLoader Domain (24xpixeladvertising .com) in TLS SNI
- [x] ET MALWARE Observed BatLoader Domain (updatecloudservice1 .com) in TLS SNI
- [x] ET MALWARE Observed BatLoader Domain (cloudupdatesss .com) in TLS SNI
- [x] ET MALWARE Playful Taurus CnC Domain (vpnkerio .com) in DNS Lookup
- [x] ET MALWARE Playful Taurus CnC Domain (scm .oracleapps .org) in DNS Lookup

- [x] ET MALWARE Playful Taurus CnC Domain (update .adboeonline .net) in DNS Lookup
- [x] ET MALWARE Playful Taurus CnC Domain (update .delldrivers .in) in DNS Lookup
- [x] ET MALWARE Kimsuky CnC Domain (lifehelper .kr) in DNS Lookup
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (allertmnemonkik .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (wagringamuk .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (windmencherser .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (elcapolis .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (klayerziluska .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (plivetrakoy .com)
- [ ] ET MALWARE IcedID CnC Domain in DNS Lookup (wcollopracket .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (ebothlips .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (qsertopinajil .com)
- [ ] ET MALWARE IcedID CnC Domain in DNS Lookup (trinazhkoma .club)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (golddisco .top)
- [ ] ET MALWARE Observed DOUBLEBACK Related Domain (barricks .org in TLS SNI)
- [x] ET MALWARE Pyramid Framework Payload Request (base-bof.py)
- [x] ET MALWARE Pyramid Framework Payload Request (base-DonPAPI.py)
- [x] ET MALWARE Pyramid Framework Payload Request (base-LaZagne.py)
- [x] ET MALWARE Pyramid Framework Payload Request (base-tunnel-inj.py)
- [x] ET MALWARE Cobalt Strike Activity (GET)
- [x] ET MALWARE DCRat Initial Checkin Server Response M6
- [x] ET MALWARE Win32/Enigma Stealer CnC Checkin
- [x] ET MALWARE Win32/Sventore.B CnC Checkin
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .rendezvous .tophandsome .gay)
- [x] ET MALWARE SLIVER Framework SMB CreateService Default ServiceName
- [x] ET MALWARE Win32/Obsidium Stealer Data Exfiltration Attempt M2
- [x] ET MALWARE Win32/Obsidium Stealer Data Exfiltration Attempt M4
- [x] ET MALWARE Win32/Obsidium Stealer Data Exfiltration Attempt M6
- [x] ET MALWARE Win32/Obsidium Stealer Data Exfiltration Attempt M8
- [x] ET MALWARE Win32/Obsidium Stealer Data Exfiltration Attempt M10
- [x] ET MALWARE Win32/HMR RAT Sending System Information
- [x] ET MALWARE Win32/DoNot Observed UA (Mozilla 105.01.05)
- [x] ET MALWARE Cobalt Strike CnC Domain (r2 .57thandnormal .com) in DNS Lookup
- [ ] ET MALWARE Observed DNS Query to IcedID Domain (swordnifhing .com)
- [ ] ET MALWARE Observed DNS Query to IcedID Domain (trotimera .com)
- [x] ET MALWARE PseudoManuscrypt Activity (POST)
- [x] ET MALWARE Malvirt/KoiVM Downloader Variant Payload Retrieval Request
- [x] ET MALWARE Observed Glupteba CnC Domain (ninhaine .com in TLS SNI)
- [x] ET MALWARE Gamaredon APT Related Activity (GET)
- [x] ET MALWARE Observed APT Actor Payload Domain (e-aks .uz in TLS SNI)
- [x] ET MALWARE ConnectWise ScreenConnect Payload Delivery Domain (win03 .xyz) in DNS Lookup
- [x] ET MALWARE ConnectWise ScreenConnect Payload Delivery Domain (win01 .xyz) in DNS Lookup
- [x] ET MALWARE GCleaner CnC Checkin M1
- [x] ET MALWARE GCleaner CnC Checkin M2
- [x] ET MALWARE Playful Taurus CnC Domain (mail .indiarailways .net) in DNS Lookup
- [x] ET MALWARE Kimsuky Related CnC
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (skaiortalop .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (headertolz .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (ertusaporf .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (dgormiugatox .com)
- [ ] ET MALWARE IcedID CnC Domain in DNS Lookup (needzolapa .com)
- [ ] ET MALWARE IcedID CnC Domain in DNS Lookup (avoymratax .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (june85 .cyou)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (ijoyzymama .com)
- [ ] ET MALWARE IcedID CnC Domain in DNS Lookup (likasertik .shop)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (umousteraton .com)
- [ ] ET MALWARE IcedID CnC Domain in DNS Lookup (brakudafear .pics)
- [ ] ET MALWARE DOUBLEBACK Related Domain in DNS Lookup (barricks .org)
- [x] ET MALWARE Pyramid Framework Payload Request (base-bh.py)
- [x] ET MALWARE Pyramid Framework Payload Request (base-clr.py)
- [x] ET MALWARE Pyramid Framework Payload Request (base-impacket-secretsdump.py)
- [x] ET MALWARE Pyramid Framework Payload Request (base-pythonmemorymodule.py)
- [x] ET MALWARE Pyramid Framework Payload Request (base-tunnel-socks5.py)
- [x] ET MALWARE DCRat Initial Checkin Server Response M5
- [x] ET MALWARE Discord .exe Download URL In HTTP Response
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .betting .cockroachracing .site)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .market .dentureforfree .online)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .signing .unitynotarypublic .com)
- [x] ET MALWARE Win32/Obsidium Stealer Data Exfiltration Attempt M1
- [x] ET MALWARE Win32/Obsidium Stealer Data Exfiltration Attempt M3
- [x] ET MALWARE Win32/Obsidium Stealer Data Exfiltration Attempt M5
- [x] ET MALWARE Win32/Obsidium Stealer Data Exfiltration Attempt M7
- [x] ET MALWARE Win32/Obsidium Stealer Data Exfiltration Attempt M9
- [x] ET MALWARE Observed Glupteba CnC Domain (spolaect .info in TLS SNI)
- [x] ET MALWARE Win32/TradingView CnC Exfil (POST)
- [x] ET MALWARE Cobalt Strike CnC Domain (020 .57thandnormal .com) in DNS Lookup
- [x] ET MALWARE Cobalt Strike CnC Domain (r1 .57thandnormal .com) in DNS Lookup
- [ ] ET MALWARE Observed DNS Query to IcedID Domain (nomaeradiur .com)
- [ ] ET MALWARE Observed DNS Query to IcedID Domain (tibloautonef .com)
- [x] ET MALWARE Luminosity Link Variant CnC Activity (get_failed)
- [x] ET MALWARE Observed Glupteba CnC Domain (nisdably .com in TLS SNI)
- [x] ET MALWARE Gamaredon APT Related Activity (GET)
- [x] ET MALWARE Observed APT Actor Payload Domain (archive-downloader .com in TLS SNI)
- [x] ET MALWARE ConnectWise ScreenConnect Payload Delivery Domain (win02 .xyz) in DNS Lookup
- [x] ET MALWARE ConnectWise ScreenConnect Payload Delivery Domain (win04 .xyz) in DNS Lookup
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (smiles .cahl4u .org)
- [x] ET MALWARE GCleaner Payload Retrieval Attempt
- [x] ET MALWARE Potential GCleaner CnC Checkin

- [x] ET MALWARE GCleaner Downloader - Payload Response
- [ ] ET MALWARE Phorpiex CnC Domain (twizt .org) in DNS Lookup
- [ ] ET MALWARE Ice Breaker Backdoor CnC Domain (ponzix .net) in DNS Lookup
- [ ] ET MALWARE Ice Breaker Backdoor CnC Domain (screenshot .icu) in DNS Lookup
- [ ] ET MALWARE Ice Breaker Backdoor CnC Domain (screenshotcap .com) in DNS Lookup
- [ ] ET MALWARE Observed DNS Query to IcedID Domain (qoipaboni .com)
- [ ] ET MALWARE Observed DNS Query to IcedID Domain (leftcatrheringg .com)
- [ ] ET MALWARE Observed DNS Query to IcedID Domain (headertolz .com)
- [x] ET MALWARE UAC-0114/Winter Vivern Screenshot Upload M2
- [x] ET MALWARE UAC-0114/Winter Vivern CnC Activity
- [x] ET MALWARE Win32/Kumquat Loader Activity (Connect)
- [x] ET MALWARE Win32/Kumquat Loader Activity (Publish)
- [x] ET MALWARE TA430/Andariel ACRES Backdoor Activity (GET)
- [x] ET MALWARE Patchwork APT BADNEWS Variant CnC Checkin M2
- [x] ET MALWARE Suspected NginxSpy Related Request (Inbound)
- [x] ET MALWARE NginxSpy Magic Bytes M1 (Outbound)
- [x] ET MALWARE Win32/Phorpiex Template 8 Active - Outbound Malicious Email Spam
- [x] ET MALWARE Win32/Gamaredon CnC Activity (POST) M1
- [x] ET MALWARE Observed DNS Query to Gamaredon Domain (antargi .ru)
- [x] ET MALWARE Win32/RecordBreaker - Observed UA M6 (01785252112)
- [x] ET MALWARE Win32/RecordBreaker - Observed UA M8 (125122112551)
- [x] ET MALWARE Win32/Spy.Banker.AAGB Checkin
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .samples .muzikcitysound .com)
- [x] ET MALWARE Win32/Disabler.NPR Checkin
- [x] ET MALWARE Win32/CrimsonRAT Activity (Outbound)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (autoprotect .com .se)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (shock .creatingaharmoniouslife .net)
- [ ] ET MALWARE DonotGroup Related Domain in DNS Lookup (records .libutires .info)
- [x] ET MALWARE NewsPenguin Domain in DNS Lookup (windowsupdates .shop)
- [x] ET MALWARE NewsPenguin Domain in DNS Lookup (sailorjobs .world)
- [ ] ET MALWARE Malicious Node.js Module aabquerys payload delivery domain (github .elemecdn .com) in DNS Lookup
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .distributor .techsavvyauto .com)
- [x] ET MALWARE Backdoored Xpopup Domain (xpopup .pe .kr) in DNS Lookup
- [ ] ET MALWARE DonotGroup Pult Downloader Activity M3
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup
- [x] ET MALWARE zgRAT Activity M3
- [ ] ET MALWARE Donot Group Related Domain in DNS Lookup (mayosasa .buzz)
- [x] ET MALWARE Win32/Loader Variant Activity (POST)
- [x] ET MALWARE Donot APT Related Domain in DNS Lookup (blogs .tourseasons .xyz)
- [x] ET MALWARE OSX/iWebUpdate CnC Activity
- [x] ET MALWARE Gamaredon Related Domain in DNS Lookup (gayado .ru)
- [x] ET MALWARE Suspected Lazarus APT Related Activity (GET)
- [ ] ET MALWARE Ice Breaker Backdoor CnC Domain (xn--screnshot-iib .net) in DNS Lookup
- [ ] ET MALWARE Ice Breaker Backdoor CnC Domain (screenshotlite .com) in DNS Lookup
- [ ] ET MALWARE Ice Breaker Backdoor CnC Domain (xn--screnshot-jib .net) in DNS Lookup
- [ ] ET MALWARE Observed DNS Query to IcedID Domain (alijhaborta .com)
- [ ] ET MALWARE Observed DNS Query to IcedID Domain (windmencherser .com)
- [ ] ET MALWARE Observed DNS Query to IcedID Domain (yelsopotre .com)
- [x] ET MALWARE UAC-0114/Winter Vivern Screenshot Upload M1
- [x] ET MALWARE UAC-0114/Winter Vivern File Exfilration
- [x] ET MALWARE Kakfum/COLDSTEEL CnC Beacon M3
- [x] ET MALWARE Win32/Kumquat Loader Activity (Subscribe)
- [x] ET MALWARE Win32/Phorpiex UDP Peer-to-Peer CnC
- [x] ET MALWARE Patchwork APT BADNEWS Variant CnC Checkin M1
- [ ] ET MALWARE Patchwork APT BADNEWS CnC Domain (bingoplant .live) in DNS Lookup
- [x] ET MALWARE NginxSpy Magic Bytes M2 (Inbound)
- [x] ET MALWARE Win32/Phorpiex Template 7 Active - Outbound Malicious Email Spam
- [x] ET MALWARE Win32/Gamaredon CnC Activity (GET)
- [x] ET MALWARE Win32/Gamaredon CnC Activity (POST) M2
- [x] ET MALWARE Observed DNS Query to Gamaredon Domain (mohsengo .shop)
- [x] ET MALWARE Win32/RecordBreaker - Observed UA M7 (1235125521512)
- [x] ET MALWARE Win32/DarkCloud Variant Exfil over SMTP (FirefoxCookies.json)
- [x] ET MALWARE Win32/Comrerop Checkin
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (telemetry .usacyberpages .net)
- [x] ET MALWARE Win32/CrimsonRAT Activity (Inbound)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (safe .doc-share .cloud)
- [x] ET MALWARE UAC-0114/Winter Vivern Redirect
- [x] ET MALWARE Suspected Gamaredon Related Activity (GET)
- [x] ET MALWARE NewsPenguin Domain in DNS Lookup (updates .win32 .live)
- [x] ET MALWARE NewsPenguin CnC Checkin
- [ ] ET MALWARE Cobalt Strike CnC Domain (cdcgov .us) in DNS Lookup
- [ ] ET MALWARE Havoc RAT CnC Domain (zh .googlecdnb .tk) in DNS Lookup
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .picture .mercedesbestphoto .store)
- [ ] ET MALWARE Backdoored Xpopup Domain (xpopup .com) in DNS Lookup
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup
- [x] ET MALWARE Gamaredon APT Related Activity (GET)
- [ ] ET MALWARE Observed Donot Group Relaed Domain (mayosasa .buzz in TLS SNI)
- [ ] ET MALWARE Donot APT Related Domain in DNS Lookup (best .tasterschoice .shop)
- [ ] ET MALWARE Donot APT Related Domain in DNS Lookup (blogs .libraryutilitis .live)
- [x] ET MALWARE Donot Group Downloader Activity (GET)
- [ ] ET MALWARE Dalbit Group CnC Domain (m00nlight .top) in DNS Lookup

- [ ] ET MALWARE Dalbit Group CnC Domain (zxcss .com) in DNS Lookup
- [x] ET MALWARE Likely APT29 Retrieving Payload Embedded In PNG 2
- [x] ET MALWARE Possible APT29 Compressed Payload Download Request
- [x] ET MALWARE APT28 Zebrocy/Zekapab POST Template Structure
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup
- [x] ET MALWARE Win32/frebniis IIS Backdoor Trigger Attempt M2
- [x] ET MALWARE APT37 M2RAT CnC Server Command - URL
- [x] ET MALWARE APT37 M2RAT CnC Server Command - RES
- [x] ET MALWARE APT37 M2RAT CnC Server Command - CMD
- [x] ET MALWARE [SEKOIA.IO] Win32/Stealc C2 Check-in
- [x] ET MALWARE Win32/Stealc Active C2 Responding with browsers Config
- [x] ET MALWARE Win32/Stealc/Vidar Stealer Active C2 Responding with plugins Config
- [x] ET MALWARE Win32/Stealc Submitting Screenshot to C2
- [x] ET MALWARE Win32/WhiskerSpy - Key Material Upload
- [x] ET MALWARE Win32/WhiskerSpy CnC Activity
- [x] ET MALWARE Win32/WhiskerSpy - FTP STOR Command M1
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .calendar .wishmarkets .com)
- [x] ET MALWARE Win32/Snojan Variant Sending System Information (POST)
- [x] ET MALWARE Win32/0xtaRAT CnC Activity M1 (GET)
- [x] ET MALWARE Observed Operation Silent Watch Domain in DNS Lookup (filecloudservices .xyz)
- [x] ET MALWARE Observed Operation Silent Watch Domain in DNS Lookup (avvpassport .info)
- [x] ET MALWARE Gamaredon C2 Domain (a0728173 .xsph .ru) in DNS Lookup
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup
- [x] ET MALWARE Win32/Atlantida Stealer Sending System Information (POST)
- [x] ET MALWARE Golang Aurora Stealer Activity (POST)
- [x] ET MALWARE Observed Malicious Domain in DNS Lookup (wpsupdate .luckfafa .com)
- [x] ET MALWARE Cobalt Strike CnC Domain (taoche .cn .wswebpic .com) in DNS Lookup
- [ ] ET MALWARE Cobalt Strike CnC Domain (alidocs .dingtalk .com .wswebpic .com) in DNS Lookup
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .decision .alshafipdk .com)
- [x] ET MALWARE Observed NimPlant UA (NimPlant)
- [ ] ET MALWARE EvilExtractor Stealer CnC Domain (evilextractor .com) in DNS Lookup
- [x] ET MALWARE PS1Loader Encoded Profiling POST
- [x] ET MALWARE NimPlant Register Activity (GET)
- [x] ET MALWARE NimPlant Register Activity M2 (POST)
- [x] ET MALWARE NimPlant Sending Task (Inbound)
- [x] ET MALWARE Gamaredon APT Related Activity (GET)
- [x] ET MALWARE Win32/S1deload Stealer CnC Checkin
- [ ] ET MALWARE Win32/S1deload Stealer CnC Domain (ytb .dolala .xyz) in DNS Lookup
- [x] ET MALWARE Win32/S1deload Stealer CnC Checkin - Coinminer Payload Retrieval M1
- [x] ET MALWARE Win32/S1deload Stealer CnC Checkin - Coinminer Payload Retrieval M3
- [x] ET MALWARE Win32/S1deload Stealer Data Exfiltration Attempt M2
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .stuff .libertydentalcourse .ca)
- [x] ET MALWARE ReverseRat 3.0 CnC Checkin M2
- [x] ET MALWARE Likely APT29 Retrieving Payload Embedded In PNG
- [ ] ET MALWARE Likely APT29 Retrieving Payload Embedded In PNG 3
- [x] ET MALWARE APT28 DealersChoice CnC Beacon Response
- [x] ET MALWARE APT28 Zebrocy/Zekapab CnC Checkin
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup
- [x] ET MALWARE Win32/frebniis IIS Backdoor Trigger Attempt M1
- [x] ET MALWARE APT37 M2RAT CnC Server Command - OKR
- [x] ET MALWARE APT37 M2RAT CnC Server Command - UPD
- [x] ET MALWARE APT37 M2RAT CnC Server Command - UNI
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (blockchain .shannongougenheim .com)
- [x] ET MALWARE Win32/Stealc Requesting browsers Config from C2
- [x] ET MALWARE Win32/Stealc Requesting plugins Config from C2
- [x] ET MALWARE Win32/Stealc Submitting System Information to C2
- [x] ET MALWARE Win32/WhiskerSpy - Machine ID Registration
- [x] ET MALWARE Win32/WhiskerSpy - Task Request
- [x] ET MALWARE Win32/WhiskerSpy - FTP - Observed Creds
- [x] ET MALWARE Win32/WhiskerSpy - FTP STOR Command M2
- [x] ET MALWARE Win32/Snojan Variant Sending System Information (GET)
- [x] ET MALWARE Villain C2 Framework CnC Exfil (POST)
- [x] ET MALWARE Observed Operation Silent Watch Domain in DNS Lookup (edupoliceam .info)
- [x] ET MALWARE Observed Operation Silent Watch Domain in DNS Lookup (filesindrive .info)
- [x] ET MALWARE Observed Operation Silent Watch Domain in DNS Lookup (mediacloud .space)
- [x] ET MALWARE Gamaredon C2 Domain (f0559838 .xsph .ru) in DNS Lookup
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup
- [x] ET MALWARE Win32/0xtaRAT CnC Activity M2 (GET)
- [x] ET MALWARE WhiteSnake Stealer Sending Data to Telegram (POST)
- [x] ET MALWARE Win32/Plugx CnC Activity (CONNECT)
- [ ] ET MALWARE Cobalt Strike CnC Domain (csc .zte .com .cn .wswebpic .com) in DNS Lookup
- [x] ET MALWARE Win32/Backdoor.Atharvan CnC Checkin
- [x] ET MALWARE WhiteSnake Stealer Response (Inbound)
- [x] ET MALWARE Observed NimPlant Server Response (Inbound)
- [x] ET MALWARE Trojan/Win32.Agent Variant Checkin
- [x] ET MALWARE Win32/Grandoreiro TCP CnC Activity
- [x] ET MALWARE NimPlant Sending Command (Inbound)
- [x] ET MALWARE NimPlant Task Activity (GET)
- [x] ET MALWARE NimPlant Result Activity (POST)
- [x] ET MALWARE Win32/S1deload Stealer CnC Domain (neukoo .top) in DNS Lookup
- [x] ET MALWARE Win32/S1deload Stealer CnC Checkin - Get Tasking
- [ ] ET MALWARE Win32/S1deload Stealer CnC Domain (shopproxy .live) in DNS Lookup
- [x] ET MALWARE Win32/S1deload Stealer CnC Checkin - Coinminer Payload Retrieval M2
- [x] ET MALWARE Win32/S1deload Stealer Data Exfiltration Attempt M1
- [x] ET MALWARE Win32/VB.AAF Checkin
- [x] ET MALWARE ReverseRat 3.0 CnC Checkin M1
- [ ] ET MALWARE Donot Group APT Related Domain in DNS Lookup (briefdeal .buzz)

- [ ] ET MALWARE Observed Donot Group APT Domain (briefdeal .buzz in TLS SNI)
- [ ] ET MALWARE Donot Group APT Related Domain in DNS Lookup (winterhero .buzz)
- [x] ET MALWARE Win32/BUGHATCH SpawnAgent Request (GET) M1
- [x] ET MALWARE Magecart Skimmer Domain in DNS Lookup (rithdigit .cyou)
- [x] ET MALWARE Magecart Skimmer Domain in DNS Lookup (yachtbars .fun)
- [x] ET MALWARE Magecart Skimmer Domain in DNS Lookup (okqtfc1 .org)
- [x] ET MALWARE Magecart Skimmer Domain in DNS Lookup (jquery-node .com)
- [x] ET MALWARE Fake ChatGPT Domain in DNS Lookup (openai-pc-pro .online)
- [ ] ET MALWARE IcedID CnC Domain (neonmilkustaers .com) in DNS Lookup
- [ ] ET MALWARE IcedID CnC Domain (trbiriumpa .com) in DNS Lookup
- [ ] ET MALWARE 8220 Gang CnC Domain (jira .letmaker .top) in DNS Lookup
- [ ] ET MALWARE 8220 Gang CnC Domain (fbi .su1001-2 .top) in DNS Lookup
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (accountability .thefenceanddeckguys .com)
- [x] ET MALWARE Observed BlackLotus SSL Certificate Observed
- [x] ET MALWARE Observed Gootloader Domain in DNS Lookup (jp .imonitorsoft .com)
- [x] ET MALWARE Observed Gootloader Domain in DNS Lookup (kristinee .com)
- [x] ET MALWARE Observed Gootloader Domain in DNS Lookup (kepw .org)
- [x] ET MALWARE Observed Gootloader Domain in DNS Lookup (junk-bros .com)
- [x] ET MALWARE Win32/GenKryptik.GCJX Data Exfiltration Attempt
- [x] ET MALWARE Win32/VBS Backdoor Sending System Information (POST)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (osmanpo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (myuridgo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (orduhanpi .ru)
- [x] ET MALWARE Parallax CnC Activity M18 (set)
- [ ] ET MALWARE Lockbit Ransomware Related Domain (poliovocalist .com) in DNS Lookup
- [x] ET MALWARE Hiatus RAT CnC Checkin
- [ ] ET MALWARE SYS01 Information Stealer CnC Domain (seemlabie .top) in DNS Lookup
- [ ] ET MALWARE SYS01 Information Stealer CnC Domain (oscarnaija .com) in DNS Lookup
- [ ] ET MALWARE SYS01 Information Stealer CnC Domain (mahinetain .top) in DNS Lookup
- [ ] ET MALWARE SYS01 Information Stealer CnC Domain (graeslavur .com) in DNS Lookup
- [ ] ET MALWARE SYS01 Information Stealer CnC Domain (baglamanotalari .com) in DNS Lookup
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (profit .3stepsprofit .com)
- [x] ET MALWARE Observed Emotet Maldoc Retrieving Payload (2023-03-07) M2
- [x] ET MALWARE Gamaredon APT Related Activity (GET)
- [x] ET MALWARE Win32/Luca Stealer Sending System Information via Telegram (GET)
- [ ] ET MALWARE PlugX Related Domain in DNS Lookup (api .imango .ink)
- [ ] ET MALWARE Observed Donot Group APT Domain (winterhero .buzz in TLS SNI)
- [x] ET MALWARE Gamaredon APT Related Activity (GET)
- [x] ET MALWARE Win32/BUGHATCH SpawnAgent Request (GET) M2
- [x] ET MALWARE Magecart Skimmer Domain in DNS Lookup (app-stat .com)
- [x] ET MALWARE Magecart Skimmer Domain in DNS Lookup (antohub .shop)
- [x] ET MALWARE Magecart Skimmer Domain in DNS Lookup (nebiltech .shop)
- [x] ET MALWARE Fake ChatGPT Domain in DNS Lookup (chat-gpt-pc .online)
- [x] ET MALWARE Fake ChatGPT Domain in DNS Lookup (chat-gpt-online-pc .com)
- [ ] ET MALWARE IcedID CnC Domain (whothitheka .com) in DNS Lookup
- [ ] ET MALWARE IcedID CnC Domain (svoykbragudern .com) in DNS Lookup
- [ ] ET MALWARE 8220 Gang CnC Domain (dw .bpdeliver .ru) in DNS Lookup
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (catalog .iroldzyn .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (oxford .courstify .com)
- [x] ET MALWARE Win32/BlackLotus CnC Activity (POST)
- [x] ET MALWARE Observed Gootloader Domain in DNS Lookup (kakiosk .adsparkdev .com)
- [x] ET MALWARE Observed Gootloader Domain in DNS Lookup (jonathanbartz .com)
- [x] ET MALWARE Observed Gootloader Domain in DNS Lookup (lakeside-fishandchips .com)
- [x] ET MALWARE MSIL/PSW.Agent.STP Data Exfiltration Attempt
- [ ] ET MALWARE Maldoc Related Domain in DNS Lookup (nationalweatherserviceapp .com)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (payampo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (muhsingo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (ogtaypi .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (muhtargo .ru)
- [x] ET MALWARE Parallax CnC Response Activity M18
- [x] ET MALWARE Observed Emotet Maldoc Retrieving Payload (2023-03-07) M1
- [x] ET MALWARE SYS01 Information Stealer - CnC Checkin
- [ ] ET MALWARE SYS01 Information Stealer CnC Domain (craceruib .top) in DNS Lookup
- [ ] ET MALWARE SYS01 Information Stealer CnC Domain (caseiden .com) in DNS Lookup
- [ ] ET MALWARE SYS01 Information Stealer CnC Domain (makananwisata .com) in DNS Lookup
- [ ] ET MALWARE SYS01 Information Stealer CnC Domain (rapadtrai .com) in DNS Lookup
- [ ] ET MALWARE SYS01 Information Stealer CnC Domain (seleriti .com) in DNS Lookup
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (use .solqueen .com)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (azure .doc-view .cloud)
- [x] ET MALWARE Gamaredon APT Related Activity (GET)
- [ ] ET MALWARE PlugX Related Domain in DNS Lookup (cdn .imango .ink)
- [x] ET MALWARE Win32/Vector Stealer Sending System Information via Telegram (POST)

- [x] ET MALWARE Hact .be Pentesting CnC Activity
- [x] ET MALWARE Win32/I'm_Better Stealer CnC Command - get_key
- [x] ET MALWARE Observed Emotet Maldoc Retrieving Payload (2023-03-07) M3
- [x] ET MALWARE Observed DNS Query to Cinoshi Stealer Domain (anaida .evisyn .lol)
- [x] ET MALWARE Win32/Cinoshi Stealer Payload Request (GET)
- [x] ET MALWARE Win32/Packed.BlackMoon.A Checkin
- [ ] ET MALWARE SocGholish NetSupport Dropper Domain in DNS Lookup (gybvhxu .top)
- [x] ET MALWARE WorldWind Stealer Sending System information via Telegram (POST)
- [ ] ET MALWARE Prometei Botnet CnC Domain (feefreepool .net) in DNS Lookup
- [x] ET MALWARE Prometei Botnet CnC Checkin - Payload Retrieval
- [x] ET MALWARE Qbot Payload Request (2023-03-13) M1
- [x] ET MALWARE Qbot Payload Request (2023-03-13) M3
- [x] ET MALWARE Qbot Payload Request (2023-03-13) M5
- [x] ET MALWARE Qbot Payload Request (2023-03-13) M7
- [x] ET MALWARE Qbot Payload Request (2023-03-13) M9
- [ ] ET MALWARE Crypto Drainer CnC Domain (pingpongtool .xyz) in DNS Lookup
- [ ] ET MALWARE Crypto Drainer CnC Domain (usdc-circle .com) in DNS Lookup
- [x] ET MALWARE Win32/Root Finder Stealer Sending System Information via Telegram (GET)
- [x] ET MALWARE Win32/HMR RAT Sending System Information M3
- [x] ET MALWARE Amadey Bot Activity (POST) M1
- [x] ET MALWARE Win32/Unknown Stealer CnC Exfil via Telegram M2
- [ ] ET MALWARE Observed DNS Query to LIGHTSHOW Domain (sede .lamarinadevalencia .com)
- [x] ET MALWARE Observed DNS Query to LIGHTSHOW Domain (doug .org)
- [ ] ET MALWARE Observed DNS Query to LIGHTSHOW Domain (webinternal .anyplex .com)
- [ ] ET MALWARE Observed DNS Query to LIGHTSHOW Domain (ruscheltelefonia .com .br)
- [ ] ET MALWARE Observed DNS Query to LIGHTSHOW Domain (keewoom .co .kr)
- [ ] ET MALWARE Observed DNS Query to LIGHTSHOW Domain (mantis .quick .net .pl)
- [ ] ET MALWARE Observed DNS Query to LIGHTSHOW Domain (crickethighlights .today)
- [x] ET MALWARE Linux DarkRadiation Ransomware Telegram Activity M1
- [x] ET MALWARE Possible Linux DarkRadiation Ransomware Telegram Activity
- [x] ET MALWARE Amadey Bot Activity (POST)
- [x] ET MALWARE SideCopy APT Related CnC Response
- [x] ET MALWARE SideCopy APT Related Backdoor Command Inbound (getinfo)
- [ ] ET MALWARE GoBruteForcer CnC Domain (fi .warmachine .su) in DNS Lookup
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (applicatwindomz .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (avroralikhaem .com)
- [x] ET MALWARE Mustang Panda APT Related Activity (GET)
- [x] ET MALWARE Mustang Panda APT Related Activity (POST)
- [x] ET MALWARE Sidecopy APT Related Activity (POST)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (ravaet .ru)
- [x] ET MALWARE Observed DNS Query to Gamaredon Domain (barakal .ru)
- [x] ET MALWARE Observed DNS Query to NanoCore Domain (nanocore2023 .duckdns .org)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .tool .pearldentalgroup .ca)
- [x] ET MALWARE SideCopy APT Related Backdoor Sending System Information (POST)
- [x] ET MALWARE Win32/Cinoshi Stealer Wallet Request (GET)
- [x] ET MALWARE Win32/I'm_Better Stealer CnC Checkin
- [ ] ET MALWARE SocGholish NetSupport CnC Domain in DNS Lookup (itugbjhb .xyz)
- [x] ET MALWARE Gamaredon APT Related Activity (GET)
- [x] ET MALWARE Prometei Botnet CnC DGA - xinchao Pattern
- [x] ET MALWARE Prometei Botnet CnC Checkin
- [x] ET MALWARE Sharp Panda Soul Framework CnC Checkin
- [x] ET MALWARE Qbot Payload Request (2023-03-13) M2
- [x] ET MALWARE Qbot Payload Request (2023-03-13) M4
- [x] ET MALWARE Qbot Payload Request (2023-03-13) M6
- [x] ET MALWARE Qbot Payload Request (2023-03-13) M8
- [x] ET MALWARE Win32/HMR RAT Sending System Information M2
- [ ] ET MALWARE Crypto Drainer CnC Domain (rewards-decentraland .com) in DNS Lookup
- [ ] ET MALWARE Crypto Drainer CnC Domain (redeem-circle .com) in DNS Lookup
- [x] ET MALWARE Win32/AMGO Keylogger - Keylogger Started Message via Telegram (POST)
- [x] ET MALWARE Win32/HMR RAT Sending System Information M4
- [x] ET MALWARE Win32/Unknown Stealer CnC Exfil via Telegram M1
- [x] ET MALWARE SIDESHOW CnC Authentication Over HTTP
- [ ] ET MALWARE Observed DNS Query to LIGHTSHOW Domain (abba-servicios .mx)
- [x] ET MALWARE Observed DNS Query to LIGHTSHOW Domain (fainstec .com)
- [x] ET MALWARE Observed DNS Query to LIGHTSHOW Domain (leadsblue .com)
- [x] ET MALWARE Observed DNS Query to LIGHTSHOW Domain (ajayjangid .in)
- [ ] ET MALWARE Observed DNS Query to LIGHTSHOW Domain (olidhealth .com)
- [ ] ET MALWARE Observed DNS Query to LIGHTSHOW Domain (toptradenews .com)
- [ ] ET MALWARE Observed DNS Query to Kimsuky Domain (mpevalr .ria .monster)
- [x] ET MALWARE Linux DarkRadiation Ransomware Telegram Activity M2
- [x] ET MALWARE Linux DarkRadiation Ransomware Telegram Activity M3
- [x] ET MALWARE SideCopy APT Related Backdoor Sending System Information (GET)
- [x] ET MALWARE SideCopy APT Related Backdoor Victim Response (infoback)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (*.favor.thehouseplantblog.com)
- [x] ET MALWARE Possible GoBruteforcer Payload Retrieval Attempt
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (skanfordiporka .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (villageskaier .com)
- [x] ET MALWARE Mustang Panda APT Related Activity (Response)
- [x] ET MALWARE Mustang Panda APT Related Activity M2 (Response)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (talehgi .ru)
- [x] ET MALWARE Observed DNS Query to Gamaredon Domain (talgatgi .ru)
- [x] ET MALWARE Observed DNS Query to Gamaredon Domain (taysirgi .ru)

- [x] ET MALWARE Observed DNS Query to Gamaredon Domain (takyygi .ru)
- [ ] ET MALWARE Wintern Vivern CnC Domain (marakanas .com) in DNS Lookup
- [ ] ET MALWARE Wintern Vivern CnC Domain (troadsecow .com) in DNS Lookup
- [ ] ET MALWARE Wintern Vivern CnC Domain (security-ocsp .com) in DNS Lookup
- [x] ET MALWARE Winter Vivern APT Aperetif Payload Retrieval Attempt M1
- [x] ET MALWARE Golang/Linux Kaiji Variant Activity
- [ ] ET MALWARE Observed DNS Query To Gamaredon Domain (paratai .ru)
- [ ] ET MALWARE Observed DNSQuery to Gamaredon Domain (omranpo .ru)
- [x] ET MALWARE Fortigate TABLEFLIP Backdoor Trigger - Magic Number Sequence
- [x] ET MALWARE Fortigate THINCRUST Backdoor Activity M2
- [x] ET MALWARE Ares Loader Observed User-Agent M2
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup
- [x] ET MALWARE Win32/keyzetsu Stealer Variant Exfil via Telegram (Response)
- [x] ET MALWARE Win32/Amadey Host Fingerprint Exfil (POST) M1
- [x] ET MALWARE Win32/Amadey Host Fingerprint Exfil (POST) M3
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (gojoxa .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (rasulla .ru)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .language .sebtomato .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (scripts .asi .services)
- [ ] ET MALWARE Observed DNS Query To Gamaredon Domain (raminla .ru)
- [ ] ET MALWARE Observed DNS Query to WinterVivern Domain (ocsp-report .com)
- [ ] ET MALWARE Observed DNS Query to Bad Magic APT Domain (webservice-srv .online)
- [x] ET MALWARE Qbot Payload Request (2023-03-21) M1
- [x] ET MALWARE Qbot Payload Request (2023-03-21) M3
- [x] ET MALWARE Qbot Payload Request (2023-03-21) M5
- [x] ET MALWARE Qbot Payload Request (2023-03-21) M7
- [x] ET MALWARE Qbot Payload Request (2023-03-21) M9
- [x] ET MALWARE DonotGroup Maldoc Activity (GET)
- [ ] ET MALWARE Xaview Stealer Admin Panel Inbound
- [x] ET MALWARE DarkCloud Stealer File Grabber Function Exfiltrating Data via Telegram
- [ ] ET MALWARE SOMNIRECORD CnC Domain in DNS Lookup (dafadfweer .top)
- [x] ET MALWARE SOMNIRECORD Backdoor CMD Command in DNS Query
- [x] ET MALWARE Win64/TrojanDownloader.AHK.CH Checkin
- [x] ET MALWARE Win32/MuggleStealer CnC ChromePwd Exfil (POST)
- [x] ET MALWARE Win32/MuggleStealer CnC DiskInfo Exfil (POST)
- [x] ET MALWARE TrojanDownloader:Win32/Sinresby.B Checkin
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup
- [x] ET MALWARE Win32/Gamaredon Payload Request (GET)
- [x] ET MALWARE LogStih Stealer CnC Checkin
- [x] ET MALWARE WorldWind Stealer Checkin via Telegram (GET)
- [x] ET MALWARE Suspected Muggle Stealer Activity M1
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (cumbersome .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (vohod .ru)
- [ ] ET MALWARE Wintern Vivern CnC Domain (bugiplaysec .com) in DNS Lookup
- [ ] ET MALWARE Wintern Vivern CnC Domain (ocs-romastassec .com) in DNS Lookup
- [ ] ET MALWARE Wintern Vivern CnC Domain (ocspdep .com) in DNS Lookup
- [x] ET MALWARE Winter Vivern APT Aperetif CnC Checkin
- [x] ET MALWARE Winter Vivern APT Aperetif Payload Retrieval Attempt M2
- [ ] ET MALWARE Observed DNS Query To Gamaredon Domain (balatu .ru)
- [ ] ET MALWARE Observed DNS Query To Gamaredon Domain (gokols .ru)
- [ ] ET MALWARE Observed DNSQuery to Gamaredon Domain (orduhanpo .ru)
- [x] ET MALWARE Fortigate THINCRUST Backdoor Activity M1
- [x] ET MALWARE Ares Loader Observed User-Agent M1
- [x] ET MALWARE Ares Loader Checkin
- [x] ET MALWARE Win32/keyzetsu Stealer exfil via Telegram (Response)
- [x] ET MALWARE Konni APT Related Activity (GET)
- [x] ET MALWARE Win32/Amadey Host Fingerprint Exfil (POST) M2
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (makasd .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (baralap .ru)
- [x] ET MALWARE Unknown Powershell Profiler Exfiltrating System Data
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (archive .vibezik .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (trackrecord .wheresbecky .com)
- [ ] ET MALWARE Observed DNS Query To Gamaredon Domain (daglarho .ru)
- [ ] ET MALWARE Observed DNS Query to WinterVivern Domain (ocsp-reloads .com)
- [ ] ET MALWARE Observed DNS Query to Bad Magic APT Domain (webservice-srv1 .online)
- [x] ET MALWARE Qbot Payload Request (2023-03-21) M2
- [x] ET MALWARE Qbot Payload Request (2023-03-21) M4
- [x] ET MALWARE Qbot Payload Request (2023-03-21) M6
- [x] ET MALWARE Qbot Payload Request (2023-03-21) M8
- [ ] ET MALWARE DonotGroup Related Domain in DNS Lookup (roosterguy .online)
- [x] ET MALWARE Win32/ZaRaza Stealer Activity via Telegram (Response)
- [x] ET MALWARE Win32/HookSpoofer Stealer Sending System Information via Telegram (GET)
- [x] ET MALWARE DarkCloud Stealer FirefoxCookies.json Exfiltration via Telegram
- [x] ET MALWARE SOMNIRECORD Backdoor PROBE Command in DNS Query
- [x] ET MALWARE SOMNIRECORD Backdoor DATA Command in DNS Query
- [x] ET MALWARE PennyWise Stealer Data Exfil M2
- [x] ET MALWARE Win32/MuggleStealer CnC Desktop Exfil (POST)
- [x] ET MALWARE Win32/MuggleStealer CnC Wincreds Exfil (POST)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup
- [x] ET MALWARE Observed DNS Query to Gamaredon Domain (sabitpo .ru)
- [x] ET MALWARE LogStih Stealer Data Exfiltration Attempt
- [x] ET MALWARE Snake Keylogger Exfil via SMTP
- [x] ET MALWARE Suspected Muggle Stealer Activity M2
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (narutasx .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (highfalutin .ru)

- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (parsimonious .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (caramelas .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (quizzical .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (heartbreaking .ru)
- [x] ET MALWARE Observed DNS Query to Gamaredon Domain (baoris .ru)
- [x] ET MALWARE Possible Bitter APT Activity (GET)
- [x] ET MALWARE Observed DNS Query to Gamaredon Domain (.ruzipo .ru)
- [x] ET MALWARE Observed DNS Query to Gamaredon Domain (narama .ru)
- [x] ET MALWARE Observed DNS Query to Gamaredon Domain (rustampo .ru)
- [x] ET MALWARE Observed DNS Query to Gamaredon Domain (sabihpo .ru)
- [x] ET MALWARE Observed DNS Query to Gamaredon Domain (savalanpo .ru)
- [x] ET MALWARE Observed DNS Query to Gamaredon Domain (ruslanpo .ru)
- [x] ET MALWARE Vidar Stealer CnC Checkin
- [x] ET MALWARE MacOS/MacStealer Data Exfiltration Attempt
- [x] ET MALWARE Win32/Inido!rts Checkin
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .lap .detroitdragway .com)
- [x] ET MALWARE Win32/PSWStealer Data Exfiltration Attempt
- [x] ET MALWARE Possible 3CX Supply Chain Attack (2023-03-29) Domain Indiciator in DNS Lookup (azuredeploystore .com)
- [x] ET MALWARE Possible 3CX Supply Chain Attack (2023-03-29) Domain Indiciator in DNS Lookup (qwepoi123098 .com)
- [x] ET MALWARE Possible 3CX Supply Chain Attack (2023-03-29) Domain Indiciator in DNS Lookup (msedgepackageinfo .com)
- [x] ET MALWARE Possible 3CX Supply Chain Attack (2023-03-29) Domain Indiciator in DNS Lookup (journalide .org)
- [x] ET MALWARE Possible 3CX Supply Chain Attack (2023-03-29) Domain Indiciator in DNS Lookup (azureonlinestorage .com)
- [x] ET MALWARE Possible 3CX Supply Chain Attack (2023-03-29) Domain Indiciator in DNS Lookup (pbxcloudeservices .com)
- [x] ET MALWARE Possible 3CX Supply Chain Attack (2023-03-29) Domain Indiciator in DNS Lookup (pbxphonenetwork .com)
- [x] ET MALWARE Possible 3CX Supply Chain Attack (2023-03-29) Domain Indiciator in DNS Lookup (pbxsources .com)
- [x] ET MALWARE Possible 3CX Supply Chain Attack (2023-03-29) Domain Indiciator in DNS Lookup (akamaicontainer .com)
- [x] ET MALWARE Possible 3CX Supply Chain Attack (2023-03-29) Domain Indiciator in DNS Lookup (sourceslabs .com)
- [x] ET MALWARE Possible 3CX Supply Chain Attack (2023-03-29) Domain Indiciator in DNS Lookup (glcloudservice .com)
- [x] ET MALWARE Possible 3CX Supply Chain Attack (2023-03-29) Domain Indiciator in DNS Lookup (zacharryblogs .com)
- [x] ET MALWARE Possible 3CX Supply Chain Attack (2023-03-29) Domain Indiciator in DNS Lookup (azureonlinecloud .com)
- [x] ET MALWARE Possible 3CX Supply Chain Attack (2023-03-29) Domain Indiciator in DNS Lookup (dunamistrd .com)
- [x] ET MALWARE Possible 3CX Supply Chain Attack (2023-03-29) Domain Indiciator in DNS Lookup (officestoragebox .com)
- [x] ET MALWARE Possible 3CX Supply Chain Attack (2023-03-29) Domain Indiciator in DNS Lookup (akamaitechcloudservices .com)
- [x] ET MALWARE Possible 3CX Supply Chain Attack (2023-03-29) Domain Indiciator in DNS Lookup (msstorageazure .com)
- [x] ET MALWARE Possible 3CX Supply Chain Attack (2023-03-29) Domain Indiciator in DNS Lookup (visualstudiofactory .com)
- [x] ET MALWARE Possible 3CX Supply Chain Attack (2023-03-29) Domain Indiciator in DNS Lookup (msstorageboxes .com)
- [x] ET MALWARE Possible 3CX Supply Chain Attack (2023-03-29) Domain Indiciator in DNS Lookup (sbmsa .wiki)
- [x] ET MALWARE Possible 3CX Supply Chain Attack (2023-03-29) Domain Indiciator in DNS Lookup (officeaddons .com)
- [x] ET MALWARE Suspected APT43 BITTERSWEET Related Activity (POST)
- [x] ET MALWARE Suspected APT43 BRAVEPRINCE Related Activity (GET)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (same .gleaming8 .battleras .ru)
- [x] ET MALWARE MalDoc/Gamaredon CnC Activity M1
- [x] ET MALWARE MalDoc/Gamaredon CnC Activity M2
- [x] ET MALWARE MalDoc/Gamaredon CnC Activity M3
- [x] ET MALWARE Bitter Elephant APT Related Activity (GET)
- [x] ET MALWARE Suspected APT37 Related Activity (GET)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (saadipo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (sabirpo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (rufatpo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (raidla .ru)
- [ ] ET MALWARE DBatLoader CnC Domain (silverline .com .sg) in DNS Lookup
- [x] ET MALWARE OpcJacker HVNC Variant Magic Packet
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (unit4 .majesticpg .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (examples .propertytax4less .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (life .judyfay .com)
- [x] ET MALWARE Observed 3CX Supply Chain Attack Cookie
- [x] ET MALWARE Observed 3CX Supply Chain Attack Cookie M2
- [x] ET MALWARE APT43 GOLDDRAGON Related Activity (GET)
- [x] ET MALWARE Crashedtech Loader Domain (crashedff .xyz) in DNS Lookup
- [x] ET MALWARE Crashedtech Loader CnC Checkin
- [x] ET MALWARE DorkBot.Downloader CnC Beacon M2
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (agreement .panworldtradersllc .com)
- [x] ET MALWARE Observed 3CX Supply Chain Attack User-Agent
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (earsplitting .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (aydynpo .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (disagreeable .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (undesirable .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (dzhafarho .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (glistening .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (krtkrt .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (materialistic .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (agonizing .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (statuesque .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (haramq .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (jafata .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (stereotyped .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (overjoyed .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (varials .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (capricious .ru)
- [x] ET MALWARE Fake Browser Update via Error Page Loader
- [x] ET MALWARE Fake Browser Update via Error Page Web Inject
- [x] ET MALWARE Fake Browser Update via Error Page Payload
- [ ] ET MALWARE Fake Browser Update Loader Domain in DNS Lookup (infoamanewonliag .online)
- [x] ET MALWARE Win32/SnakeKeyLogger Payload Request (GET)

- [ ] ET MALWARE SnakeKeyLogger Domain in DNS Lookup (xfl .mooo .com)
- [ ] ET MALWARE Malicious NetSupport Loader Domain in DNS Lookup (tumnt .top)
- [ ] ET MALWARE Malicious NetSupport CnC Domain in DNS Lookup (dfrgb .fun)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (aychobanpo .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (altamishpo .ru)
- [x] ET MALWARE Rilide Stealer Domain in DNS Lookup (vceilinichego .ru)
- [x] ET MALWARE Ekipa RAT Domain in DNS Lookup (nch-software .info)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .cloudid .teacherhamish .com)
- [x] ET MALWARE Cylance Ransomware Sending System Information (POST)
- [x] ET MALWARE Win32/Gamaredon CnC Activity (POST) M4
- [x] ET MALWARE Fake Google Chrome Error Domain in DNS Lookup (fastjscdn .org)
- [x] ET MALWARE Fake Google Chrome Error Domain in DNS Lookup (yhdmb .xyz)
- [x] ET MALWARE Win32/Agartha Stealer Activity via Telegram (Response)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (safe .shared-document .cloud)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (arbordeck .co .in)
- [x] ET MALWARE Suspected Tick Group APT Related Activity (GET)
- [x] ET MALWARE MalDoc/Konni APT CnC Activity (GET) M1
- [x] ET MALWARE MalDoc/Konni APT CnC Activity (GET) M3
- [x] ET MALWARE Win32/Spy.Mekotio.ER Checkin
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (sithoparka .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (abigelofraj .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (yhorneedminf .com)
- [x] ET MALWARE Tick Group APT Activity (GET)
- [x] ET MALWARE Win32/TrojanDropper.Agent.SSQ Variant Checkin
- [x] ET MALWARE Win32/StormKitty CnC Telegram Notification M1
- [x] ET MALWARE StormKitty Download Request With Minimal Headers
- [x] ET MALWARE TyphonStealer Exfil via AnonFiles (POST)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .reseller .wonderfulworldblog .com)
- [ ] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (unsuitable .ru)
- [ ] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (hctntmc .ru)
- [x] ET MALWARE Win32/LeftHook Stealer CnC Activity (GET) M1
- [x] ET MALWARE Win32/LeftHook Stealer Browser Extension Config Inbound
- [x] ET MALWARE Win32/LeftHook Stealer CnC Command - get_socket (POST)
- [x] ET MALWARE Win32/LeftHook Stealer Payload Inbound
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (atonpi .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (aktaypo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (amonbo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (aydinpo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (addzhobo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (agshinpo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (akyuldizpo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (alpaslanpo .ru)
- [ ] ET MALWARE Malicious NetSupport CnC Domain in DNS Lookup (irejhg .fun)
- [ ] ET MALWARE Malicious NetSupport Loader Domain in DNS Lookup (rtern .top)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (aykutpo .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (ayzakpo .ru)
- [x] ET MALWARE Rilide Stealer Domain in DNS Lookup (ashgrrwt .click)
- [x] ET MALWARE Aurora Stealer Domain in DNS Lookup (nvidia-graphics .top)
- [x] ET MALWARE VBS/TrojanDownloader.Agent.XAO Payload Inbound
- [x] ET MALWARE KWN Clipper Checkin via Telegram
- [x] ET MALWARE Win32/Gamaredon CnC Activity (POST) M3
- [x] ET MALWARE Win32/QakBot CnC Payload Request (GET)
- [x] ET MALWARE Fake Google Chrome Error Domain in DNS Lookup (chromedistcdn .cloud)
- [x] ET MALWARE Fake Google Chrome Error Domain in DNS Lookup (chrome-error .co)
- [ ] ET MALWARE ClouudAtlas APT Related Domain in DNS Lookup (supportpanel .agent-group .org)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (spirtblockchain .com)
- [x] ET MALWARE Suspected Tick Group APT Related Activity (GET)
- [x] ET MALWARE RaccoonStealer Admin Console Inbound
- [x] ET MALWARE MalDoc/Konni APT CnC Activity (GET) M2
- [x] ET MALWARE Win32/ScarCruf Payload Inbound
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (askamoshopsi .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (tadernost .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (beepkauftagers .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (troffyfrutlot .com)
- [ ] ET MALWARE Donot Domain in DNS Lookup (dripgift .live)
- [x] ET MALWARE Gamaredon APT Maldoc Retrieving Remote Template (GET)
- [x] ET MALWARE Win32/StormKitty CnC Telegram Notification M2
- [x] ET MALWARE TyphonStealer Exfil via Telegram
- [x] ET MALWARE PlutoCrypt Decryption Key Exfil
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (apoligazanattions .com)
- [ ] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (vesterac .ru)
- [ ] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (superficial .ru)
- [x] ET MALWARE RedLine Stealer - CheckConnect Response
- [x] ET MALWARE Win32/LeftHook Stealer CnC Activity (GET) M2
- [x] ET MALWARE Win32/LeftHook Stealer CnC Command - save_cookies (POST)
- [x] ET MALWARE Win32/LeftHook Stealer - CnC Response (get_socket)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (akenatonbo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (anumbo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (asheypi .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (azibobo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (altugpo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (velevas .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (garame .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (adempo .ru)

- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (uranic .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (agasypo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (ayrympo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (aydoganpo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (aktanpo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (aytashpo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (nalogw .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (aytyurkpo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (baharas .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (lefant .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (agakiypo .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (agastanpo .ru)
- [ ] ET MALWARE Observed DNS Query to Nemesis Domain (es-megadom .com)
- [ ] ET MALWARE Observed DNS Query to Nemesis Domain (plus-lema .com)
- [ ] ET MALWARE Observed DNS Query to Nemesis Domain (deveparty .com)
- [ ] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (barakapi .ru)
- [ ] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (badrupi .ru)
- [ ] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (ahmozpi .ru)
- [ ] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (bakaripi .ru)
- [ ] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (akenatonbo .ru)
- [ ] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (asheypi .ru)
- [ ] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (atonpi .ru)
- [ ] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (anumbo .ru)
- [ ] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (aktaypo .ru)
- [ ] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (amonbo .ru)
- [x] ET MALWARE Win32/Fabookie.ek CnC Domain in DNS Lookup
- [x] ET MALWARE Win32/Fabookie.ek CnC Request M4 (GET)
- [ ] ET MALWARE Win32/Fabookie.ek CnC Activity M2
- [x] ET MALWARE Domino Loader CnC Domain (upperdunk .com) in DNS Lookup
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (tet .dnx .capital)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (dmarc .onlineshares .cloud)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (onlineshares .cloud)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (cloud .azurehosting .co)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (altair-vc .com)
- [x] ET MALWARE Observed DNSQuery to TA444 Domain (256ventures .us)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (doc .gdocshare .one)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (down .tomming .us)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (safe .doc-share .pro)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (cloud .j-ic .co)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (inter .gpmtreit .co)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (cloud .j-ic .com)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (fs .digiboxes .us)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (down .j-ic .com)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (internal .j-ic .co)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (down .j-ic .co)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (cloud .gpmtreit .co)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (cloud .mekongcapital .net)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (deck .toyota-ai .org)
- [x] ET MALWARE Observed DNSQuery to TA444 Domain (docsend .me)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (cloud .anobaka .info)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (safe .doc-share .top)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (altair-vc .co .uk)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (protectedviewer .co)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (ms .msteam .biz)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (share .1drvmicrosoft .com)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (down .gpmtreit .us)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (down .gpmtreit .co)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (site .siteshare .me)
- [ ] ET MALWARE Observed DNSQuery to TA444 Domain (cloud .dnx .capital)
- [ ] ET MALWARE Observed DNS Query to TA444 Domain (nbright .best)
- [ ] ET MALWARE FROZENBARENTS (SANDWORM) APT Related Domain in DNS Lookup (cpcpipe .org)
- [ ] ET MALWARE FROZENBARENTS (SANDWORM) APT Related Domain in DNS Lookup (ukroboronprom .com .ukr .pm)
- [ ] ET MALWARE FROZENBARENTS (SANDWORM) APT Related Domain in DNS Lookup (cpcpipe .com)
- [x] ET MALWARE FROZENLAKE (APT 28) Related Domain in DNS Lookup (setnewcreds .ukr .net .frge .io)
- [x] ET MALWARE FROZENLAKE (APT 28) Related Domain in DNS Lookup (robot-876 .frge .io)
- [x] ET MALWARE FROZENLAKE (APT 28) Related Domain in DNS Lookup (ukrprivatesite .frge .io)
- [x] ET MALWARE PUSHCHA Related Domain in DNS Lookup (passport-ua .site)
- [x] ET MALWARE PUSHCHA Related Domain in DNS Lookup (meta-l .space)
- [x] ET MALWARE PUSHCHA Related Domain in DNS Lookup (passport-log .online)
- [x] ET MALWARE Cuba Ransomware Related Domain in DNS Lookup (masterofdigital .org)

- [x] ET MALWARE Cuba Ransomware Related Domain in DNS Lookup (chatgpt4beta .com)
- [x] ET MALWARE Win32/Injector.DYZG Variant Checkin
- [x] ET MALWARE Jasmin Ransomware Panel Activity (Response)
- [x] ET MALWARE Donot Group Activity (GET)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (ewyersbetter .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (nizanigrola .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (pingwiskot .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (klonpiparf .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (skigimeetroc .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (auronavtimor .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (jinowera .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (animamagaznaf .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (plitspiritnox .com)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup
- [ ] ET MALWARE DNS Query to Gamaredon Domain (bankoulpi .ru)
- [ ] ET MALWARE DNS Query to Gamaredon Domain (barutipi .ru)
- [ ] ET MALWARE DNS Query to Gamaredon Domain (apispi .ru)
- [ ] ET MALWARE DNS Query to Gamaredon Domain (anherpi .ru)
- [ ] ET MALWARE DNS Query to Gamaredon Domain (fushiguro .ru)
- [ ] ET MALWARE DNS Query to Gamaredon Domain (22defeated .ayrympo .ru)
- [x] ET MALWARE Roopy File Grabber Exfiltration Attempt
- [x] ET MALWARE JLORAT CnC Checkin
- [x] ET MALWARE Suspected DPRK APT Related Activity (GET)
- [x] ET MALWARE Observed Malicious SSL Cert (AsyncRAT)
- [ ] ET MALWARE DNS Query to Blind Eagle Domain (dfdagsdsag .con-ip .com)
- [x] ET MALWARE ZStealer Admin Panel Inbound
- [ ] ET MALWARE Gamaredon APT Domain in DNS Lookup (ruizchris .ru)
- [ ] ET MALWARE Gamaredon APT Domain in DNS Lookup (valasati .ru)
- [ ] ET MALWARE Gamaredon APT Domain in DNS Lookup (ayarimar .ru)
- [ ] ET MALWARE Gamaredon APT Domain in DNS Lookup (nutriag .ru)
- [ ] ET MALWARE Gamaredon APT Domain in DNS Lookup (vilaverde .ru)
- [ ] ET MALWARE Gamaredon APT Domain in DNS Lookup (fortunyzo .ru)
- [ ] ET MALWARE Gamaredon APT Domain in DNS Lookup (dussaut .ru)
- [ ] ET MALWARE Gamaredon APT Domain in DNS Lookup (samiseto .ru)
- [ ] ET MALWARE Gamaredon APT Domain in DNS Lookup (boraito .ru)
- [ ] ET MALWARE Gamaredon APT Domain in DNS Lookup (enokida .ru)
- [ ] ET MALWARE Gamaredon APT Domain in DNS Lookup (kaigitang .ru)
- [ ] ET MALWARE TA453 Domain in DNS Lookup (update-windows-security .tk)
- [ ] ET MALWARE TA453 Domain in DNS Lookup (sync-system-time .cf)
- [ ] ET MALWARE TA453 Domain in DNS Lookup (oracle-java .cf)
- [ ] ET MALWARE TA453 Domain in DNS Lookup (dns-iprecords .tk)
- [x] ET MALWARE Themedata Embedded OLE Object Maldoc Related Domain in DNS Lookup (support-zabbix .com)
- [x] ET MALWARE Win32/Spy.Banker.ZZN Variant Checkin
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (zalikomanperis .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (alockajilly .com)
- [x] ET MALWARE Suspected Win32/HMR RAT/LOBSHOT Initial Handshake
- [x] ET MALWARE Possible Raspberry Robin Activity M2 (GET)
- [x] ET MALWARE Win32/Cryptbotv2 CnC Activity (POST) M2
- [x] ET MALWARE Atomic macOS (AMOS) Stealer Domain in DNS Lookup (amos-malware .ru)
- [x] ET MALWARE Atomic macOS (AMOS) Stealer Data Exfiltration Attempt
- [x] ET MALWARE TA453 BellaCiao CnC Domain in DNS Lookup (msn-service .co)
- [x] ET MALWARE TA453 BellaCiao CnC Domain in DNS Lookup (msn-center .uk)
- [x] ET MALWARE TA453 BellaCiao CnC Domain in DNS Lookup (maill-support .com)
- [x] ET MALWARE TA453 BellaCiao CnC Domain in DNS Lookup (mailupdate .info)
- [x] ET MALWARE TA453 BellaCiao CnC Domain in DNS Lookup (twittsupport .com)
- [x] ET MALWARE TA453 BellaCiao CnC Domain in DNS Lookup (mail-updateservice .info)
- [x] ET MALWARE TA453 Modified IIS-Raid Backdoor Module Headers in HTTP Request
- [x] ET MALWARE TA453 IIS Credential Stealer Module/Backdoor Headers in HTTP Request
- [x] ET MALWARE TA453 BellaCiao ASPX Backdoor User-Agent in HTTP Request
- [x] ET MALWARE IIS-Raid Module Backdoor Default Headers in HTTP Request
- [x] ET MALWARE IIS-Raid Module Backdoor Ping in HTTP Request
- [ ] ET MALWARE Gamaredon APT Domain in DNS Lookup (nahalx .ru)
- [ ] ET MALWARE Gamaredon APT Domain in DNS Lookup (baraslx .ru)
- [x] ET MALWARE Win32/Phorpiex Template 9 Active - Outbound Malicious Email Spam
- [ ] ET MALWARE Win32/Phorpiex Requesting Compromised Email Credentials List
- [x] ET MALWARE Win32/Cryptbotv2 CnC Activity (POST) M2
- [x] ET MALWARE Donot Group Pult Downloader Activity (POST) M4
- [ ] ET MALWARE Donot Group APT Related Domain in DNS Lookup (pic .onesolution .buzz)
- [x] ET MALWARE Donot Group Pult Downloader Activity (POST) M5
- [ ] ET MALWARE Donot Group APT Related Domain in DNS Lookup (epiczplus .buzz)
- [ ] ET MALWARE DNS Query to MageCart Domain (genlytec .us)
- [ ] ET MALWARE DNS Query to MageCart Domain (pyatiticdigt .shop)
- [ ] ET MALWARE DNS Query to MageCart Domain (shumtech .shop)
- [ ] ET MALWARE DNS Query to MageCart Domain (interytec .shop)
- [ ] ET MALWARE DNS Query to MageCart Domain (stacstocuh .quest)
- [ ] ET MALWARE DNS Query to MageCart Domain (daichetmob .sbs)
- [ ] ET MALWARE DNS Query to MageCart Domain (zapolmob .sbs)
- [x] ET MALWARE MageCart Skimmer Header Observed Outbound
- [ ] ET MALWARE Gamaredon APT Domain in DNS Lookup (decorous .ru)
- [ ] ET MALWARE Gamaredon APT Domain in DNS Lookup (judicious .ru)
- [ ] ET MALWARE Gamaredon APT Domain in DNS Lookup (succinct .ru)
- [ ] ET MALWARE Alloy Taurus APT Related Domain in DNS Lookup (yrhsywu2009 .zapto .org)
- [ ] ET MALWARE Alloy Taurus APT Related Domain in DNS Lookup (vpn729380678 .softether .net)
- [ ] ET MALWARE Alloy Taurus APT Related Domain in DNS Lookup (saspecialforces .co .za)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (bgreenglobus .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (rtofmethough .top)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (alepscoking .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (xairdone .com)
- [x] ET MALWARE MSIL/Whitesnake Variant Stealer Sending System Info via Telegram (GET)
- [ ] ET MALWARE Ducktail Stealer Related Domain in DNS Lookup (techvibeo .com)
- [x] ET MALWARE Havoc Framework Header in HTTP Response
- [ ] ET MALWARE DNS Query to RokRat Domain (link .b4a .app)
- [ ] ET MALWARE DNS Query to RokRat Domain (daum-store .com)
- [ ] ET MALWARE DNS Query to RokRat Domain (docx1 .b4a .app)

- [ ] ET MALWARE DNS Query to RokRat Domain (nate-download .com)
- [x] ET MALWARE DNS Query to RokRat Domain (naver-storage .com)
- [x] ET MALWARE Win32/RokRat CnC Activity (POST)
- [x] ET MALWARE CMDASP Webshell Default Title in HTTP Response
- [ ] ET MALWARE CloudAtlas APT Related Domain in DNS Lookup
- [x] ET MALWARE WarHawk/Spyder Activity (Deploy)
- [x] ET MALWARE TrueBot/Silence.Downloader CnC Checkin 4
- [x] ET MALWARE Suspected CloudAtlas APT Related Activity (GET)
- [x] ET MALWARE Gamaredon APT Related Activity (GET)
- [x] ET MALWARE Win32/BlackSun.B Retrieving Payload
- [x] ET MALWARE Possible Lockbit CnC Checkin
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (z7s .org)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (d0 .wf)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (w0iq .com)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (c0 .wf)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (5v0 .nl)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (s8 .cx)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (b9 .pm)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (6w .re)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (3y .nu)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (5g7 .at)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (1u .pm)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (4j .pm)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (g4 .nu)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (6t .pm)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (u8wp .com)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (9r .re)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (5jb .me)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (n5k .me)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (7yfb .com)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (t7 .nz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (w0 .pm)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (mz3 .biz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (fnx .wf)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (mirw .wf)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (4n .wf)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (0p .rs)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (4xq .nl)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (k5m .co)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (4w .wf)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (bcomb .net)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (e9 .wf)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (5qe8 .com)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (6xj .xyz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (nk0 .club)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (k5j .one)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (1u .wf)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (w4 .rs)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (euya .cn)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (2t .pm)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (nzm .one)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (0i .wf)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (1i .pm)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (q2 .rs)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (2jks .com)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (l0 .wf)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (4j1 .xyz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (k0 .pm)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (ubv5 .com)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (2kbq .com)
- [ ] ET MALWARE DNS Query to RokRat Domain (naver-file .com)
- [x] ET MALWARE Win32/RokRat CnC Activity (GET)
- [x] ET MALWARE CMDASP Webshell Command Request
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .score .symposiumhaiti .com)
- [x] ET MALWARE Win32/WarHawk/Spyder Sending Windows System Information (POST) M2
- [x] ET MALWARE Truebot/Silence.Downloader No Tasking Response from Server
- [x] ET MALWARE DarkCloud Stealer Key Logger Function Exfiltrating Data via Telegram
- [x] ET MALWARE Donot Group Pult Downloader Activity (POST) M6
- [x] ET MALWARE Win32/80mb3rm4n Grabber CnC Exfil via Discord (POST)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (promo .kingdombusinessconnections .com)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (2t .wf)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (6uy .at)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (trzx .eu)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (2yd .eu)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (yuiw .xyz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (lwxa .eu)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (r6 .nz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (c4z .pl)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (y3x .biz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (xz4 .biz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (3e .pm)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (3h1 .xyz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (21k .website)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (h6 .re)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (xtabr .com)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (fgcz .net)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (2j4 .xyz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (kr4 .xyz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (l5k .xyz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (rx3 .xyz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (d4j .club)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (zf0 .ro)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (3h .wf)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (xjam .hk)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (7d .rs)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (s0 .pm)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (4w .pm)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (6y .re)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (n51 .biz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (0j .re)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (fz .ms)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (1j4 .xyz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (oj8 .eu)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (cb3u .com)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (q0 .wf)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (7r6 .nl)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (4k1 .xyz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (6c .nz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (ej3 .xyz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (0j .wf)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (j5m .biz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (60i .nl)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (gz3 .nl)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (w4 .nz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (w6 .nz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (omzk .org)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (jrtz .re)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (8t .pm)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (5j8 .xyz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (u0 .nz)

- ET MALWARE DNS Query to Raspberry Robin Domain (g0 .pm)
- ET MALWARE DNS Query to Raspberry Robin Domain (4w .rs)
- ET MALWARE DNS Query to Raspberry Robin Domain (j1n .me)
- ET MALWARE DNS Query to Raspberry Robin Domain (6ax .nl)
- ET MALWARE DNS Query to Raspberry Robin Domain (ri7 .biz)
- ET MALWARE DNS Query to Raspberry Robin Domain (66j .me)
- ET MALWARE DNS Query to Raspberry Robin Domain (1h3 .me)
- ET MALWARE DNS Query to Raspberry Robin Domain (lwip .re)
- ET MALWARE DNS Query to Raspberry Robin Domain (zxn .fyi)
- ET MALWARE DNS Query to Raspberry Robin Domain (uqw .futbol)
- ET MALWARE DNS Query to Raspberry Robin Domain (6gcr .com)
- ET MALWARE DNS Query to Raspberry Robin Domain (0v .wf)
- ET MALWARE DNS Query to Raspberry Robin Domain (5z .wf)
- ET MALWARE DNS Query to Raspberry Robin Domain (3z .nu)
- ET MALWARE DNS Query to Raspberry Robin Domain (zie5 .com)
- ET MALWARE DNS Query to Raspberry Robin Domain (fxb .tw)
- ET MALWARE DNS Query to Raspberry Robin Domain (vs .gy)
- ET MALWARE DNS Query to Raspberry Robin Domain (0w .pm)
- ET MALWARE DNS Query to Raspberry Robin Domain (m0 .nu)
- ET MALWARE DNS Query to Raspberry Robin Domain (j2 .gy)
- ET MALWARE DNS Query to Raspberry Robin Domain (msix .pm)
- ET MALWARE DNS Query to Raspberry Robin Domain (k5x .xyz)
- ET MALWARE DNS Query to Raspberry Robin Domain (2i .wf)
- ET MALWARE DNS Query to Raspberry Robin Domain (0dz .me)
- ET MALWARE DNS Query to Raspberry Robin Domain (ejk .bz)
- ET MALWARE DNS Query to Raspberry Robin Domain (j4z .xyz)
- ET MALWARE DNS Query to Raspberry Robin Domain (k6c .org)
- ET MALWARE DNS Query to Raspberry Robin Domain (ynns .uk)
- ET MALWARE DNS Query to Raspberry Robin Domain (r0 .wf)
- ET MALWARE DNS Query to Raspberry Robin Domain (bo2sv .com)
- ET MALWARE DNS Query to Raspberry Robin Domain (b3vv .com)
- ET MALWARE DNS Query to Raspberry Robin Domain (iyw5 .com)
- ET MALWARE DNS Query to Raspberry Robin Domain (l6nk .com)
- ET MALWARE DNS Query to Raspberry Robin Domain (2i .nu)
- ET MALWARE DNS Query to Raspberry Robin Domain (6t .re)
- ET MALWARE DNS Query to Raspberry Robin Domain (uz3 .me)
- ET MALWARE DNS Query to Raspberry Robin Domain (uoej .net)
- ET MALWARE DNS Query to Raspberry Robin Domain (4q .pm)
- ET MALWARE DNS Query to Raspberry Robin Domain (c7 .lc)
- ET MALWARE DNS Query to Raspberry Robin Domain (i1 .pm)
- ET MALWARE DNS Query to Raspberry Robin Domain (27o .nl)
- ET MALWARE DNS Query to Raspberry Robin Domain (zk5 .co)
- ET MALWARE DNS Query to Raspberry Robin Domain (v0 .cx)
- ET MALWARE DNS Query to Raspberry Robin Domain (1n4 .xyz)
- ET MALWARE DNS Query to Raspberry Robin Domain (bpyo .in)
- ET MALWARE DNS Query to Raspberry Robin Domain (r0 .pm)
- ET MALWARE DNS Query to Raspberry Robin Domain (j3n .xyz)
- ET MALWARE DNS Query to Raspberry Robin Domain (2i .pm)
- ET MALWARE DNS Query to Raspberry Robin Domain (5kx .me)
- ET MALWARE DNS Query to Raspberry Robin Domain (nt3 .xyz)
- ET MALWARE DNS Query to Raspberry Robin Domain (kglo .link)
- ET MALWARE DNS Query to Raspberry Robin Domain (kjaj .top)
- ET MALWARE DNS Query to Raspberry Robin Domain (z19 .ro)
- ET MALWARE DNS Query to Raspberry Robin Domain (n5 .ms)
- ET MALWARE DNS Query to Raspberry Robin Domain (gloa .in)
- ET MALWARE DNS Query to Raspberry Robin Domain (zi9f .com)
- ET MALWARE DNS Query to Raspberry Robin Domain (8t .wf)
- ET MALWARE DNS Query to Raspberry Robin Domain (g4 .tel)
- ET MALWARE DNS Query to Raspberry Robin Domain (p0 .wf)
- ET MALWARE DNS Query to Raspberry Robin Domain (7k .rs)
- ET MALWARE DNS Query to Raspberry Robin Domain (u0 .pm)
- ET MALWARE DNS Query to Raspberry Robin Domain (l9b .org)
- ET MALWARE DNS Query to Raspberry Robin Domain (i49 .xyz)
- ET MALWARE DNS Query to Raspberry Robin Domain (5ap .nl)
- ET MALWARE DNS Query to Raspberry Robin Domain (glnj .nl)
- ET MALWARE DNS Query to Raspberry Robin Domain (03s30 .com)
- ET MALWARE DNS Query to Raspberry Robin Domain (qmpo .art)
- ET MALWARE DNS Query to Raspberry Robin Domain (4j5 .xyz)
- ET MALWARE DNS Query to Raspberry Robin Domain (q0 .pm)
- ET MALWARE DNS Query to Raspberry Robin Domain (g3 .rs)
- ET MALWARE DNS Query to Raspberry Robin Domain (p9 .tel)
- ET MALWARE DNS Query to Raspberry Robin Domain (dsi .mk)
- ET MALWARE DNS Query to Raspberry Robin Domain (y0 .pm)
- ET MALWARE DNS Query to Raspberry Robin Domain (j8 .si)
- ET MALWARE DNS Query to Raspberry Robin Domain (jjl .one)
- ET MALWARE DNS Query to Raspberry Robin Domain (tz6 .org)
- ET MALWARE DNS Query to Raspberry Robin Domain (tiua .uk)
- ET MALWARE DNS Query to Raspberry Robin Domain (5qw .pw)
- ET MALWARE DNS Query to Raspberry Robin Domain (y0 .wf)
- ET MALWARE DNS Query to Raspberry Robin Domain (t0 .wf)
- ET MALWARE DNS Query to Raspberry Robin Domain (f0 .tel)
- ET MALWARE DNS Query to Raspberry Robin Domain (6t4 .nl)
- ET MALWARE DNS Query to Raspberry Robin Domain (r4e .pl)
- ET MALWARE DNS Query to Raspberry Robin Domain (j4z .co)
- ET MALWARE DNS Query to Raspberry Robin Domain (i6n .xyz)
- ET MALWARE DNS Query to Raspberry Robin Domain (kj1 .xyz)
- ET MALWARE DNS Query to Raspberry Robin Domain (jzm .pw)
- ET MALWARE DNS Query to Raspberry Robin Domain (lgf .pw)
- ET MALWARE DNS Query to Raspberry Robin Domain (6t .nz)
- ET MALWARE DNS Query to Raspberry Robin Domain (j0 .wf)
- ET MALWARE DNS Query to Raspberry Robin Domain (jrx .fr)
- ET MALWARE DNS Query to Raspberry Robin Domain (p3 .ms)
- ET MALWARE DNS Query to Raspberry Robin Domain (u7u .ro)
- ET MALWARE DNS Query to Raspberry Robin Domain (zbs .is)
- ET MALWARE DNS Query to Raspberry Robin Domain (mwgq .net)
- ET MALWARE DNS Query to Raspberry Robin Domain (aij .hk)
- ET MALWARE DNS Query to Raspberry Robin Domain (0i .pm)
- ET MALWARE DNS Query to Raspberry Robin Domain (0x9 .biz)
- ET MALWARE DNS Query to Raspberry Robin Domain (0e .si)
- ET MALWARE DNS Query to Raspberry Robin Domain (6wr9 .com)
- ET MALWARE DNS Query to Raspberry Robin Domain (o7car .com)
- ET MALWARE DNS Query to Raspberry Robin Domain (5jk .club)
- ET MALWARE DNS Query to Raspberry Robin Domain (j4r .xyz)
- ET MALWARE DNS Query to Raspberry Robin Domain (i0 .wf)
- ET MALWARE DNS Query to Raspberry Robin Domain (4aw .ro)
- ET MALWARE DNS Query to Raspberry Robin Domain (j5n .xyz)
- ET MALWARE DNS Query to Raspberry Robin Domain (as3 .biz)
- ET MALWARE DNS Query to Raspberry Robin Domain (rn9v .com)
- ET MALWARE DNS Query to Raspberry Robin Domain (a0 .pm)
- ET MALWARE DNS Query to Raspberry Robin Domain (7d .wf)
- ET MALWARE DNS Query to Raspberry Robin Domain (h0 .pm)
- ET MALWARE DNS Query to Raspberry Robin Domain (vn6 .co)
- ET MALWARE DNS Query to Raspberry Robin Domain (m5n .biz)
- ET MALWARE DNS Query to Raspberry Robin Domain (5z .pm)
- ET MALWARE DNS Query to Raspberry Robin Domain (dj2 .biz)
- ET MALWARE DNS Query to Raspberry Robin Domain (u0 .rs)
- ET MALWARE DNS Query to Raspberry Robin Domain (mnem .wf)
- ET MALWARE DNS Query to Raspberry Robin Domain (i4x .xyz)
- ET MALWARE DNS Query to Raspberry Robin Domain (4m .wf)
- ET MALWARE DNS Query to Raspberry Robin Domain (5qy .ro)
- ET MALWARE DNS Query to Raspberry Robin Domain (ldnr .net)
- ET MALWARE DNS Query to Raspberry Robin Domain (1j .pm)
- ET MALWARE DNS Query to Raspberry Robin Domain (tu6p .com)
- ET MALWARE DNS Query to Raspberry Robin Domain (4s3 .me)
- ET MALWARE DNS Query to Raspberry Robin Domain (3p .ms)
- ET MALWARE DNS Query to Raspberry Robin Domain (6id .xyz)
- ET MALWARE DNS Query to Raspberry Robin Domain (4kx .xyz)
- ET MALWARE DNS Query to Raspberry Robin Domain (k6j .pw)
- ET MALWARE DNS Query to Raspberry Robin Domain (m0 .yt)
- ET MALWARE DNS Query to Raspberry Robin Domain (doem .re)

- [x] ET MALWARE DNS Query to Raspberry Robin Domain (ejk .li)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (wak .rocks)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (ue2 .eu)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (b8x .org)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (jrx .tw)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (vqdn .net)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (gz .qa)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (k1n .club)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (h0 .wf)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (egso .net)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (79r .nl)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (nwz .li)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (w4 .wf)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (pjz .one)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (eznb .net)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (e0 .wf)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (n3 .wf)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (9r .sk)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (krrz .pm)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (g4 .wf)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (n9fz .com)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (nz4 .xyz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (j68 .info)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (4s .pm)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (joysaketshops .com)
- [x] ET MALWARE DNS Query to KEKW Variant Domain (blackcap .ru)
- [x] ET MALWARE Papercut MF/NG User/Group Sync Python Backdoor Trigger
- [x] ET MALWARE Win32/KLBanker Activity (GET)
- [x] ET MALWARE Win32/Ducktail Exfil Via Telegram (POST)
- [x] ET MALWARE Win32/DarkVision RAT CnC Checkin M1
- [x] ET MALWARE Win32/DarkVision RAT CnC Checkin M2
- [ ] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (files-dwn .shop)
- [x] ET MALWARE MrRobot LYON Phish Kit Exfil (POST) M2
- [x] ET MALWARE Globe Imposter Ransomware Activity (GET)
- [x] ET MALWARE MalDoc/TA427 Payload Request (GET)
- [x] ET MALWARE FSB Snake CnC Activity Outbound via TCP (AA23-129A) M2
- [x] ET MALWARE FSB Snake CnC Activity Inbound via TCP (AA23-129A) M2
- [x] ET MALWARE FSB Snake CnC Activity Inbound via TCP (AA23-129A) M4
- [ ] ET MALWARE DNS Query to TA444 Domain (myfirmdocument .online)
- [x] ET MALWARE DNS Query to TA444 Domain (docs-send .online)
- [x] ET MALWARE DNS Query to TA444 Domain (drop-box .cloud)
- [x] ET MALWARE DNS Query to TA444 Domain (altair-vc .info)
- [x] ET MALWARE DNS Query to TA444 Domain (acuitykp .co)
- [x] ET MALWARE DNS Query to TA444 Domain (docsend .business)
- [x] ET MALWARE DNS Query to TA444 Domain (nextera .capital)
- [x] ET MALWARE DNS Query to TA444 Domain (docs-send .cloud)
- [x] ET MALWARE DNS Query to TA444 Domain (sabrpatners .com)
- [x] ET MALWARE DNS Query to TA444 Domain (forumpatners .com)
- [x] ET MALWARE DNS Query to TA444 Domain (docsend-host .cloud)
- [x] ET MALWARE DNS Query to TA444 Domain (j-ic .co .in)
- [x] ET MALWARE DNS Query to TA444 Domain (cryptyk .sytes .net)
- [x] ET MALWARE DNS Query to TA444 Domain (cryptyk .cloud)
- [x] ET MALWARE BPFDoor V2 UDP Magic Packet Inbound
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (li1iv .com)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (13j .me)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (k6j .me)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (1k4 .xyz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (i0up .com)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (zk4 .me)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (2um .xyz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (m0 .wf)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (mzjc .is)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (5kj .xyz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (6j2 .xyz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (iz .gy)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (5s .pm)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (0t .yt)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (skqv .eu)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (mn1 .biz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (zk .qa)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (zjc .bz)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (qji6 .com)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (3lzj .com)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (4c .pm)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (6qo .at)
- [x] ET MALWARE DNS Query to Raspberry Robin Domain (n54 .me)
- [x] ET MALWARE Win32/Umbral-Stealer CnC Exfil via Discord (POST)
- [x] ET MALWARE W32/Snojan.BNQKZQH Payload Inbound
- [x] ET MALWARE DNS Query to KEKW Variant Domain (kekwltd .ru)
- [x] ET MALWARE Papercut MF/NG User/Group Sync FTP Backdoor trigger
- [x] ET MALWARE MSIL/Spyware Activity via Telegram (Response)
- [x] ET MALWARE Win32/Ducktail Exfil Via Telegram CnC Response
- [x] ET MALWARE Win32/DarkVision RAT CnC Checkin M3
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (backroom .tauetaepsilon .org)
- [x] ET MALWARE MrRobot LYON Phish Kit Exfil (POST) M1
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (framework .rankinfiles .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (prototype .siliconvalleyga .com)
- [x] ET MALWARE FSB Snake CnC Activity Outbound via TCP (AA23-129A) M1
- [x] ET MALWARE FSB Snake CnC Activity Inbound via TCP (AA23-129A) M1
- [x] ET MALWARE FSB Snake CnC Activity Inbound via TCP (AA23-129A) M3
- [ ] ET MALWARE DNS Query to TA444 Domain (parallaxdigital .online)
- [ ] ET MALWARE DNS Query to TA444 Domain (morganstanleycorp .co .uk)
- [x] ET MALWARE DNS Query to TA444 Domain (cyberwalletsecurity .online)
- [x] ET MALWARE DNS Query to TA444 Domain (gunosis .global)
- [x] ET MALWARE DNS Query to TA444 Domain (cryptyk .webredirect .org)
- [x] ET MALWARE DNS Query to TA444 Domain (doc .linkpc .net)
- [x] ET MALWARE DNS Query to TA444 Domain (werfaultserver .com)
- [x] ET MALWARE DNS Query to TA444 Domain (companydeck .cloud)
- [x] ET MALWARE DNS Query to TA444 Domain (docs-send .com)
- [x] ET MALWARE DNS Query to TA444 Domain (cryptyk .online)
- [x] ET MALWARE DNS Query to TA444 Domain (autoupdatecheck .work .gd)
- [x] ET MALWARE DNS Query to TA444 Domain (hyperchaincapital .online)
- [x] ET MALWARE DNS Query to TA444 Domain (docupload .site)
- [x] ET MALWARE DNS Query to TA444 Domain (companydeck .online)
- [x] ET MALWARE BPFDoor V2 TCP Magic Packet Inbound
- [x] ET MALWARE BPFDoor V2 SCTP Magic Packet Inbound

- [ ] ET MALWARE SocGholish Domain in DNS Lookup (product .sammyhallam .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (support .newshoop .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (books .friendsofthefolsomlibrary .org)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (jobdescription .us .com)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (doc-send .online)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (contractresearch .blog)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (shared-document .cloud)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (contract-research .blog)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (doc-send .com)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (verifydocument .online)
- [ ] ET MALWARE DNS Query to Glupteba Domain (geofaps .com)
- [ ] ET MALWARE DNS Query to Glupteba Domain (cdneurops .health)
- [x] ET MALWARE Win32/Arid Gopher CnC Exfil (POST)
- [x] ET MALWARE DNS Query to Gamaredon Domain (kaziyapa .ru)
- [x] ET MALWARE DNS Query to Gamaredon Domain (80delay .dzhabaripa .ru)
- [x] ET MALWARE DNS Query to Gamaredon Domain (zaherpa .ru)
- [x] ET MALWARE DNS Query to Gamaredon Domain (iknatonpa .ru)
- [x] ET MALWARE DNS Query to Gamaredon Domain (dzhabaripa .ru)
- [ ] ET MALWARE Fake Quickbooks Domain in DNS Lookup (quickbooks12 .hopto .org)
- [ ] ET MALWARE Fake Quickbooks Domain in DNS Lookup (quickbooks149 .hopto .org)
- [x] ET MALWARE Win32/Amadey Payload Request (GET)
- [x] ET MALWARE Win32/Packed.BlackMoon.A Variant Checkin
- [x] ET MALWARE Stellar Stealer Data Exfiltration Attempt M2
- [x] ET MALWARE Stellar Stealer Data Exfiltration Attempt M4
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .accounting .bridgemastersllc .com)
- [ ] ET MALWARE DonotGroup Maldoc Activity (GET)
- [x] ET MALWARE DonotGroup Maldoc Activity (GET)
- [x] ET MALWARE Win32/BeamWinHTTP CnC Activity M2 (GET)
- [x] ET MALWARE BotLoader CnC Checkin
- [x] ET MALWARE DeltaStealer CnC Domain (deltastealer .xyz) in DNS Lookup
- [x] ET MALWARE Observed DeltaStealer Domain (deltaproject .us) in TLS SNI
- [x] ET MALWARE Observed DeltaStealer Domain (deltastealer .gq) in TLS SNI
- [x] ET MALWARE DeltaStealer CnC Checkin
- [ ] ET MALWARE TA427 Related Domain in DNS Lookup (com-people .click)
- [ ] ET MALWARE TA427 Related Domain in DNS Lookup (com-www .click)
- [ ] ET MALWARE TA427 Related Domain in DNS Lookup (com-otp .click)
- [ ] ET MALWARE TA427 Related Domain in DNS Lookup (kr-me .click)
- [ ] ET MALWARE TA427 Related Domain in DNS Lookup (cf-health .click)
- [x] ET MALWARE Suspected Kimsuky Related Actvity (GET)
- [x] ET MALWARE Suspected Gamaredon Related Maldoc Activity M2
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (vip .dueprocess .us)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (broadcast .ninemuses .io)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (forum .leewhitman-raymond .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (games .iglesiaelarca .org)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (achievements .ritagamer .com)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (cryptofundsresearch .com)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (cryptyk .info)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (bdcc .bio)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (espcapital .co .in)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (javarepo .net)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (gumi-cryptos .loan)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (smart-contracts .blog)
- [x] ET MALWARE DNS Query to SmokeLoader Domain (potunulit .org)
- [ ] ET MALWARE DNS Query to Glupteba Domain (twopixis .com)
- [ ] ET MALWARE DNS Query to Glupteba Domain (beegolang .com)
- [x] ET MALWARE DNS Query to Gamaredon Domain (kahotepa .ru)
- [x] ET MALWARE DNS Query to Gamaredon Domain (OpenAsTextStream .zuberipa .ru)
- [x] ET MALWARE DNS Query to Gamaredon Domain (71delay .dzhahipa .ru)
- [x] ET MALWARE DNS Query to Gamaredon Domain (goruspa .ru)
- [x] ET MALWARE DNS Query to Gamaredon Domain (dzhahipa .ru)
- [x] ET MALWARE DNS Query to Gamaredon Domain (zuberipa .ru)
- [ ] ET MALWARE Fake Quickbooks Domain in DNS Lookup (findproadvisors .com)
- [x] ET MALWARE Win32/Amadey Bot Activity (POST) M2
- [x] ET MALWARE Camaro Dragon APT - Horse Shell CnC Checkin
- [x] ET MALWARE Stellar Stealer Data Exfiltration Attempt M1
- [x] ET MALWARE Stellar Stealer Data Exfiltration Attempt M3
- [x] ET MALWARE Stellar Stealer Data Exfiltration Attempt M5
- [ ] ET MALWARE DonotGroup Related Domain in DNS Lookup (lovebirdsshop .club)
- [x] ET MALWARE Gamaredon APT Related Activity (GET)
- [ ] ET MALWARE DonotGroup Maldoc Activity (GET)
- [x] ET MALWARE BotLoader Retrieving Additional Payloads
- [x] ET MALWARE DeltaStealer CnC Domain (deltaproject .us) in DNS Lookup
- [x] ET MALWARE DeltaStealer CnC Domain (deltastealer .gq) in DNS Lookup
- [x] ET MALWARE Observed DeltaStealer Domain (deltastealer .xyz) in TLS SNI
- [x] ET MALWARE DeltaStealer Exfiltrating Data to gofile .io
- [ ] ET MALWARE SparkRAT Related Domain in DNS Lookup (gwekekccef .webull .day)
- [ ] ET MALWARE TA427 Related Domain in DNS Lookup (com-price .space)
- [ ] ET MALWARE TA427 Related Domain in DNS Lookup (com-def .asia)
- [ ] ET MALWARE TA427 Related Domain in DNS Lookup (de-file .online)
- [ ] ET MALWARE TA427 Related Domain in DNS Lookup (com-port .space)
- [ ] ET MALWARE TA427 Related Domain in DNS Lookup (kr-angry .click)
- [x] ET MALWARE Suspected Gamaredon Related Maldoc Activity M1
- [x] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (tube .saltminecomics .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (commercial .tedgorka .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (teaching .eduvisuo .com)

- [ ] ET MALWARE SocGholish Domain in DNS Lookup (round .macayafoundation .org)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (friends .foflib .org)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (assist .cabinetelcea .com)
- [x] ET MALWARE Win64/Rozena.TD Variant CnC Activity (GET)
- [x] ET MALWARE UAC-0063 Domain in DNS Lookup (diagnostic-resolver .com)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (mbiziso .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (koseyso .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (kuaashiso .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (maatso .ru)
- [ ] ET MALWARE CloudWizard APT Related Domain in DNS Lookup (curveroad .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (internal .metro1properties .us)
- [ ] ET MALWARE DNS Query to Cobalt Strike Domain (aicsoftware .com)
- [x] ET MALWARE DNS Query to IcedID Domain (guaracheza .pics)
- [x] ET MALWARE DNS Query to IcedID Domain (simipimi .com)
- [x] ET MALWARE DNS Query to IcedID Domain (stayersa .art)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (initiatives .ayitiexpo .com)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .offer .rpacxtaxappeal .com)
- [x] ET MALWARE Win32/RootTeam Stealer CnC Exfil M1
- [x] ET MALWARE WhiteSnake Stealer Telegram Checkin
- [x] ET MALWARE Suspected Gamaredon APT Related Activity
- [x] ET MALWARE pswshopro_bot Stealer data exfiltration attempt
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (sapphire .abogados .services)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (archives .finanpress .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (practices .bodyandsoulmassage .com)
- [x] ET MALWARE [ANY.RUN] LgoogLoader Retrieving Config File
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (background .bodyguardchicago .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (masterclass .teamupnetwork .org)
- [x] ET MALWARE [ANY.RUN] Observed Malicious Powershell Related Activity (GET)
- [x] ET MALWARE Observed DNS Query to Gamaredon Domain (rashidiso .ru)
- [x] ET MALWARE Observed DNS Query to Gamaredon Domain (neferzi .ru)
- [x] ET MALWARE Observed DNS Query to Gamaredon Domain (minkazi .ru)
- [x] ET MALWARE Observed DNS Query to Gamaredon Domain (panahaziso .ru)
- [x] ET MALWARE Observed DNS Query to Gamaredon Domain (nebibizi .ru)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (static .laytonroadconstruction .com)
- [x] ET MALWARE Win32/DarkPink KamiKakaBot CnC Exfil (POST)
- [x] ET MALWARE [DCSO] Possible Andariel Exfil Activity
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (havxcq .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (okparaso .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (ozirisso .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (oddzhiso .ru)
- [x] ET MALWARE SocGholish Domain in DNS Lookup (trademark .iglesiaelarca .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (training .defcon1 .us)
- [x] ET MALWARE [ANY.RUN] RCRU64 Ransomware Variant CnC Activity
- [x] ET MALWARE UAC-0063 Domain in DNS Lookup (net-certificate .services)
- [x] ET MALWARE UAC-0063 Domain in DNS Lookup (ms-webdav-miniredir .com)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (kontarso .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (menesso .ru)
- [ ] ET MALWARE Observed DNS Query to Gamaredon Domain (lizimbaso .ru)
- [x] ET MALWARE Kraken Stealer SMTP Data Exfiltration Attempt
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (booty .midatlanticlaw .org)
- [ ] ET MALWARE DNS Query to Cobalt Strike Domain (iconnectgs .com)
- [x] ET MALWARE DNS Query to IcedID Domain (kicknocisd .com)
- [x] ET MALWARE DNS Query to IcedID Domain (curabiebarristie .com)
- [x] ET MALWARE DNS Query to IcedID Domain (belliecow .wiki)
- [x] ET MALWARE Cobalt Strike CnC Beacon (POST)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (reporting .theamericasfashionfest .com)
- [x] ET MALWARE Bandit Stealer Data Exfiltration Attempt
- [x] ET MALWARE [ANY.RUN] WhiteSnake Stealer Reporting Request (Outbound)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (strategy .transversalgroup .co)
- [x] ET MALWARE pswshopro_bot Stealer CnC Checkin
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (enterprise .alliantlaw .us)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (exclusive .transversalbranding .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (deploy .vanquicktech .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (old .onepercentage .org)
- [x] ET MALWARE BellaCiao ASPX Backdoor Response
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (hardware .deltavis .com)
- [x] ET MALWARE [ANY.RUN] RedLine Stealer/MetaStealer Family Related (MC-NMF Authorization)
- [x] ET MALWARE Redline Stealer/MetaStealer Family Activity (Response)
- [x] ET MALWARE Observed DNS Query to Gamaredon Domain (mhotepzi .ru)
- [x] ET MALWARE Observed DNS Query to Gamaredon Domain (naborzi .ru)
- [x] ET MALWARE Observed DNS Query to Gamaredon Domain (nahtizi .ru)
- [x] ET MALWARE Observed DNS Query to Gamaredon Domain (nebtoizi .ru)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (failure .mathgeniusa .com)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .nodes .gammalambdalambda .org)
- [x] ET MALWARE [DCSO] Andariel Exfil Activity
- [x] ET MALWARE [DCSO] Andariel CnC Activity, Check String
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (ozaharso .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (omariso .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (remmaoso .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (itoram .ru)

- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (rvawc .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (xopekar .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (blootundicht .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (boptizol .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (viratuk .ru)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (stockroom .baybeboutiquellc .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (prepare .dawarel3mda .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (reception .q-dent .com)
- [x] ET MALWARE Redline Stealer TCP CnC Activity
- [x] ET MALWARE Redline Stealer/MetaStealer Family TCP CnC Activity - MSValue (Response)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (donkorpa .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (neythzi .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (dakareypa .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (muhvanazi .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (keymnvatipa .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (luzidzhso .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (trulazek .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (porotad .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (galofad .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (mensaso .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (kemnebipa .ru)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (templates .jdlaytongrademaker .com)
- [x] ET MALWARE Sharp Panda APT RTF Retrieval (Response)
- [x] ET MALWARE [ANY.RUN] Win32/ObserverStealer CnC Activity (Screenshot)
- [x] ET MALWARE [ANY.RUN] Win32/ObserverStealer CnC Activity (Check-in)
- [x] ET MALWARE [ANY.RUN] Win32/ObserverStealer CnC Activity (END)
- [x] ET MALWARE Possible MEME#4CHAN Exfil Activity
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (illustrations .ipocla .org)
- [x] ET MALWARE CMDEmber Backdoor Style Request
- [x] ET MALWARE [ANY.RUN] Win32/ObserverStealer CnC Activity (Loading) M2
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (cosplay .univisuo .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (roadmap .jufp .com)
- [x] ET MALWARE IIS-Raid Module Backdoor - INJ Command in HTTP Request
- [x] ET MALWARE Win32/0xtaRAT CnC Activity M3 (GET)
- [x] ET MALWARE Win32/0xtaRAT CnC Activity M5 (POST)
- [ ] ET MALWARE Observed Maldoc Macro Request (GET)
- [x] ET MALWARE Suspected Stealth Soldier Backdoor Related Activity M2 (GET)
- [x] ET MALWARE Suspected Stealth Soldier Backdoor Related Activity M4 (GET)
- [ ] ET MALWARE Stealth Soldier Backdoor Related Domain in DNS Lookup (filestoragehub .live)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (perccottuspi .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (dzhabrailho .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (reyyfadsf .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (bladefishpi .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (gawcq .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (albacorepi .ru)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (specific .autonerdmobilerepairs .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (form .haysllc .net)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (gajasx .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (nalfas .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (tulocal .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (yorisant .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (reposant .ru)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (collaboration .porchlightcs .org)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (dashboard .smartmetereducationnetwork .com)
- [x] ET MALWARE Redline Stealer Stager WebPage Inbound
- [x] ET MALWARE Redline Stealer/MetaStealer Family TCP CnC Activity - MSValue (Outbound)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (kafiripa .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (badarus .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (mudadazi .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (ishakpa .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (kemoziripa .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (butiram .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (karoanpa .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (idogbpa .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (dzhibeydpa .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (dzhumoukpa .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (knemuso .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (imenandpa .ru)
- [x] ET MALWARE Sharp Panda APT Style RTF Request (GET)
- [x] ET MALWARE Observed Sharp Panda APT Related Activity M2
- [x] ET MALWARE [ANY.RUN] Win32/ObserverStealer CnC Activity (System Information)
- [x] ET MALWARE [ANY.RUN] Win32/ObserverStealer CnC Activity (Activity)
- [x] ET MALWARE [ANY.RUN] Win32/ObserverStealer CnC Response
- [x] ET MALWARE MEME#4CHAN Redirect Activity to Payload
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (wholesale .surewareusa .com)
- [x] ET MALWARE [ANY.RUN] Win32/ObserverStealer CnC Activity (Loading) M1
- [x] ET MALWARE Cobalt Strike Domain in DNS Lookup
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (portable .nodirtyelectricity .com)
- [x] ET MALWARE IIS-Raid Module Backdoor - Successful PING in HTTP Response (PONG)
- [x] ET MALWARE IIS-Raid Module Backdoor - Successful INJ Command in HTTP Response
- [x] ET MALWARE Win32/0xtaRAT CnC Activity M4 (GET)
- [x] ET MALWARE [ANY.RUN] Win32/DynamicRAT CnC Activity
- [x] ET MALWARE Suspected Stealth Soldier Backdoor Related Activity M1 (GET)
- [x] ET MALWARE Suspected Stealth Soldier Backdoor Related Activity M3 (GET)
- [x] ET MALWARE Stealth Soldier Backdoor Related Activity M1 (POST)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (gawsxc .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (razuiso .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (tispai .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (dumerilipi .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (spatulapi .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (agonepi .ru)
- [x] ET MALWARE Trojan.PSW.Autoit Data Exfiltration Attempt
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (mentoring .yogayield .net)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (forbes .firstmillionaires .com)

- [ ] ET MALWARE SocGholish Domain in DNS Lookup (names .expressyourselfesthetics .com)
- [x] ET MALWARE Asylum Ambuscade Related CnC Activity (GET) M1
- [x] ET MALWARE Asylum Ambuscade Related CnC Activity (GET) M3
- [x] ET MALWARE Asylum Ambuscade Related CnC Activity (install)
- [x] ET MALWARE Successful Win32/TrojanDownloader.VB.RUI Exfil Activity M2
- [x] ET MALWARE Kimsuky ReconShark Payload Retrieval Request M1
- [x] ET MALWARE Kimsuky ReconShark Related APT Activity
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (ibm .deltavis .net)
- [x] ET MALWARE GreetingGhoul Stealer Domain in DNS Lookup (cryptohedgefund .us)
- [x] ET MALWARE [ANY.RUN] RisePro TCP (External IP)
- [x] ET MALWARE [ANY.RUN] RisePro TCP (Activity)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (toolkit .mobileautorepairmechanic .com)
- [x] ET MALWARE [Mandiant] UNC4841 SEASPY Backdoor Activity M1
- [ ] ET MALWARE [Mandiant] UNC4841 SEASPY Backdoor Activity M3
- [ ] ET MALWARE [Mandiant] UNC4841 SEASPY Backdoor Activity M5
- [ ] ET MALWARE [Mandiant] UNC4841 SEASPY Backdoor Activity M7
- [x] ET MALWARE UNC4841 Related Domain in DNS Lookup (goldenunder .com)
- [x] ET MALWARE UNC4841 Related Domain in DNS Lookup (singamofing .com)
- [x] ET MALWARE UNC4841 Related Domain in DNS Lookup (troublendsef .com)
- [x] ET MALWARE UNC4841 Related Domain in DNS Lookup (gesturefavour .com)
- [x] ET MALWARE GreetingGhoul Stealer CnC Exfil (POST)
- [x] ET MALWARE Mystic Stealer C2 Client Hello Packet
- [x] ET MALWARE LegionLoader CnC Domain (legions .win) in DNS Lookup
- [x] ET MALWARE LegionLoader Activity Observed (LegionClient)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .rfc .zitoprohealth .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (nerfgamesarche .com)
- [x] ET MALWARE Observed Glupteba CnC Domain (deepsound .live in TLS SNI)
- [x] ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
- [x] ET MALWARE Suspected Kimsuky Activity (POST)
- [x] ET MALWARE Suspected Kimsuky Related Activity (Response)
- [x] ET MALWARE Possible DarkFinger Payload Retrieval Attempt - ps10
- [x] ET MALWARE Possible DarkFinger tasklist Retrieval attempt
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (described .moraver .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (artwork .siddavisart .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (career .humandesigns .com)
- [x] ET MALWARE Suspected Blackmoon Related Activity (GET)
- [x] ET MALWARE [ANY.RUN] Win32/Lumma Stealer Configuration Request Attempt
- [x] ET MALWARE DNS Query to SupremeBot Domain (shadowlegion .duckdns .org)
- [x] ET MALWARE Win32/SupremeBot CnC Checkin (POST) M1
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (namibbo .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (bukatam .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (totalav .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (gutarax .ru)
- [x] ET MALWARE [ANY.RUN] Possible Gh0stRat Checkin
- [x] ET MALWARE [ANY.RUN] Gh0stBins RDP Remote Connection
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (superposition .mathgeniusacademy .com)
- [x] ET MALWARE Asylum Ambuscade Related CnC Activity (GET) M2
- [x] ET MALWARE Asylum Ambuscade Related CnC Activity (SendLog)
- [x] ET MALWARE Successful Win32/TrojanDownloader.VB.RUI Exfil Activity M1
- [x] ET MALWARE Win32/TrojanDownloader.VB.RUI Checkin
- [x] ET MALWARE Kimsuky ReconShark Payload Retrieval Request M2
- [x] ET MALWARE Kimsuky HTA Payload Retrieval Attempt
- [ ] ET MALWARE APT-C-36 Related Domain in DNS Lookup (travel-ag .com)
- [x] ET MALWARE [ANY.RUN] RisePro TCP (Token)
- [x] ET MALWARE [ANY.RUN] RisePro TCP v.0.x (Get_settings)
- [x] ET MALWARE [ANY.RUN] RisePro TCP (Exfiltration)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (webdog .ilinkads .com)
- [x] ET MALWARE [Mandiant] UNC4841 SEASPY Backdoor Activity M2
- [ ] ET MALWARE [Mandiant] UNC4841 SEASPY Backdoor Activity M4
- [ ] ET MALWARE [Mandiant] UNC4841 SEASPY Backdoor Activity M6
- [x] ET MALWARE UNC4841 Related Domain in DNS Lookup (togetheroffway .com)
- [x] ET MALWARE UNC4841 Related Domain in DNS Lookup (fessionalwork .com)
- [x] ET MALWARE UNC4841 Related Domain in DNS Lookup (bestfindthetruth .com)
- [x] ET MALWARE UNC4841 Related Domain in DNS Lookup (singnode .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (subscription .provijuns .com)
- [x] ET MALWARE Mystic Stealer Admin Panel 2023-06-16
- [ ] ET MALWARE Mystic Stealer C2 Session Key Response Packet
- [x] ET MALWARE Observed LegionLoader Domain in TLS SNI (legions .win)
- [x] ET MALWARE Zenlod System Information Retrieval
- [x] ET MALWARE [ANY.RUN] Meduza Stealer Exfiltration M1
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (kojgimagi .com)
- [x] ET MALWARE Observed Glupteba CnC Domain (biggames .online in TLS SNI)
- [x] ET MALWARE Observed Malicious SSL Cert (Ursnif CnC)
- [x] ET MALWARE Suspected Kimsuky Related Activity (set)
- [x] ET MALWARE Possible DarkFinger Payload Retrieval Attempt - nc10
- [x] ET MALWARE Possible DarkFinger ipconfig Retrieval Attempt
- [x] ET MALWARE Win32/RedEnergy System Information Retrieval Attempt
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (inside .awesomepotions .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (brands .shopperstreets .com)
- [ ] ET MALWARE Suspected Blackmoon Related Domain in DNS Lookup
- [x] ET MALWARE Suspected Blackmoon Related Activity (Response)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (devops .livinginthenowbook .info)
- [x] ET MALWARE DNS Query to SupremeBot Domain (silentlegion .duckdns .org)
- [x] ET MALWARE Win32/SupremeBot CnC Checkin (POST) M2
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (kyzylkumbo .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (negevbo .ru)
- [ ] ET MALWARE Gamaredon Domain in DNS Lookup (durakam .ru)
- [x] ET MALWARE [ANY.RUN] Gh0stBins Checkin
- [x] ET MALWARE [ANY.RUN] Gh0stBins Kernel Download Request
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (marathon .teachmemoney .net)

- [ ] ET MALWARE SocGholish Domain in DNS Lookup (therapy .rationallifestyleconsulting .org)
- [x] ET MALWARE Win32/SparkRAT CnC Checkin (GET)
- [x] ET MALWARE Golang Easy Stealer Exfil (POST)
- [x] ET MALWARE JokerSpy Domain in DNS Lookup (app .influmarket .org)
- [x] ET MALWARE ThirdEye Stealer CnC Checkin
- [x] ET MALWARE DDoSia Client Target Retrieval
- [x] ET MALWARE Gamaredon APT Related CnC Activity (POST) M3
- [x] ET MALWARE TA444 Domain in DNS Lookup (docsend .linkpc .net)
- [x] ET MALWARE Observed TA444 Domain in TLS SNI (jaicvc .com)
- [x] ET MALWARE JokerSpy Domain in DNS Lookup (git-hub .me)
- [x] ET MALWARE RedLine Stealer Domain in DNS Lookup (nordvpn-media .com)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (starbucls .xyz)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup
- [ ] ET MALWARE [ANY.RUN] Hydrochasma Fast Reverse Proxy M1
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (ideolot .ru)
- [x] ET MALWARE GobRAT CnC Domain in DNS Lookup (ktlvz .dnsfailover .net)
- [x] ET MALWARE GobRAT CnC Domain in DNS Lookup (su .vealcat .com)
- [x] ET MALWARE Observed GobRAT Domain (wpksi .mefound .com) in TLS SNI
- [ ] ET MALWARE TA444 Domain in DNS Lookup (cloud .dnx .capital)
- [x] ET MALWARE Win32/Ramgex.D Checkin
- [x] ET MALWARE SmugX Domain in DNS Lookup (newsmailnet .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (launch .viewthesteps .com)
- [x] ET MALWARE TA444 Domain in DNS Lookup
- [ ] ET MALWARE Playful Taurus Domain in TLS SNI (update .delldrivers .in)
- [ ] ET MALWARE Playful Taurus Domain in TLS SNI (update .adboeonline .net)
- [x] ET MALWARE Win32/zgRAT CnC Activity (GET)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (orientalebi .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (for30 .procellarumbi .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (loop71 .procellarumbi .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (to30 .procellarumbi .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (opela .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (len61 .procellarumbi .ru)
- [x] ET MALWARE Observed Gamaredon Domain (iraty .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon Domain (for71 .procellarumbi .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon Domain (procellarumbi .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon Domain (marginisbi .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon Domain (uteroma .ru in TLS SNI)
- [x] ET MALWARE SocGholish Domain in DNS Lookup (content .garretttrails .org)
- [ ] ET MALWARE Playful Taurus Domain in TLS SNI (proxy .oracleapps .org)
- [x] ET MALWARE DNS Query to UNK_BisonBooster Domain (forsports .xyz)
- [x] ET MALWARE Cinoshi Clipper Domain (tryno .ru) in TLS SNI
- [x] ET MALWARE SmugX Domain (newsmailnet .com) in TLS SNI
- [x] ET MALWARE Win32/RootTeam Stealer CnC Response
- [x] ET MALWARE [ANY.RUN] StatusRecorder Stealer Sending System Information
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (sandwiches .tropipackfood .com)
- [x] ET MALWARE Golang Easy Stealer CnC Response
- [x] ET MALWARE ThirdEye Stealer System Information Gathering Attempt
- [x] ET MALWARE DDoSia Client CnC Checkin
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (editions .seattlemysterylovers .com)
- [ ] ET MALWARE Observed Trojan.Boxter/winlnk Domain (arm .texchi .xyz in TLS SNI)
- [x] ET MALWARE TA444 Domain in DNS Lookup (jaicvc .com)
- [x] ET MALWARE Observed TA444 Domain in TLS SNI (docsend .linkpc .net)
- [x] ET MALWARE Observed JokerSpy Domain (git-hub .me in TLS SNI)
- [ ] ET MALWARE TA444 Related Domain in DNS Lookup (crypto .hondchain .com)
- [x] ET MALWARE Win32/Sinresby.B Checkin
- [ ] ET MALWARE Observed DuckTail Domain (techvibeo .com in TLS SNI)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (hanotip .ru)
- [x] ET MALWARE [ANY.RUN] Remcos RAT Checkin 861
- [x] ET MALWARE GobRAT CnC Domain in DNS Lookup (wpksi .mefound .com)
- [x] ET MALWARE Observed GobRAT Domain (ktlvz .dnsfailover .net) in TLS SNI
- [x] ET MALWARE Observed GobRAT Domain (su .vealcat .com) in TLS SNI
- [ ] ET MALWARE TA444 Domain in DNS Lookup (crypto .hondchain .com)
- [ ] ET MALWARE Cinoshi Clipper Related Domain in DNS Lookup (tryno .ru)
- [x] ET MALWARE SmugX Domain in DNS Lookup (jcswcd .com)
- [x] ET MALWARE [ANY.RUN] Hydrochasma Fast Reverse Proxy M2
- [ ] ET MALWARE Playful Taurus Domain in TLS SNI (scm .oracleapps .org)
- [ ] ET MALWARE Playful Taurus Domain in TLS SNI (vpnkerio .com)
- [ ] ET MALWARE Playful Taurus Domain in TLS SNI (mail .indiarailways .net)
- [ ] ET MALWARE Observed Turla/Crutch Domain (hotspot .accesscam .org in TLS SNI)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (iraty .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (for71 .procellarumbi .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (procellarumbi .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (marginisbi .ru)
- [x] ET MALWARE Gamaredon Domain in DNS Lookup (uteroma .ru)
- [x] ET MALWARE Observed Gamaredon Domain (orientalebi .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon Domain (for30 .procellarumbi .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon Domain (loop71 .procellarumbi .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon Domain (to30 .procellarumbi .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon Domain (opela .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon Domain (len61 .procellarumbi .ru in TLS SNI)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (creativity .kinchcorp .com)
- [x] ET MALWARE DNS Query to UNK_BisonBooster Domain (booster724 .online)
- [x] ET MALWARE DNS Query to UNK_BisonBooster Domain (speedup-pc .online)
- [x] ET MALWARE SmugX Domain (jcswcd .com) in TLS SNI
- [x] ET MALWARE Win32/RootTeam Stealer CnC Exfil M2
- [x] ET MALWARE Storm-0978 RomCom RAT CnC Checkin

- [ ] ET MALWARE RomCom CnC Domain in DNS Lookup (finformservice .com)
- [ ] ET MALWARE RomCom CnC Domain in DNS Lookup (penofach .com)
- [ ] ET MALWARE RomCom CnC Domain in DNS Lookup (altimata .org)
- [ ] ET MALWARE RomCom CnC Domain in DNS Lookup (bentaxworld .com)
- [x] ET MALWARE [ANY.RUN] Konni.APT Exfiltration
- [x] ET MALWARE [ANY.RUN] Konni.APT Keep-Alive
- [ ] ET MALWARE [ANY.RUN] DNS Query to Konni APT Domain (cachecast001 .com)
- [ ] ET MALWARE [ANY.RUN] DNS Query to Konni APT Domain (elinline .com)
- [x] ET MALWARE MalDoc/Konni APT CnC Activity (GET)
- [x] ET MALWARE Mallox Ransomware CnC Domain (whyers .io) in DNS Lookup
- [x] ET MALWARE Observed Mallox Ransomware Domain (whyers .io) in TLS SNI
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .plan .gemmadeealexander .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (skofilldrom .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (anscowerbrut .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (wiraofise .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (illboardinj .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (hloyagorepa .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (newwildtuna .top)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (appkasnofert .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (firestansinbox .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (fishofgloster .pw)
- [x] ET MALWARE Observed Glupteba CnC Domain (robloxcdneu .net in TLS SNI)
- [x] ET MALWARE Golang/Bandit Stealer Telegram Exfil Activity (POST)
- [x] ET MALWARE Kaiten User Agent
- [ ] ET MALWARE SocGholish CnC Domain in TLS SNI (* .plan .gemmadeealexander .com)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (x64 .nvize .com)
- [ ] ET MALWARE SocGholish Domain in TLS SNI (x64 .nvize .com)
- [x] ET MALWARE CHAOS RAT/AlfaC2 Client Checkin
- [x] ET MALWARE CHAOS RAT/AlfaC2 CnC Server Status Check
- [x] ET MALWARE Suspected Andariel RexPot CnC Checkin M1
- [x] ET MALWARE Suspected Andariel RexPot CnC Checkin M2
- [x] ET MALWARE Win32/Cryptbot CnC Activity (POST)
- [x] ET MALWARE Observed Glupteba CnC Domain (ggjump .ru in TLS SNI)
- [x] ET MALWARE PS1/Kimsuky CnC Exfil (POST)
- [ ] ET MALWARE DNS Query for IcedID Domain (filtaferamoza .com)
- [ ] ET MALWARE DNS Query for IcedID Domain (autokamertos .com)
- [ ] ET MALWARE DNS Query for IcedID Domain (magiketchinn .com)
- [ ] ET MALWARE DNS Query for IcedID Domain (flarkonafaero .com)
- [ ] ET MALWARE DNS Query for IcedID Domain (lohmotarufos .com)
- [ ] ET MALWARE DNS Query for IcedID Domain (magizanqomo .com)
- [x] ET MALWARE Win32/Rage Stealer CnC Exfil via Telegram (POST)
- [ ] ET MALWARE Observed IcedID Domain (flarkonafaero .com in TLS SNI)
- [ ] ET MALWARE Observed IcedID Domain (autokamertos .com in TLS SNI)
- [ ] ET MALWARE Observed IcedID Domain (lohmotarufos .com in TLS SNI)
- [ ] ET MALWARE Observed IcedID Domain (filtaferamoza .com in TLS SNI)
- [ ] ET MALWARE Observed IcedID Domain (magizanqomo .com in TLS SNI)
- [ ] ET MALWARE Observed IcedID Domain (magiketchinn .com in TLS SNI)
- [x] ET MALWARE NanoCore RAT Keepalive 1
- [x] ET MALWARE NanoCore RAT Keepalive 2
- [x] ET MALWARE NanoCore RAT Keepalive Response 1
- [x] ET MALWARE NanoCore RAT Keepalive Response 2
- [x] ET MALWARE NanoCore RAT Keepalive Response 3
- [x] ET MALWARE NanoCore RAT Keepalive 3
- [x] ET MALWARE NanoCore RAT Keepalive 4
- [x] ET MALWARE NanoCore RAT CnC 7
- [x] ET MALWARE NanoCore RAT CnC 24
- [ ] ET MALWARE NanoCore RAT CnC 26
- [x] ET MALWARE NanoCore RAT Keep-Alive Beacon (Inbound)
- [x] ET MALWARE NanoCore RAT CnC 28
- [x] ET MALWARE NanoCore RAT CnC 23
- [x] ET MALWARE NanoCore RAT Keepalive Response 4
- [ ] ET MALWARE NanoCore RAT Keepalive Response 5
- [x] ET MALWARE TraderTraitor CnC Domain in DNS Lookup (launchruse .com)
- [x] ET MALWARE TraderTraitor CnC Domain in DNS Lookup (datadog-graph .com)
- [x] ET MALWARE TraderTraitor CnC Domain in DNS Lookup (alwaysckain .com)
- [x] ET MALWARE TraderTraitor CnC Domain in DNS Lookup (centos-pkg .org)
- [x] ET MALWARE TraderTraitor CnC Domain in DNS Lookup (canolagroove .com)
- [x] ET MALWARE TraderTraitor CnC Domain in DNS Lookup (reggedrobin .com)
- [x] ET MALWARE TraderTraitor CnC Domain in DNS Lookup (nomadpkgs .com)
- [x] ET MALWARE TraderTraitor CnC Domain in DNS Lookup (primerosauxiliosperu .com)
- [x] ET MALWARE TraderTraitor CnC Domain in DNS Lookup (toyourownbeat .com)
- [x] ET MALWARE TraderTraitor CnC Domain in DNS Lookup (datadog-cloud .com)
- [x] ET MALWARE TraderTraitor CnC Domain in DNS Lookup (centos-repos .org)
- [x] ET MALWARE TraderTraitor CnC Domain in DNS Lookup (nomadpkg .com)
- [x] ET MALWARE Observed TraderTraitor Domain (launchruse .com in TLS SNI)
- [x] ET MALWARE Observed TraderTraitor Domain (datadog-graph .com in TLS SNI)
- [x] ET MALWARE Observed TraderTraitor Domain (alwaysckain .com in TLS SNI)
- [x] ET MALWARE Observed TraderTraitor Domain (centos-pkg .org in TLS SNI)
- [x] ET MALWARE Observed TraderTraitor Domain (canolagroove .com in TLS SNI)
- [x] ET MALWARE Observed TraderTraitor Domain (reggedrobin .com in TLS SNI)
- [x] ET MALWARE Observed TraderTraitor Domain (nomadpkgs .com in TLS SNI)
- [x] ET MALWARE Observed TraderTraitor Domain (primerosauxiliosperu .com in TLS SNI)
- [x] ET MALWARE Observed TraderTraitor Domain (toyourownbeat .com in TLS SNI)
- [x] ET MALWARE Observed TraderTraitor Domain (datadog-cloud .com in TLS SNI)
- [x] ET MALWARE Observed TraderTraitor Domain (centos-repos .org in TLS SNI)
- [x] ET MALWARE Observed TraderTraitor Domain (nomadpkg .com in TLS SNI)
- [ ] ET MALWARE SocGholish Domain in TLS SNI (content .garretttrails .org)
- [ ] ET MALWARE SocGholish Domain in TLS SNI (creativity .kinchcorp .com)

- [x] ET MALWARE Pupy RAT Default TLS Proxy Certificate
- [x] ET MALWARE [ANY.RUN] Hydrochasma Fast Reverse Proxy M3
- [x] ET MALWARE Observed IcedID Domain (vrondafarih .com in TLS SNI)
- [x] ET MALWARE Pupy DNS Request with SPI M1
- [x] ET MALWARE Pupy DNS Request with SPI M3
- [x] ET MALWARE Pupy DNS Request without SPI M1
- [x] ET MALWARE Pupy DNS Request without SPI M3
- [x] ET MALWARE WikiLoader Activity M1 (GET)
- [x] ET MALWARE WikiLoader Activity M2 (Response)
- [x] ET MALWARE WikiLoader Activity M2 (GET)
- [ ] ET MALWARE Win32/Trojan.Fruity Domain in DNS Lookup (atiflash .ru)
- [ ] ET MALWARE Win32/Trojan.Fruity Domain in DNS Lookup (balena-etcher .com)
- [ ] ET MALWARE Win32/Trojan.Fruity Domain in DNS Lookup (nvidiainspector .ru)
- [ ] ET MALWARE Win32/Trojan.Fruity Domain in DNS Lookup (btc-tools .ru)
- [ ] ET MALWARE Win32/Trojan.Fruity Domain in DNS Lookup (sapphiretrixx .com)
- [ ] ET MALWARE Win32/Trojan.Fruity Domain in DNS Lookup (nvflash .ru)
- [ ] ET MALWARE Win32/Trojan.Fruity Domain in DNS Lookup (techpowerup-gpu-z .com)
- [ ] ET MALWARE Win32/Trojan.Fruity Domain in DNS Lookup (atikmdagpatcher .com)
- [ ] ET MALWARE Win32/Trojan.Fruity Domain (atiflash .ru) in TLS SNI
- [ ] ET MALWARE Win32/Trojan.Fruity Domain (balena-etcher .com) in TLS SNI
- [ ] ET MALWARE Win32/Trojan.Fruity Domain (nvidiainspector .ru) in TLS SNI
- [ ] ET MALWARE Win32/Trojan.Fruity Domain (btc-tools .ru) in TLS SNI
- [ ] ET MALWARE Win32/Trojan.Fruity Domain (sapphiretrixx .com) in TLS SNI
- [ ] ET MALWARE Win32/Trojan.Fruity Domain (nvflash .ru) in TLS SNI
- [ ] ET MALWARE Win32/Trojan.Fruity Domain (techpowerup-gpu-z .com) in TLS SNI
- [ ] ET MALWARE Win32/Trojan.Fruity Domain (atikmdagpatcher .com) in TLS SNI
- [x] ET MALWARE MacOS/Realst CnC Checkin
- [x] ET MALWARE Observed IcedID Domain (mineskateroff .com in TLS SNI)
- [x] ET MALWARE abubasbanditbot CnC Checkin
- [x] ET MALWARE Observed Bahamut APT Group Domain (laborer-posted .nl) in TLS SNI
- [x] ET MALWARE Bitter APT CHM CnC Activity (GET) M4
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (pireltotus .com)
- [x] ET MALWARE Observed IcedID Domain (pireltotus .com in TLS SNI)
- [x] ET MALWARE Donot Group Related Activity (Response)
- [ ] ET MALWARE SocGholish CnC Domain in TLS SNI (* .excluded .everyadpaysmefirst .com)
- [x] ET MALWARE [ANY.RUN] PovertyStealer Check-In via TCP
- [x] ET MALWARE [ANY.RUN] Phemedrone Stealer Exfiltration via Telegram
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (humorumbi .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (bulot .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (baruta .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (mojavebo .ru)
- [x] ET MALWARE MalDoc/Gamaredon CnC Activity M4
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (vrondafarih .com)
- [x] ET MALWARE PennyWise Stealer Data Exfil M4
- [x] ET MALWARE Pupy DNS Request with SPI M2
- [x] ET MALWARE Pupy DNS Request with SPI M4
- [x] ET MALWARE Pupy DNS Request without SPI M2
- [x] ET MALWARE Pupy DNS Request without SPI M4
- [x] ET MALWARE WikiLoader Activity M1 (Response)
- [x] ET MALWARE WikiLoader Activity M3 (Response)
- [ ] ET MALWARE Win32/Trojan.Fruity Domain in DNS Lookup (polaris-bios-editor .ru)
- [ ] ET MALWARE Win32/Trojan.Fruity Domain in DNS Lookup (overdriventool .ru)
- [ ] ET MALWARE Win32/Trojan.Fruity Domain in DNS Lookup (evga-precision .com)
- [ ] ET MALWARE Win32/Trojan.Fruity Domain in DNS Lookup (ryzen-master .com)
- [ ] ET MALWARE Win32/Trojan.Fruity Domain in DNS Lookup (more-power-tool .com)
- [ ] ET MALWARE Win32/Trojan.Fruity Domain in DNS Lookup (clockgen64 .com)
- [ ] ET MALWARE Win32/Trojan.Fruity Domain in DNS Lookup (srbpolaris .ru)
- [ ] ET MALWARE Win32/Trojan.Fruity Domain in DNS Lookup (riva-tuner .com)
- [ ] ET MALWARE Win32/Trojan.Fruity Domain (polaris-bios-editor .ru) in TLS SNI
- [ ] ET MALWARE Win32/Trojan.Fruity Domain (overdriventool .ru) in TLS SNI
- [ ] ET MALWARE Win32/Trojan.Fruity Domain (evga-precision .com) in TLS SNI
- [ ] ET MALWARE Win32/Trojan.Fruity Domain (ryzen-master .com) in TLS SNI
- [ ] ET MALWARE Win32/Trojan.Fruity Domain (more-power-tool .com) in TLS SNI
- [ ] ET MALWARE Win32/Trojan.Fruity Domain (clockgen64 .com) in TLS SNI
- [ ] ET MALWARE Win32/Trojan.Fruity Domain (srbpolaris .ru) in TLS SNI
- [ ] ET MALWARE Win32/Trojan.Fruity Domain (riva-tuner .com) in TLS SNI
- [x] ET MALWARE Win32/OriginLoader CnC Checkin
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (mineskateroff .com)
- [x] ET MALWARE Possible Raspberry Robin Activity (GET) M3
- [x] ET MALWARE Bahamut APT Group CnC Domain in DNS Lookup (laborer-posted .nl)
- [x] ET MALWARE Earth Preta PUBLOAD Activity M1
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (ultrafoks .com)
- [x] ET MALWARE Observed IcedID Domain (ultrafoks .com in TLS SNI)
- [x] ET MALWARE Suspected Donot Group Related Activity (POST)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .excluded .everyadpaysmefirst .com)
- [ ] ET MALWARE IcedID CnC Domain in DNS Lookup (pireltotus .com)
- [x] ET MALWARE [ANY.RUN] PovertyStealer Exfiltration M1
- [x] ET MALWARE Redis-p2pinfect TLS Certificate Serial Number Observed in SSL Certificate
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (aethionemaso .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (alliumso .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (nicsan .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (imbriumbi .ru)

- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (acaenaso .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (alceaso .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (butoza .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (acorusso .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (achilleaso .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (anguisbi .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (cresozoq .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (wahibabo .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (tolofa .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (cupata .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (aconitumso .ru)
- [ ] ET MALWARE 8Base Ransomware Domain in DNS Lookup (sentrex219 .xyz)
- [x] ET MALWARE Win32/Agniane Stealer CnC Exfil (POST)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (achilleaso .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (wahibabo .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (adiantumso .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (acaenaso .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (butoza .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (alceaso .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (saharabo .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (mojavebo .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (aethionemaso .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (rogac .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (patrios .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (alismaso .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (baruta .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (tolofa .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (bulot .ru in TLS SNI)
- [x] ET MALWARE Reptile Rootkit Default TCP Magic Packet Trigger
- [x] ET MALWARE Reptile Rootkit Default ICMP Magic Packet Trigger
- [ ] ET MALWARE TA446 Domain in DNS Lookup (storagewarden .com)
- [ ] ET MALWARE TA446 Domain in DNS Lookup (clouddefsystems .com)
- [ ] ET MALWARE TA446 Domain in DNS Lookup (pdfdirectglobal .com)
- [ ] ET MALWARE TA446 Domain in DNS Lookup (configuregatewayglobal .com)
- [ ] ET MALWARE TA446 Domain in DNS Lookup (yourdirectinfospace .com)
- [ ] ET MALWARE TA446 Domain in DNS Lookup (gawecryptoinfosolutions .com)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (bolonna .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (acanthusso .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (patrios .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (buritoc .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (wadibo .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (saharabo .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (alismaso .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (adiantumso .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (rogac .ru)
- [x] ET MALWARE Gamaredon APT Related Domain in DNS Lookup (macda .ru)
- [ ] ET MALWARE 8Base Ransomware Domain in DNS Lookup (dexblog45 .xyz)
- [ ] ET MALWARE DNS Query for TA401 Controlled Domain (cryptoanalyzetech .com)
- [x] ET MALWARE Observed TA401 Related Domain in TLS SNI
- [x] ET MALWARE Observed Gamaredon APT Related Domain (wadibo .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (anguisbi .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (bolonna .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (cresozoq .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (acanthusso .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (macda .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (nicsan .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (alliumso .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (buritoc .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (cupata .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (acorusso .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (humorumbi .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (imbriumbi .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon APT Related Domain (aconitumso .ru in TLS SNI)
- [x] ET MALWARE [ANY.RUN] Parallax RAT Check-In
- [x] ET MALWARE Reptile Rootkit Default UDP Magic Packet Trigger
- [ ] ET MALWARE TA446 Domain in DNS Lookup (directdocumentgate .com)
- [ ] ET MALWARE TA446 Domain in DNS Lookup (commandentrance .com)
- [ ] ET MALWARE TA446 Domain in DNS Lookup (sourcedoorway .com)
- [ ] ET MALWARE TA446 Domain in DNS Lookup (controlgatestorage .com)
- [ ] ET MALWARE TA446 Domain in DNS Lookup (storageinfogate .com)
- [ ] ET MALWARE TA446 Domain in DNS Lookup (shortinfoonline .com)
- [ ] ET MALWARE TA446 Domain in DNS Lookup (sourcedoorways .com)

- ☐ ET MALWARE TA446 Domain in DNS Lookup (bittechllc .net)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (shielditlabel .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (itgatestorage .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (realeasyconfiguregateway .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (stateinfospace .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (gateinfosecure .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (secureglobaltele .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (yourspaceprotector .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (infostorageroute .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (prokeeperit .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (webgateway .ru)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (directexpressgateway .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (myittechnext .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (definform .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (oneinformationcrypto .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (solutionsseccloud .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (meshgoin .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (controlstoragesolutions .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (storagekeeperinfopro .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (directdocumentgateway .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (storagecryptoweb .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (pdfsecxcloudroute .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (serverguarditweb .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (gatecryptospace .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (infogatestorage .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (informationswitchsystems .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (threatcenterofreaserch .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (suppdatacent .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (protectordocumentcenter .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (getinfostarter .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (gatewayrecord .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (documentdirectto .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (infocryptogate .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (networkgoin .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (checkscreenit .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (datagatewayglobal .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (informationcoindata .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (realitsolutionprimary .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (centeritdefcity .com)
- ☐ ET MALWARE TA446 Domain in TLS SNI (storagewarden .com)
- ☐ ET MALWARE TA446 Domain in TLS SNI (clouddefsystems .com)
- ☐ ET MALWARE TA446 Domain in TLS SNI (pdfdirectglobal .com)
- ☐ ET MALWARE TA446 Domain in TLS SNI (configuregatewayglobal .com)
- ☐ ET MALWARE TA446 Domain in TLS SNI (yourdirectinfospace .com)
- ☐ ET MALWARE TA446 Domain in TLS SNI (gawecryptoinfosolutions .com)
- ☐ ET MALWARE TA446 Domain in TLS SNI (bittechllc .net)
- ☐ ET MALWARE TA446 Domain in TLS SNI (shielditlabel .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (entrywaycenter .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (storagecryptogate .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (managercodepro .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (intelligencerepository .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (safetydocsgateway .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (transfer-dns .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (truncstorage .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (prodefendme .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (documentdirectllc .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (itinfogate .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (datastoragecrypto .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (cloudcpanelhost .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (skycithereforeit .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (myitappnext .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (webgatewayenter .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (computingtechstudio .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (gatewayitsol .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (cryptdatagate .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (incappcloud .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (gatestoragetech .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (cryptothistech .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (controlsstoragedirect .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (gatewaydocsint .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (storagetruncservices .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (cloudrootstorage .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (computertechdirectsystems .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (po .vatangate .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (directstoragegate .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (datagatellc .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (cryptotechdirect .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (storagerootconnect .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (keepitlabgroup .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (docsinfogate .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (deskactivitygm .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (storagekeeperinfotech .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (webinterstellar .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (protectedviews .com)
- ☐ ET MALWARE TA446 Domain in DNS Lookup (gateblurbrepository .com)
- ☐ ET MALWARE TA446 Domain in TLS SNI (directdocumentgate .com)
- ☐ ET MALWARE TA446 Domain in TLS SNI (commandentrance .com)
- ☐ ET MALWARE TA446 Domain in TLS SNI (sourcedoorway .com)
- ☐ ET MALWARE TA446 Domain in TLS SNI (controlgatestorage .com)
- ☐ ET MALWARE TA446 Domain in TLS SNI (storageinfogate .com)
- ☐ ET MALWARE TA446 Domain in TLS SNI (shortinfoonline .com)
- ☐ ET MALWARE TA446 Domain in TLS SNI (sourcedoorways .com)
- ☐ ET MALWARE TA446 Domain in TLS SNI (entrywaycenter .com)
- ☐ ET MALWARE TA446 Domain in TLS SNI (storagecryptogate .com)

- [ ] ET MALWARE TA446 Domain in TLS SNI (itgatestorage .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (realeasyconfiguregateway .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (stateinfospace .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (gateinfosecure .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (secureglobaltele .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (yourspaceprotector .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (infostorageroute .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (prokeeperit .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (webgateway .ru)
- [ ] ET MALWARE TA446 Domain in TLS SNI (directexpressgateway .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (myittechnext .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (definform .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (oneinformationcrypto .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (solutionsseccloud .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (meshgoin .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (controlstoragesolutions .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (storagekeeperinfopro .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (directdocumentgateway .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (storagecryptoweb .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (pdfsecxcloudroute .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (serverguarditweb .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (gatecryptospace .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (infogatestorage .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (informationswitchsystems .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (threatcenterofreaserch .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (suppdatacent .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (protectordocumentcenter .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (getinfostarter .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (gatewayrecord .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (documentdirectto .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (infocryptogate .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (networkgoin .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (checkscreenit .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (datagatewayglobal .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (informationcoindata .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (realitsolutionprimary .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (centeritdefcity .com)
- [x] ET MALWARE Win32/Unknown Stealer CnC Exfil (POST)
- [ ] ET MALWARE MacOS/RustBucket CnC Domain in DNS Lookup (autodynamics .work .gd)
- [ ] ET MALWARE SocGholish CnC Domain in TLS SNI (* .timeline .transversallearning .com)
- [x] ET MALWARE [ANY.RUN] Win32/Stealc Checkin (POST)
- [x] ET MALWARE Win32/Amadey Payload Request (GET) M2
- [x] ET MALWARE MacOS/Adload Proxy Node Beacon
- [x] ET MALWARE Suspected Bitter Elephant APT Related Activity (GET)
- [x] ET MALWARE APT29 CnC Domain in DNS Lookup (toyy .zulipchat .com)
- [x] ET MALWARE Observed APT29 Domain (sgrhf .org .pk) in TLS SNI
- [x] ET MALWARE Observed APT29 Domain (edenparkweddings .com) in TLS SNI
- [x] ET MALWARE APT29 HTA Dropper Checkin Observed
- [x] ET MALWARE QwixxRAT - Telegram CnC Checkin
- [ ] ET MALWARE SocGholish CnC Domain in TLS SNI (* .photo .beyoudcor .com)
- [ ] ET MALWARE SocGholish CnC Domain in TLS SNI (* .workout .oystergardener .net)
- [x] ET MALWARE [ANY.RUN] Win32/RootTeam Stealer CnC Exfil M3
- [ ] ET MALWARE Python Stealer/Clipper Related Domain in DNS Lookup (kekwltd .ru)
- [ ] ET MALWARE TA446 Domain in TLS SNI (managercodepro .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (intelligencerepository .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (safetydocsgateway .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (transfer-dns .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (truncstorage .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (prodefendme .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (documentdirectllc .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (itinfogate .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (datastoragecrypto .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (cloudcpanelhost .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (skycithereforeit .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (myitappnext .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (webgatewayenter .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (computingtechstudio .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (gatewayitsol .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (cryptdatagate .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (incappcloud .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (gatestoragetech .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (cryptothistech .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (controlsstoragedirect .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (gatewaydocsint .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (storagetruncservices .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (cloudrootstorage .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (computertechdirectsystems .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (po .vatangate .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (directstoragegate .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (datagatellc .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (cryptotechdirect .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (storagerootconnect .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (keepitlabgroup .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (docsinfogate .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (deskactivitygm .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (storagekeeperinfotech .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (webinterstellar .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (protectedviews .com)
- [ ] ET MALWARE TA446 Domain in TLS SNI (gateblurbrepository .com)
- [x] ET MALWARE Win32/Agniane Stealer CnC Exfil (POST) M2
- [x] ET MALWARE MacOS/RustBucket System Information Exfiltration Attempt
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .timeline .transversallearning .com)
- [x] ET MALWARE Filez Downloader Checkin
- [x] ET MALWARE Win32/Amadey Payload Request (GET) M1
- [x] ET MALWARE MacOS/Adload CnC Beacon
- [x] ET MALWARE MacOS/Adload Proxy Node Response
- [x] ET MALWARE APT29 CnC Domain in DNS Lookup (sgrhf .org .pk)
- [x] ET MALWARE APT29 CnC Domain in DNS Lookup (edenparkweddings .com)
- [x] ET MALWARE Observed APT29 Domain (toyy .zulipchat .com) in TLS SNI
- [x] ET MALWARE APT29 Duke Variant Malware CnC Checkin Observed
- [x] ET MALWARE JanelaRAT CnC Checkin Observed
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .photo .beyoudcor .com)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .workout .oystergardener .net)
- [x] ET MALWARE [ANY.RUN] Win32/RootTeam Stealer Related User-Agent
- [x] ET MALWARE Malicious Powershell Activity (GET)
- [ ] ET MALWARE Observed Python Stealer/Clipper Related Domain (kekwltd .ru in TLS SNI)

- [x] ET MALWARE Spark RAT CnC Checkin (POST)
- [x] ET MALWARE MacOS/XLOADER Domain in DNS Lookup (www .qhsbobfv .top)
- [x] ET MALWARE MacOS/XLOADER Domain in DNS Lookup (www .hatch .computer)
- [x] ET MALWARE MacOS/XLOADER Domain in DNS Lookup (www .spv88 .online)
- [x] ET MALWARE MacOS/XLOADER Domain in DNS Lookup (www .activ-ketodietakjsy620 .cloud)
- [x] ET MALWARE MacOS/XLOADER Domain in DNS Lookup (www .qq9122 .com)
- [x] ET MALWARE MacOS/XLOADER Domain in DNS Lookup (www .growind .info)
- [x] ET MALWARE MacOS/XLOADER Domain in DNS Lookup (www .akrsnamchi .com)
- [x] ET MALWARE MacOS/XLOADER Domain in DNS Lookup (www .switchmerge .com)
- [x] ET MALWARE Win32/NewsRat CnC Exfil via Telegram (POST)
- [x] ET MALWARE Commonly Abused Domain in DNS Lookup (gk-stst .ru)
- [x] ET MALWARE Suspected TA430/Andariel CollectionRAT Related Activity (GET)
- [x] ET MALWARE Observed DNS Query to TA444 Domain
- [x] ET MALWARE Observed TA444 Domain in TLS SNI
- [x] ET MALWARE Agent Tesla Reverse Base64 Encoded MZ In Image
- [x] ET MALWARE ZenRAT Ping Command
- [x] ET MALWARE ZenRAT Get Status Command
- [x] ET MALWARE ZenRAT Change Status Command
- [x] ET MALWARE ZenRAT Request Module CnC Response
- [x] ET MALWARE ZenRAT Update CnC Response (Already Actual)
- [x] ET MALWARE ZenRAT Tasking CnC Response M1
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (manderatapple .com)
- [x] ET MALWARE Glupteba CnC Domain in DNS Lookup (dazhiruoyu .org)
- [x] ET MALWARE Win32/Steallerium Stealer Data Exfil via Telegram (POST)
- [x] ET MALWARE [ANY.RUN] TheBoxClipper CnC Activity (getkeys)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (assay .porchlightcommunity .org)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (ewacootili .com)
- [x] ET MALWARE Observed IcedID Domain (ewacootili .com in TLS SNI)
- [x] ET MALWARE TA409 Related DNS Lookup (navercorp .ru)
- [x] ET MALWARE LNK/Konni APT CnC Checkin (GET)
- [x] ET MALWARE Observed Raspberry Robin Domain (w0 .pm in TLS SNI)
- [ ] ET MALWARE SocGholish Domain in TLS SNI (standard .architech3 .com)
- [ ] ET MALWARE UAC-0173 Related Domain in DNS Lookup (minijusfil .com)
- [ ] ET MALWARE Observed UAC-0173 Related Domain (filetransrediremin .com in TLS SNI)
- [ ] ET MALWARE TA444 CnC Domain in DNS Lookup (datasend .fun)
- [ ] ET MALWARE TA444 CnC Domain in DNS Lookup (trustmeeting .online)
- [ ] ET MALWARE TA444 CnC Domain in DNS Lookup (video-meet .xyz)
- [ ] ET MALWARE TA444 CnC Domain in DNS Lookup (internal-meeting .online)
- [ ] ET MALWARE Observed TA444 Domain (ubi-safemeeting .live in TLS SNI)
- [ ] ET MALWARE Observed TA444 Domain (internal-meeting .online in TLS SNI)
- [ ] ET MALWARE Observed TA444 Domain (cryptowave .capital in TLS SNI)
- [x] ET MALWARE [ANY.RUN] Echida Botnet Check-In M1
- [x] ET MALWARE CoinMiner Domain in DNS Lookup (pool .supportxmr .com)
- [x] ET MALWARE MacOS/XLOADER Domain in DNS Lookup (www .brioche-amsterdam .com)
- [x] ET MALWARE MacOS/XLOADER Domain in DNS Lookup (www .mommachic .com)
- [x] ET MALWARE MacOS/XLOADER Domain in DNS Lookup (www .nationalrecoveryllc .com)
- [x] ET MALWARE MacOS/XLOADER Domain in DNS Lookup (www .raveready .shop)
- [x] ET MALWARE MacOS/XLOADER Domain in DNS Lookup (www .lushespets .com)
- [x] ET MALWARE MacOS/XLOADER Domain in DNS Lookup (www .corkagenexus .com)
- [x] ET MALWARE MacOS/XLOADER Domain in DNS Lookup (www .kiavisa .com)
- [x] ET MALWARE MacOS/XLOADER Domain in DNS Lookup (www .pinksugarpopmontana .com)
- [x] ET MALWARE Carderbee APT Related Activity
- [x] ET MALWARE LNK/Unknown Downloader CnC Checkin (POST)
- [x] ET MALWARE [ANY.RUN] Mekotio Banking Trojan TCP Request
- [x] ET MALWARE Observed DNS Query to TA444 Domain
- [x] ET MALWARE Observed TA444 Domain in TLS SNI
- [x] ET MALWARE Win32/CosmicRust TA444 CnC Activity (GET)
- [x] ET MALWARE Base64 Encoded MZ In Image
- [x] ET MALWARE ZenRAT CnC OK Response
- [x] ET MALWARE ZenRAT Status Response
- [x] ET MALWARE ZenRAT Request Module Command
- [x] ET MALWARE ZenRAT Update Command
- [x] ET MALWARE ZenRAT Tasking Command
- [x] ET MALWARE ZenRAT Tasking CnC Response M2
- [x] ET MALWARE Observed IcedID Domain (manderatapple .com in TLS SNI)
- [x] ET MALWARE Observed Glupteba Domain (dazhiruoyu .org in TLS SNI)
- [x] ET MALWARE [ANY.RUN] TheBoxClipper (addbild)
- [x] ET MALWARE [ANY.RUN] TheBoxClipper (updatebildchange)
- [ ] ET MALWARE SocGholish Domain in TLS SNI (assay .porchlightcommunity .org)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (oopscokir .com)
- [x] ET MALWARE Observed IcedID Domain (oopscokir .com in TLS SNI)
- [x] ET MALWARE Observed TA409 Related Domain (navercorp .ru in TLS SNI)
- [x] ET MALWARE Raspberry Robin CnC Domain in DNS Lookup (w0 .pm)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (standard .architech3 .com)
- [ ] ET MALWARE UAC-0173 Related Domain in DNS Lookup (filetransrediremin .com)
- [ ] ET MALWARE Observed UAC-0173 Related Domain (minijusfil .com in TLS SNI)
- [x] ET MALWARE Observed Malicious Powershell Loader Payload Request (GET)
- [ ] ET MALWARE TA444 CnC Domain in DNS Lookup (cryptowave .capital)
- [ ] ET MALWARE TA444 CnC Domain in DNS Lookup (ubi-safemeeting .online)
- [ ] ET MALWARE TA444 CnC Domain in DNS Lookup (ubi-safemeeting .live)
- [ ] ET MALWARE Observed TA444 Domain (trustmeeting .online in TLS SNI)
- [ ] ET MALWARE Observed TA444 Domain (video-meet .xyz in TLS SNI)
- [ ] ET MALWARE Observed TA444 Domain (ubi-safemeeting .online in TLS SNI)
- [ ] ET MALWARE Observed TA444 Domain (datasend .fun in TLS SNI)
- [x] ET MALWARE [ANY.RUN] Echida Botnet Check-In M2
- [x] ET MALWARE Observed CoinMiner Domain (pool .supportxmr .com in TLS SNI)

- [x] ET MALWARE Epsilon Stealer CnC Domain in DNS Lookup (epsilon1337 .com)
- [x] ET MALWARE Observed Epsilon Stealer Domain (epsilon1337 .com) in TLS SNI
- [x] ET MALWARE Win32/Bumblebee Loader Checkin Activity (set)
- [x] ET MALWARE Win32/Bumblebee Loader Checkin Activity
- [ ] ET MALWARE Malicious Debugging Application Related Domain in DNS Lookup (dbgsymbol .com)
- [ ] ET MALWARE Observed Malicious Debugging Application Related Domain (dbgsymbol .com in TLS SNI)
- [ ] ET MALWARE Malicious Debugging Application Related Domain in DNS Lookup (blgbeach .com)
- [ ] ET MALWARE Observed Malicious Debugging Application Related Domain (blgbeach .com in TLS SNI)
- [x] ET MALWARE Red Wolf/RedCurl Payload Retrieval Attempt M1
- [x] ET MALWARE Red Wolf/RedCurl Payload Retrieval Attempt M2
- [x] ET MALWARE Red Wolf/RedCurl Payload Retrieval Attempt M3
- [x] ET MALWARE Red Wolf/RedCurl Payload Retrieval Attempt M4
- [x] ET MALWARE Red Wolf/RedCurl Payload Retrieval Attempt M5
- [x] ET MALWARE Red Wolf/RedCurl Payload Retrieval Attempt M6
- [x] ET MALWARE Red Wolf/RedCurl Implant Checkin
- [x] ET MALWARE Red Wolf/RedCurl Domain in DNS Lookup (msftcloud .click)
- [x] ET MALWARE Red Wolf/RedCurl Domain in DNS Lookup (servicehost .click)
- [x] ET MALWARE Red Wolf/RedCurl Domain in DNS Lookup (amscloudhost .com)
- [x] ET MALWARE Red Wolf/RedCurl Domain (servicehost .click) in TLS SNI
- [x] ET MALWARE Red Wolf/RedCurl Domain (amscloudhost .com) in TLS SNI
- [x] ET MALWARE Red Wolf/RedCurl Domain (msftcloud .click) in TLS SNI
- [x] ET MALWARE Atomic macOS (AMOS) Stealer Payload Delivery Domain in DNS Lookup (trabingviews .com)
- [x] ET MALWARE Atomic macOS (AMOS) Stealer Payload Delivery Domain in DNS Lookup (xn--tradgsvews-0ubd3y .com)
- [x] ET MALWARE Atomic macOS (AMOS) Stealer Payload Delivery Domain in DNS Lookup (app-downloads .org)
- [x] ET MALWARE Observed Atomic macOS (AMOS) Stealer Payload Deliver Domain (trabingviews .com) in TLS SNI
- [x] ET MALWARE Observed Atomic macOS (AMOS) Stealer Payload Deliver Domain (xn--tradgsvews-0ubd3y .com) in TLS SNI
- [x] ET MALWARE Observed Atomic macOS (AMOS) Stealer Payload Deliver Domain (app-downloads .org) in TLS SNI
- [x] ET MALWARE SocGholish Domain in DNS Lookup (ghost .blueecho88 .com)
- [x] ET MALWARE SocGholish Domain in TLS SNI (ghost .blueecho88 .com)
- [x] ET MALWARE Red Wolf/RedCurl Domain in DNS Lookup (eap .byethost10 .com)
- [x] ET MALWARE Red Wolf/RedCurl Domain in DNS Lookup (tdnmouse .atspace .eu)
- [x] ET MALWARE Red Wolf/RedCurl Domain in DNS Lookup (buyhighroad .scienceontheweb .net)
- [x] ET MALWARE Red Wolf/RedCurl Domain in DNS Lookup (earthmart .c1 .biz)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .2023 .ebeenj .com)
- [ ] ET MALWARE SocGholish CnC Domain in TLS SNI (* .2023 .ebeenj .com)
- [ ] ET MALWARE DNS Query to TA444 Domain (updatecheck .store)
- [ ] ET MALWARE DNS Query to TA444 Domain (updatecheck .site)
- [ ] ET MALWARE DNS Query to TA444 Domain (antiviruscheck .store)
- [x] ET MALWARE DNS Query to TA444 Domain (waitingfor .cfd)
- [ ] ET MALWARE DNS Query to TA444 Domain (antifirmware .store)
- [ ] ET MALWARE DNS Query to TA444 Domain (alwayswait .site)
- [ ] ET MALWARE DNS Query to TA444 Domain (unbelievableresult .site)
- [ ] ET MALWARE DNS Query to TA444 Domain (antiviruscheck .site)
- [ ] ET MALWARE DNS Query to TA444 Domain (remoteproweb .cfd)
- [ ] ET MALWARE DNS Query to TA444 Domain (auditprovidre .store)
- [ ] ET MALWARE DNS Query to TA444 Domain (alwayswait .online)
- [x] ET MALWARE DNS Query to TA444 Domain (auditprovidre .site)
- [x] ET MALWARE DNS Query to TA444 Domain (antifirmware .site)
- [ ] ET MALWARE DNS Query to TA444 Domain (auditprovidre .online)
- [ ] ET MALWARE DNS Query to TA444 Domain (unbelievableresult .store)
- [x] ET MALWARE DNS Query to TA444 Domain (systemupdate .site)
- [ ] ET MALWARE DNS Query to TA444 Domain (newcoming .cfd)
- [ ] ET MALWARE DNS Query to TA444 Domain (systemupdate .store)
- [ ] ET MALWARE DNS Query to TA444 Domain (antifirmware .online)
- [ ] ET MALWARE Observed TA444 Domain (updatecheck .store in TLS SNI)
- [ ] ET MALWARE Observed TA444 Domain (updatecheck .site in TLS SNI)
- [ ] ET MALWARE Observed TA444 Domain (antiviruscheck .store in TLS SNI)
- [ ] ET MALWARE Observed TA444 Domain (waitingfor .cfd in TLS SNI)
- [ ] ET MALWARE Observed TA444 Domain (antifirmware .store in TLS SNI)
- [ ] ET MALWARE Observed TA444 Domain (alwayswait .site in TLS SNI)
- [ ] ET MALWARE Observed TA444 Domain (unbelievableresult .site in TLS SNI)
- [ ] ET MALWARE Observed TA444 Domain (antiviruscheck .site in TLS SNI)
- [ ] ET MALWARE Observed TA444 Domain (remoteproweb .cfd in TLS SNI)
- [ ] ET MALWARE Observed TA444 Domain (auditprovidre .store in TLS SNI)
- [ ] ET MALWARE Observed TA444 Domain (alwayswait .online in TLS SNI)
- [ ] ET MALWARE Observed TA444 Domain (auditprovidre .site in TLS SNI)
- [ ] ET MALWARE Observed TA444 Domain (antifirmware .site in TLS SNI)
- [ ] ET MALWARE Observed TA444 Domain (auditprovidre .online in TLS SNI)
- [ ] ET MALWARE Observed TA444 Domain (unbelievableresult .store in TLS SNI)
- [ ] ET MALWARE Observed TA444 Domain (systemupdate .site in TLS SNI)
- [ ] ET MALWARE Observed TA444 Domain (newcoming .cfd in TLS SNI)
- [ ] ET MALWARE Observed TA444 Domain (systemupdate .store in TLS SNI)
- [ ] ET MALWARE Observed TA444 Domain (antifirmware .online in TLS SNI)
- [x] ET MALWARE TA406 Related Domain in DNS Lookup
- [x] ET MALWARE Observed TA406 Related Domain in TLS SNI
- [x] ET MALWARE TA406 Related Activity (GET)
- [x] ET MALWARE Reptile Linux LKM Rootkit Backdoor Activity
- [x] ET MALWARE Win32/Chifrax.a CnC Exfil via TCP
- [x] ET MALWARE Free Download Manager Backdoor Domain in DNS Lookup (fdmpkg .org)
- [x] ET MALWARE Redfly APT Shadowpad Backdoor Domain in DNS Lookup (websencl .com)
- [x] ET MALWARE Darkgate Stealer CnC Checkin
- [x] ET MALWARE Invoke-Phant0m Payload Request (GET)
- [x] ET MALWARE [ANY.RUN] Win32/Lumma Stealer Check-In
- [x] ET MALWARE [ANY.RUN] Win32/Lumma Stealer Exfiltration
- [x] ET MALWARE [ANY.RUN] DarkCrystal Rat Check-in (POST)
- [x] ET MALWARE DarkGate CnC Domain in DNS Lookup (zochao .com)
- [x] ET MALWARE Observed DarkGate Domain (zochao .com in TLS SNI)
- [x] ET MALWARE DarkGate AutoIt Downloader

- [x] ET MALWARE DCRAT CnC Domain in DNS Lookup (akamaitechcdns .com)
- [ ] ET MALWARE Observed Atomic MacOS Stealer Domain (maybe .host in TLS SNI)
- [x] ET MALWARE Earth Lusca/SprySOCKS CnC Domain in DNS Lookup
- [x] ET MALWARE Transparent Tribe/CapraRAT CnC Domain in DNS Lookup
- [x] ET MALWARE Transparent Tribe/CapraRAT CnC Domain in DNS Lookup
- [ ] ET MALWARE SocGholish CnC Domain in TLS SNI (* .layout .oystergardens .us)
- [x] ET MALWARE Earth Lusca/SprySOCKS CnC Checkin
- [x] ET MALWARE Win32/Gh0stRat C2 Checkin
- [x] ET MALWARE [ANY.RUN] DarkCrystal Rat Exfiltration (POST)
- [x] ET MALWARE DNS Query to TA444 Domain (doc .apple .com .premienoe .aidl .eonw .line .pm)
- [x] ET MALWARE DNS Query to TA444 Domain (tp-globa .xyz)
- [x] ET MALWARE Observed TA444 Domain (doc .apple .com .premienoe .aidl .eonw .line .pm) in TLS SNI
- [x] ET MALWARE Observed TA444 Domain (tp-globa .xyz) in TLS SNI
- [ ] ET MALWARE SocGholish Domain in TLS SNI (cpanel .gtiyeshua .com)
- [x] ET MALWARE Sandman APT LuaDream Backdoor Domain in DNS Lookup (mode .encagil .com)
- [x] ET MALWARE Observed Sandman APT LuaDream Backdoor Domain (mode .encagil .com) in TLS SNI
- [x] ET MALWARE Stately Taurus APT Related Domain in DNS Lookup (Feed-5613 .coderformylife .info)
- [x] ET MALWARE TA577 Style Response (2023-05-15)
- [x] ET MALWARE Win32/nstealer CnC Exfiltration (POST) M2
- [x] ET MALWARE Possible OwlProxy activity M2
- [x] ET MALWARE Possible OwlProxy activity M4
- [x] ET MALWARE Possible OwlProxy activity M6
- [x] ET MALWARE TA577 Style Request (2023-05-15)
- [x] ET MALWARE TA577 Style Request (2023-05-15)
- [x] ET MALWARE TA577 Style Request (2023-05-15)
- [x] ET MALWARE TA577 Style Request (2023-05-15)
- [x] ET MALWARE TA577 Style Request (2023-05-15)
- [x] ET MALWARE Observed Ducktail Malware Related Domain in TLS SNI (ductai .xyz)
- [x] ET MALWARE [ANY.RUN] Win32/EternityClipper CnC Activity (Address Change) (POST)
- [x] ET MALWARE Possible ToneShell CnC Checkin M3
- [x] ET MALWARE Alloy Taurus Reshell Backdoor URI pattern Observed M1
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (skrgerona .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (majzolimka .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (awindakizend .com)
- [x] ET MALWARE PeepingTitle Backdoor Related Activity
- [x] ET MALWARE TA444 MacOS/ProcessRequest CnC Domain in DNS Lookup (swissborg .blog)
- [x] ET MALWARE Maldoc Sending Registration Information (GET)
- [x] ET MALWARE Lu0bot CnC Domain in DNS Lookup (apo .eus80 .fun)
- [x] ET MALWARE Lu0bot CnC Domain in DNS Lookup (mko .tinh73 .shop)
- [x] ET MALWARE [ANY.RUN] Lu0bot-Style DNS Query in DNS Lookup M2
- [x] ET MALWARE [ANY.RUN] Lu0bot-Style DNS Query in DNS Lookup M4
- [x] ET MALWARE AtlasAgent Activity (POST)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (carsfootyelo .com)
- [x] ET MALWARE Observed Glupteba Domain (ramboclub .net in TLS SNI)
- [x] ET MALWARE Win32/Agniane Stealer CnC Activity (GET) M2
- [x] ET MALWARE Akira Stealer CnC Domain in DNS Lookup (akira .red)
- [x] ET MALWARE Win32/Lumma Stealer Data Exfiltration in URI (GET)
- [x] ET MALWARE BlackDolphin Ransomware Builder Landing Page M2
- [x] ET MALWARE BlackDolphin Ransomware Builder Landing Page M4
- [ ] ET MALWARE Atomic MacOS Stealer CnC Domain in DNS Lookup (maybe .host)
- [x] ET MALWARE Atomic MacOS Stealer CnC Exfil (POST)
- [x] ET MALWARE Earth Lusca/SprySOCKS CnC Domain in DNS Lookup
- [x] ET MALWARE Transparent Tribe/CapraRAT CnC Domain in DNS Lookup
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .layout .oystergardens .us)
- [x] ET MALWARE Suspected Periscope Framework Agent Related Activity
- [x] ET MALWARE TA427 Suspected ReconShark Related Response (Inbound)
- [x] ET MALWARE Win32/Gh0stRat C2 Response (X11 SelectionNotify)
- [ ] ET MALWARE DNS Query to TA444 Domain (swissborg .blog)
- [x] ET MALWARE DNS Query to TA444 Domain (pre .alwayswait .site)
- [x] ET MALWARE Observed TA444 Domain (swissborg .blog) in TLS SNI
- [x] ET MALWARE Observed TA444 Domain (pre .alwayswait .site) in TLS SNI
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (cpanel .gtiyeshua .com)
- [x] ET MALWARE Sandman APT LuaDream Backdoor Domain in DNS Lookup (ssl .explorecell .com)
- [x] ET MALWARE Observed Sandman APT LuaDream Backdoor Domain (ssl .explorecell .com) in TLS SNI
- [x] ET MALWARE Stately Taurus APT Toneshell Backdoor Domain in DNS Lookup (www .uvfr43p .com)
- [x] ET MALWARE TA577 Style Request (2023-05-15)
- [x] ET MALWARE Win32/nstealer CnC Exfiltration (POST) M1
- [x] ET MALWARE Possible OwlProxy activity M1
- [x] ET MALWARE Possible OwlProxy activity M3
- [x] ET MALWARE Possible OwlProxy activity M5
- [ ] ET MALWARE Possible ToneShell CnC Checkin M1
- [x] ET MALWARE TA577 Style Request (2023-05-15)
- [x] ET MALWARE TA577 Style Request (2023-05-15)
- [x] ET MALWARE TA577 Style Request (2023-05-15)
- [x] ET MALWARE TA577 Style Request (2023-05-15)
- [x] ET MALWARE Ducktail Malware Related Domain in DNS Lookup (ductai .xyz)
- [x] ET MALWARE [ANY.RUN] Win32/EternityClipper CnC Activity (Successful Installation) (POST)
- [ ] ET MALWARE Possible ToneShell CnC Checkin M2
- [x] ET MALWARE Alloy Taurus APT Zapoa Backdoor Activity
- [x] ET MALWARE Alloy Taurus Reshell Backdoor URI pattern Observed M2
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (restohalto .site)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (minutozhart .online)
- [ ] ET MALWARE Observed Malicious SSL Cert (Cobalt Strike)
- [x] ET MALWARE TA444 MacOS/ProcessRequest CnC Checkin
- [x] ET MALWARE Maldoc Sending Windows System Information (POST)
- [x] ET MALWARE Lu0bot CnC Domain in DNS Lookup (hsh .juz09 .cfd)
- [x] ET MALWARE Lu0bot CnC Domain in DNS Lookup (bic .xdk03 .fun)
- [x] ET MALWARE [ANY.RUN] Lu0bot-Style DNS Query in DNS Lookup M1
- [x] ET MALWARE [ANY.RUN] Lu0bot-Style DNS Query in DNS Lookup M3
- [x] ET MALWARE [ANY.RUN] Lu0bot-Style DNS Query in DNS Lookup M5
- [x] ET MALWARE AtlasAgent Activity (GET)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (mestorycallin .com)
- [x] ET MALWARE Win32/Agniane Stealer CnC Activity (GET) M1
- [x] ET MALWARE Win32/Agniane Stealer CnC Activity (GET) M3
- [x] ET MALWARE Observed Akira Stealer Domain (akira .red) in TLS SNI
- [x] ET MALWARE Observed BlackDolphin Ransomware Builder Cookie
- [x] ET MALWARE BlackDolphin Ransomware Builder Landing Page M3
- [x] ET MALWARE BlackDolphin Ransomware Builder Landing Page M1

- [x] ET MALWARE BunnyLoader - Initial CnC Checkin
- [x] ET MALWARE BunnyLoader Initial CnC Checkin Response
- [x] ET MALWARE BunnyLoader CnC Checkin - Retrieve Tasking
- [x] ET MALWARE BunnyLoader CnC Tasking Response
- [x] ET MALWARE BunnyLoader CnC Checkin - Echoer
- [x] ET MALWARE BunnyLoader CnC Checkin - Heartbeat
- [x] ET MALWARE BunnyLoader Heartbeat Acknowledgement
- [x] ET MALWARE BunnyLoader CnC Checkin - ResultCMD
- [x] ET MALWARE BunnyLoader Data Exfiltration Attempt
- [x] ET MALWARE LNK/Sherlock Stealer Host Process List Exfil (POST)
- [x] ET MALWARE LNK/Sherlock Stealer Payload Inbound
- [x] ET MALWARE Malicious Domain in DNS Lookup (jscloud .live)
- [x] ET MALWARE Malicious Domain in DNS Lookup (cloudjs .live)
- [x] ET MALWARE Malicious Domain in DNS Lookup (jscloud .ink)
- [x] ET MALWARE Malicious Domain in DNS Lookup (jscloud .biz)
- [x] ET MALWARE Malicious Domain in DNS Lookup (jscdn .biz)
- [x] ET MALWARE [ANY.RUN] Win32/Gh0stRat Activity
- [x] ET MALWARE [ANY.RUN] Win32/Gh0stRat Keep-Alive
- [x] ET MALWARE Observed Malicious Domain (jscloud .live in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (cloudjs .live in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (jscloud .ink in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (jscloud .biz in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (jscdn .biz in TLS SNI)
- [x] ET MALWARE DNS Query to Ursnif Domain (communicalink .com)
- [x] ET MALWARE Ursnif Payload Downloader Inbound
- [x] ET MALWARE DNS Query to Ursnif Domain (mifrutty .com)
- [x] ET MALWARE Observed Ursnif Domain (mifrutty .com in TLS SNI)
- [ ] ET MALWARE Observed IcedID CnC Domain (mestorycallin .com in TLS SNI)
- [ ] ET MALWARE Observed IcedID CnC Domain (carsfootyelo .com in TLS SNI)
- [x] ET MALWARE UAC-006 Domain in DNS Lookup (ukr-net-download-files-php-name .ru)
- [x] ET MALWARE UAC-006 Domain in TLS SNI (ukr-net-download-files-php-name .ru)
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (sommelier .peppertreecanyon .com)
- [ ] ET MALWARE SocGholish Domain in TLS SNI (sommelier .peppertreecanyon .com)
- [x] ET MALWARE Darkgate Stealer CnC Checkin (POST)
- [ ] ET MALWARE Cytrox Predator Spyware Related Domain in DNS Lookup
- [ ] ET MALWARE Observed Cytrox Predator Spyware Related Domain (southchinapost .net in TLS SNI)
- [x] ET MALWARE Win32/MataDoor CnC Beacon Over UDP
- [x] ET MALWARE [ANY.RUN] DarkGate Check-In HTTP Header (POST)
- [x] ET MALWARE Win32/DarkWatchMan Checkin Activity (POST) M2
- [x] ET MALWARE Possible Win32/DarkWatchMan User Agent M2
- [x] ET MALWARE Possible Win32/DarkWatchMan User Agent M1
- [x] ET MALWARE DNS Query to Fake Chrome Landing Page (chromiumbase .site)
- [x] ET MALWARE DNS Query to Fake Chrome Landing Page (chromiumtxt .space)
- [x] ET MALWARE DNS Query to Fake Chrome Landing Page (chromiumlink .site)
- [x] ET MALWARE Observed Fake Chrome Landing Domain (chromiumbase .site in TLS SNI)
- [x] ET MALWARE Observed Fake Chrome Landing Domain (chromiumtxt .space in TLS SNI)
- [x] ET MALWARE Observed Fake Chrome Landing Domain (chromiumlink .site in TLS SNI)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (abegelkunic .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (seedkraproboy .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (maufusjiop .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (joekairbos .com)
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup (aptekoagraliy .com)
- [x] ET MALWARE Observed IcedID Domain (abegelkunic .com in TLS SNI)
- [x] ET MALWARE Observed Glupteba CnC Domain (statsexplorer .org in TLS SNI)
- [x] ET MALWARE Observed Glupteba CnC Domain (filesdumpplace .org in TLS SNI)
- [x] ET MALWARE Observed Glupteba CnC Domain (dumperstats .org in TLS SNI)
- [x] ET MALWARE Observed Glupteba CnC Domain (thestatsfiles .ru in TLS SNI)
- [x] ET MALWARE Observed Glupteba CnC Domain (realupdate .ru in TLS SNI)
- [x] ET MALWARE Observed Glupteba CnC Domain (parrotcare .net in TLS SNI)
- [x] ET MALWARE Observed Glupteba CnC Domain (mypushtimes .net in TLS SNI)
- [x] ET MALWARE Observed Glupteba CnC Domain (safarimexican .net in TLS SNI)
- [x] ET MALWARE Observed Glupteba CnC Domain (rentalhousezz .net in TLS SNI)
- [x] ET MALWARE Win32/Common RAT CnC Activity (GET)
- [x] ET MALWARE Win32/Common RAT Host Checkin (GET)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .result .garrettcountygranfondo .org)
- [ ] ET MALWARE SocGholish CnC Domain in TLS SNI (* .result .garrettcountygranfondo .org)
- [x] ET MALWARE TA401 Domain in DNS Lookup (isabeljwade .icu)
- [x] ET MALWARE TA401 Domain in DNS Lookup (francescatmorrison .icu)
- [x] ET MALWARE TA401 Domain in DNS Lookup (jayyburrows .icu)
- [x] ET MALWARE TA401 Domain in DNS Lookup (jessicakphillips .icu)
- [x] ET MALWARE TA401 Domain in TLS SNI (isabeljwade .icu)
- [x] ET MALWARE TA401 Domain in TLS SNI (francescatmorrison .icu)
- [x] ET MALWARE TA401 Domain in TLS SNI (jayyburrows .icu)
- [x] ET MALWARE TA401 Domain in TLS SNI (jessicakphillips .icu)
- [ ] ET MALWARE HAMAS affiliated Domain in DNS Lookup (alqassam .ps)
- [ ] ET MALWARE HAMAS affiliated Domain in DNS Lookup (nikanps .top)
- [ ] ET MALWARE HAMAS affiliated Domain in DNS Lookup (hamrah .nikanps .top)
- [ ] ET MALWARE HAMAS affiliated Domain in DNS Lookup (modir .nikanps .top)
- [ ] ET MALWARE HAMAS affiliated Domain in DNS Lookup (admin .nikanps .top)
- [ ] ET MALWARE HAMAS affiliated Domain in DNS Lookup (user .nikanps .top)
- [ ] ET MALWARE HAMAS affiliated Domain in DNS Lookup (nikanpsx .top)
- [ ] ET MALWARE HAMAS affiliated Domain in DNS Lookup (hz .nikanpsx .top)
- [ ] ET MALWARE HAMAS affiliated Domain in DNS Lookup (nikanpsx .hopto .org)
- [ ] ET MALWARE HAMAS affiliated Domain in TLS SNI (alqassam .ps)
- [ ] ET MALWARE HAMAS affiliated Domain in TLS SNI (nikanps .top)
- [ ] ET MALWARE HAMAS affiliated Domain in TLS SNI (hamrah .nikanps .top)
- [ ] ET MALWARE HAMAS affiliated Domain in TLS SNI (modir .nikanps .top)
- [ ] ET MALWARE HAMAS affiliated Domain in TLS SNI (admin .nikanps .top)
- [ ] ET MALWARE HAMAS affiliated Domain in TLS SNI (user .nikanps .top)
- [ ] ET MALWARE HAMAS affiliated Domain in TLS SNI (nikanpsx .top)

- [ ] ET MALWARE HAMAS affiliated Domain in TLS SNI (hz .nikanpsx .top)
- [x] ET MALWARE Fake Chrome Landing Domain Activity (chromiumbase .site)
- [x] ET MALWARE Fake Chrome Landing Domain Activity (chromiumlink .site)
- [ ] ET MALWARE Observed IcedID Loader Related Domain in TLS SNI
- [ ] ET MALWARE Observed IcedID Related Loader Domain in TLS SNI
- [ ] ET MALWARE Observed IcedID Loader Related Domain in TLS SNI
- [ ] ET MALWARE Observed IcedID Loader Related Domain in TLS SNI
- [x] ET MALWARE PovertyStealer Exfiltration M3
- [x] ET MALWARE Golang Easy Stealer Activiy M2 (POST)
- [x] ET MALWARE [ANY.RUN] PureLogs Stealer Data Exfiltration Attempt M1
- [ ] ET MALWARE [ANY.RUN] PureLogs Stealer C2 Connection M1
- [x] ET MALWARE Suspected Bumblebee Loader Activity
- [x] ET MALWARE Possible Konni RAT Domain in DNS Lookup (documentoffice .club)
- [x] ET MALWARE TA444 Domain in DNS Lookup (video-meet .team)
- [x] ET MALWARE TA444 Domain in DNS Lookup (docshared .col-link .linkpc .net)
- [x] ET MALWARE TA444 Domain in DNS Lookup (bitscrunch .pd .linkpc .net)
- [x] ET MALWARE TA444 Domain in DNS Lookup (bitscrunch .deck .linkpc .net)
- [x] ET MALWARE TA444 Domain in DNS Lookup (bitscrunch .tech .linkpc .net)
- [x] ET MALWARE TA444 Domain in DNS Lookup (doc .global-link .run .place)
- [x] ET MALWARE TA444 Domain in DNS Lookup (bitscrunch .zapto .org)
- [x] ET MALWARE TA444 Domain in DNS Lookup (www .bitscrunch .co)
- [x] ET MALWARE TA444 Domain in DNS Lookup (voldemort .myvnc .com)
- [x] ET MALWARE TA444 Domain in DNS Lookup (nor-health .xyz)
- [x] ET MALWARE TA444 Domain in TLS SNI (cisco-webex .online)
- [x] ET MALWARE TA444 Domain in TLS SNI (internal .group .link-net .publicvm .com)
- [x] ET MALWARE TA444 Domain in TLS SNI (on-global .xyz)
- [x] ET MALWARE TA444 Domain in TLS SNI (bitscrunch .ddns .net)
- [x] ET MALWARE TA444 Domain in TLS SNI (indaddy .xyz)
- [x] ET MALWARE TA444 Domain in TLS SNI (bitscrunch .presentations .life)
- [x] ET MALWARE TA444 Domain in TLS SNI (internalpdfviewer .ddns .net)
- [x] ET MALWARE TA444 Domain in TLS SNI (bitscrunch .serveirc .com)
- [x] ET MALWARE TA444 Domain in TLS SNI (bitscrunch .im .linkpc .net)
- [x] ET MALWARE TA444 Domain in TLS SNI (bitscrunchtech .linkpc .net)
- [x] ET MALWARE TA444 Domain in TLS SNI (document .shared-link .line .pm)
- [x] ET MALWARE Generic VBS Backdoor Sending Windows Information (POST)
- [x] ET MALWARE DNS Query to SockRacket/KANDYKORN Domain (bitscrunnch .linkpc .net)
- [x] ET MALWARE Observed SockRacket/KANDYKORN Domain (bitscrunnch .linkpc .net in TLS SNI)
- [x] ET MALWARE DNS Query to SockRacket/KANDYKORN Domain (datasend .linkpc .net)
- [x] ET MALWARE DNS Query to SockRacket/KANDYKORN Domain (docsendinfo .linkpc .net)
- [x] ET MALWARE DNS Query to SockRacket/KANDYKORN Domain (jobintro .linkpc .net)
- [x] ET MALWARE DNS Query to SockRacket/KANDYKORN Domain (bitscrunnch .run .place)
- [x] ET MALWARE Observed SockRacket/KANDYKORN Domain (datasend .linkpc .net in TLS SNI)
- [ ] ET MALWARE HAMAS affiliated Domain in TLS SNI (nikanpsx .hopto .org)
- [x] ET MALWARE Fake Chrome Landing Domain Activity (chromiumtxt .space)
- [ ] ET MALWARE IcedID Related Loader Domain in DNS Lookup
- [ ] ET MALWARE IcedID Loader Related Domain in DNS Lookup
- [ ] ET MALWARE IcedID Loader Related Domain in DNS Lookup
- [ ] ET MALWARE IcedID Loader Related Domain in DNS Lookup
- [x] ET MALWARE Latrodectus Loader Related Activity (POST)
- [x] ET MALWARE Golang Easy Stealer Activiy (POST)
- [x] ET MALWARE Volt Typhoon User-Agent
- [x] ET MALWARE [ANY.RUN] PureLogs Stealer C2 Connection M2
- [x] ET MALWARE Win32/NewsRat CnC Response
- [x] ET MALWARE Possible Konni RAT Related Activity Observed
- [x] ET MALWARE TA444 Domain in DNS Lookup (cisco-webex .online)
- [x] ET MALWARE TA444 Domain in DNS Lookup (internal .group .link-net .publicvm .com)
- [x] ET MALWARE TA444 Domain in DNS Lookup (on-global .xyz)
- [x] ET MALWARE TA444 Domain in DNS Lookup (bitscrunch .ddns .net)
- [x] ET MALWARE TA444 Domain in DNS Lookup (indaddy .xyz)
- [x] ET MALWARE TA444 Domain in DNS Lookup (bitscrunch .presentations .life)
- [x] ET MALWARE TA444 Domain in DNS Lookup (internalpdfviewer .ddns .net)
- [x] ET MALWARE TA444 Domain in DNS Lookup (bitscrunch .serveirc .com)
- [x] ET MALWARE TA444 Domain in DNS Lookup (bitscrunch .im .linkpc .net)
- [x] ET MALWARE TA444 Domain in DNS Lookup (bitscrunchtech .linkpc .net)
- [x] ET MALWARE TA444 Domain in DNS Lookup (document .shared-link .line .pm)
- [x] ET MALWARE TA444 Domain in TLS SNI (video-meet .team)
- [x] ET MALWARE TA444 Domain in TLS SNI (docshared .col-link .linkpc .net)
- [x] ET MALWARE TA444 Domain in TLS SNI (bitscrunch .pd .linkpc .net)
- [x] ET MALWARE TA444 Domain in TLS SNI (bitscrunch .deck .linkpc .net)
- [x] ET MALWARE TA444 Domain in TLS SNI (bitscrunch .tech .linkpc .net)
- [x] ET MALWARE TA444 Domain in TLS SNI (doc .global-link .run .place)
- [x] ET MALWARE TA444 Domain in TLS SNI (bitscrunch .zapto .org)
- [x] ET MALWARE TA444 Domain in TLS SNI (www .bitscrunch .co)
- [x] ET MALWARE TA444 Domain in TLS SNI (voldemort .myvnc .com)
- [x] ET MALWARE TA444 Domain in TLS SNI (nor-health .xyz)
- [x] ET MALWARE Suspected TA404 SIGNBT Backdoor Activity (POST)
- [x] ET MALWARE DNS Query to SockRacket/KANDYKORN Domain (tp-globa .xyz)
- [x] ET MALWARE Observed SockRacket/KANDYKORN Domain (tp-globa .xyz in TLS SNI)
- [x] ET MALWARE Malicious SockRacket/KANDYKORN SSL Certificate Detected
- [x] ET MALWARE DNS Query to SockRacket/KANDYKORN Domain (coupang-networks .pics)
- [x] ET MALWARE DNS Query to SockRacket/KANDYKORN Domain (exodus .linkpc .net)
- [x] ET MALWARE DNS Query to SockRacket/KANDYKORN Domain (docsenddata .linkpc .net)
- [x] ET MALWARE DNS Query to SockRacket/KANDYKORN Domain (jobdescription .linkpc .net)
- [x] ET MALWARE Observed SockRacket/KANDYKORN Domain (coupang-networks .pics in TLS SNI)

- [x] ET MALWARE Observed SockRacket/KANDYKORN Domain (docsendinfo .linkpc .net in TLS SNI)
- [x] ET MALWARE Observed SockRacket/KANDYKORN Domain (exodus .linkpc .net in TLS SNI)
- [x] ET MALWARE Observed SockRacket/KANDYKORN Domain (jobintro .linkpc .net in TLS SNI)
- [x] ET MALWARE Observed SockRacket/KANDYKORN Domain (docsenddata .linkpc .net in TLS SNI)
- [x] ET MALWARE Observed SockRacket/KANDYKORN Domain (bitscrunnch .run .place in TLS SNI)
- [x] ET MALWARE Observed SockRacket/KANDYKORN Domain (jobdescription .linkpc .net in TLS SNI)
- [x] ET MALWARE SockRacket/KANDYKORN Client Connect (Random Number)
- [x] ET MALWARE SockRacket/KANDYKORN CnC Response (Nonce)
- [x] ET MALWARE SockRacket/KANDYKORN Client Challenge
- [x] ET MALWARE SockRacket/KANDYKORN CnC Response
- [x] ET MALWARE Malicious Base64 Encoded Payload In Image
- [x] ET MALWARE GCleaner Downloader IP Address Retrieval Attempt M2
- [x] ET MALWARE GCleaner Downloader Activity M11
- [x] ET MALWARE Win32/Unknown CnC Domain in DNS Lookup (hackermania .org)
- [x] ET MALWARE Win32/Unknown Domain (hackermania .org) in TLS SNI
- [x] ET MALWARE Suspected APT34 Related SSD Backdoor Activity (POST)
- [x] ET MALWARE Suspected APT34 Related SSD Backdoor Response
- [x] ET MALWARE RisePro TCP Heartbeat Packet
- [x] ET MALWARE Suspected Higaisa APT Related Domain in DNS Lookup (insightinteriors .im)
- [ ] ET MALWARE DNS Query to IcedID Domain (asleytomafa .com)
- [x] ET MALWARE DNS Query to IcedID Domain (manjuskploman .com)
- [x] ET MALWARE DNS Query to IcedID Domain (brojizuza .com)
- [ ] ET MALWARE DNS Query to IcedID Domain (grafielucho .com)
- [x] ET MALWARE DNS Query to IcedID Domain (qousahaff .com)
- [x] ET MALWARE Observed IcedID Domain (asleytomafa .com in TLS SNI)
- [x] ET MALWARE Observed IcedID Domain (manjuskploman .com in TLS SNI)
- [x] ET MALWARE Observed IcedID Domain (brojizuza .com in TLS SNI)
- [x] ET MALWARE Observed IcedID Domain (grafielucho .com in TLS SNI)
- [x] ET MALWARE Observed IcedID Domain (qousahaff .com in TLS SNI)
- [x] ET MALWARE NodeStealer CnC Activity from Downloaded Archive (GET)
- [x] ET MALWARE JS/Z1_Loader Activity (POST)
- [x] ET MALWARE Win32/Stealc/Vidar Stealer Style Headers In HTTP POST
- [ ] ET MALWARE Bitter APT Related Domain in DNS Lookup
- [ ] ET MALWARE Observed Bitter APT Related Domain in TLS SNI
- [x] ET MALWARE Lazarus CnC Domain in DNS Lookup (online-meeting .team)
- [x] ET MALWARE Lazarus CnC Domain in DNS Lookup (team-meet .online)
- [x] ET MALWARE Lazarus CnC Domain in DNS Lookup (safemeeting .online)
- [x] ET MALWARE Lazarus CnC Domain in DNS Lookup (videomeethub .online)
- [x] ET MALWARE Observed Lazarus Domain (team-meet .online in TLS SNI)
- [x] ET MALWARE Observed Lazarus Domain (videomeethub .online in TLS SNI)
- [ ] ET MALWARE Observed Lazarus Domain (online-meeting .team in TLS SNI)
- [ ] ET MALWARE Observed Lazarus Domain (safemeeting .online in TLS SNI)
- [x] ET MALWARE Socks5Systemz CnC Checkin M2
- [x] ET MALWARE Socks5SystemZ CnC Checkin Response M1
- [x] ET MALWARE Socks5SystemZ CnC Checkin Response M2
- [x] ET MALWARE Bandit Stealer Config Inbound
- [x] ET MALWARE Bandit Stealer Host Details Exfil
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .caching .oysterfloats .com)
- [ ] ET MALWARE SocGholish CnC Domain in TLS SNI (* .caching .oysterfloats .com)
- [x] ET MALWARE MACE C2 Framework Activity (GET)
- [x] ET MALWARE MACE C2 Framework Response M1
- [x] ET MALWARE MACE C2 Framework Response M2
- [x] ET MALWARE Win32/Fewin Stealer Data Exfiltration Attempt
- [ ] ET MALWARE SocGholish Domain in DNS Lookup (modification .grebcocontractors .com)
- [x] ET MALWARE SocGholish Domain in DNS Lookup (sermon .pastorbriantubbs .com)
- [ ] ET MALWARE SocGholish Domain in TLS SNI (modification .grebcocontractors .com)
- [x] ET MALWARE SocGholish Domain in TLS SNI (sermon .pastorbriantubbs .com)
- [x] ET MALWARE Win32/Unknown RAT CnC Server Acknowledgement
- [x] ET MALWARE Win32/Unknown RAT CnC Checkin
- [x] ET MALWARE Win32/TA402 CnC User-Agent
- [x] ET MALWARE Win32/TA402 CnC Response M1
- [x] ET MALWARE Win32/TA402 CnC Response M2
- [x] ET MALWARE Win32/TA402 Checkin
- [x] ET MALWARE Win32/TA402 Checkin M2
- [x] ET MALWARE TA402 CnC Domain in DNS Lookup
- [x] ET MALWARE Observed TA402 Domain in TLS SNI
- [x] ET MALWARE TA402 CnC Domain in DNS Lookup
- [x] ET MALWARE Observed TA402 Domain in TLS SNI
- [x] ET MALWARE Win32/TA402 CnC Activity (POST)
- [x] ET MALWARE Win32/TA402 CnC Activity (GET)
- [ ] ET MALWARE DNS Query to Remcos Domain (retghrtgwtrgtg .bounceme .net)
- [ ] ET MALWARE DNS Query to Remcos Domain (listpoints .online)
- [ ] ET MALWARE DNS Query to Remcos Domain (listpoints .click)
- [ ] ET MALWARE Observed Remcos Domain (retghrtgwtrgtg .bounceme .net in TLS SNI)
- [ ] ET MALWARE Observed Remcos Domain (listpoints .online in TLS SNI)
- [ ] ET MALWARE Observed Remcos Domain (listpoints .click in TLS SNI)
- [x] ET MALWARE Arkei/Vidar/Mars Stealer Variant DLL GET Request M2
- [x] ET MALWARE QuickBooks Pop-Up Scam - Request for QB Download Locations
- [x] ET MALWARE QuickBooks Pop-Up Scam - Download Locations Response
- [x] ET MALWARE QuickBooks Pop-Up Scam - Checkin Response
- [x] ET MALWARE QuickBooks Pop-Up Scam - Pop-Up Details Request
- [x] ET MALWARE QuickBooks Pop-Up Scam - Pop-Up Details Response
- [x] ET MALWARE QuickBooks Pop-Up Scam - Checkin
- [x] ET MALWARE Latrodectus Alive Request (GET)
- [x] ET MALWARE Latrodectus Alive Response M1
- [x] ET MALWARE Latrodectus 404 Response
- [x] ET MALWARE DNS Query to Scattered Spider Domain (victimname-sso .com
- [x] ET MALWARE DNS Query to Scattered Spider Domain (victimname-servicedesk .com

- [x] ET MALWARE DNS Query to Scattered Spider Domain (victimname-okta .com
- [x] ET MALWARE Observed Scattered Spider Domain (victimname-servicedesk .com in TLS SNI)
- [x] ET MALWARE DNS Query to Malicious Domain (drive-google-com .tk)
- [x] ET MALWARE [ANY.RUN] Stealc/Vidar Stealer TLS Certificate
- [x] ET MALWARE Turla APT/Kazuar Backdoor CnC Activity (POST)
- [ ] ET MALWARE SocGholish CnC Domain in TLS SNI (* .novelty .akibacreative .com)
- [x] ET MALWARE WikiLoader Activity M4 (Response)
- [x] ET MALWARE TA444 Related JS Activity Sending Windows System Process Information (POST)
- [x] ET MALWARE DNS Query to Malicious Domain (mydatayxnhzcs .tech)
- [x] ET MALWARE LNK/imageres CnC Payload Request (GET)
- [x] ET MALWARE TA422 Related Activity M4
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .sync .oystergardens .club)
- [x] ET MALWARE DNS Query to SysJoker Domain (sharing-u-file .com)
- [x] ET MALWARE DNS Query to SysJoker Domain (audiosound-visual .com)
- [x] ET MALWARE SysJoker Successful Command Execution (POST)
- [x] ET MALWARE SysJoker Bot Registration (POST)
- [x] ET MALWARE SysJoker User-Agent Observed
- [x] ET MALWARE TA406 Win32/Updog Backdoor Data Exfiltration Attempt
- [x] ET MALWARE WebDAV Retrieving .exe from .url M1 (CVE-2023-36025)
- [x] ET MALWARE WebDAV Retrieving .zip from .url M2 (CVE-2023-36025)
- [x] ET MALWARE Andariel Group Nukesped Variant CnC Checkin
- [x] ET MALWARE [ANY.RUN] Socks5Systemz TCP Backconnect Client Traffic
- [x] ET MALWARE WebDAV Retrieving .vbs from .url M2 (CVE-2023-36025)
- [x] ET MALWARE JynxLoaderV2 CnC Checkin
- [x] ET MALWARE SugarGh0st RAT Domain in DNS Lookup (login .drive-google-com .tk)
- [x] ET MALWARE SocGholish Domain in DNS Lookup (dashboard .renovationsruth .com)
- [x] ET MALWARE Suspected ToddyCat APT Curlu Related Activity M1
- [ ] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (tirechinecarpett .pw)
- [ ] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (musclefarelongea .pw)
- [ ] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (freckletropsao .pw)
- [ ] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (medicinebuckerrysa .pw)
- [ ] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (definefolkeloi .pw)
- [x] ET MALWARE DNS Query to Malicious Domain (2311forget .online)
- [x] ET MALWARE Observed Malicious Domain in TLS SNI (2311forget .online)
- [x] ET MALWARE Darkgate Stealer CnC Checkin (POST) M2
- [x] ET MALWARE DNS Query to Darkgate Domain (trans1ategooglecom .com)
- [x] ET MALWARE Observed Darkgate Domain (trans1ategooglecom .com in TLS SNI)
- [x] ET MALWARE Suspected TA453 Related Domain in DNS Lookup (metahelpservice .net)
- [x] ET MALWARE Suspected TA453 Related Domain in DNS Lookup (metaemailsecurity .net)
- [x] ET MALWARE Suspected TA453 Related Domain in DNS Lookup (metasecurityemail .org)
- [x] ET MALWARE Suspected TA453 Related Domain in DNS Lookup (metasupportmail .com)
- [x] ET MALWARE Observed Suspected TA453 Related Domain (metahelpservice .net in TLS SNI)
- [x] ET MALWARE Observed Scattered Spider Domain (victimname-sso .com in TLS SNI)
- [x] ET MALWARE Observed Scattered Spider Domain (victimname-okta .com in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (drive-google-com .tk in TLS SNI)
- [x] ET MALWARE Suspected Malicious JS Loader Activity (GET)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .novelty .akibacreative .com)
- [x] ET MALWARE WikiLoader Activity M3 (GET)
- [x] ET MALWARE TA404 Comebacker Related Activity (POST)
- [x] ET MALWARE MetaStealer Activity (Response)
- [x] ET MALWARE DNS Query to Malicious Domain (flyfggfdbvcbvcbc .online)
- [x] ET MALWARE TA422 Related Activity M3
- [x] ET MALWARE TA422 Related Activity M5
- [ ] ET MALWARE SocGholish CnC Domain in TLS SNI (* .sync .oystergardens .club)
- [x] ET MALWARE DNS Query to SysJoker Domain (filestorage-short .org)
- [x] ET MALWARE SysJoker Host Details Exfil (POST)
- [x] ET MALWARE SysJoker Bot Configuration Request (POST)
- [x] ET MALWARE SysJoker User-Agent Observed
- [x] ET MALWARE SysJoker CnC Checkin (POST)
- [x] ET MALWARE TA406 Win32/Updog CnC Checkin
- [x] ET MALWARE WebDAV Retrieving .zip from .url M1 (CVE-2023-36025)
- [x] ET MALWARE WebDAV Retrieving .exe from .url M2 (CVE-2023-36025)
- [x] ET MALWARE Marai Variant Activity (Inbound)
- [x] ET MALWARE WebDAV Retrieving .vbs from .url M1 (CVE-2023-36025)
- [x] ET MALWARE ToddyCat APT Related CurCore Activity (POST)
- [x] ET MALWARE SugarGh0st RAT CnC Checkin
- [x] ET MALWARE SugarGh0st RAT Domain in DNS Lookup (account .drive-google-com .tk)
- [x] ET MALWARE SocGholish Domain in TLS SNI (dashboard .renovationsruth .com)
- [x] ET MALWARE Suspected ToddyCat APT Curlu Related Activity M2
- [ ] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (hemispheredonkkl .pw)
- [ ] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (ownerbuffersuperw .pw)
- [ ] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (fanlumpactiras .pw)
- [ ] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (helpfulsteepyi .pw)
- [x] ET MALWARE PS1/Unknown Payload C2 Downloader (GET)
- [x] ET MALWARE DNS Query to Malicious Domain (hijackson .org)
- [x] ET MALWARE Observed Malicious Domain in TLS SNI (hijackson .org)
- [x] ET MALWARE DNS Query to Darkgate Domain (saintelzearlava .com)
- [x] ET MALWARE Observed Darkgate Domain (saintelzearlava .com in TLS SNI)
- [x] ET MALWARE Win32/Unknown Grabber Base64 Data Exfiltration Attempt
- [x] ET MALWARE Suspected TA453 Related Domain in DNS Lookup (xn--metaspport-v43e .com)
- [x] ET MALWARE Suspected TA453 Related Domain in DNS Lookup (metasupportmail .co)
- [x] ET MALWARE Suspected TA453 Related Domain in DNS Lookup (metaemailsecurity .com)
- [x] ET MALWARE Suspected TA453 Related Domain in DNS Lookup (igsecurity .email)
- [x] ET MALWARE Observed Suspected TA453 Related Domain (xn--metaspport-v43e .com in TLS SNI)

- [x] ET MALWARE Observed Suspected TA453 Related Domain (metaemailsecurity .net in TLS SNI)
- [x] ET MALWARE Observed Suspected TA453 Related Domain (metasecurityemail .org in TLS SNI)
- [x] ET MALWARE Observed Suspected TA453 Related Domain (metasupportmail .com in TLS SNI)
- [x] ET MALWARE Suspected TA453 Related Domain in DNS Lookup (metasupport .com)
- [x] ET MALWARE [ANY.RUN] Socks5Systemz HTTP C2 Connection M1
- [x] ET MALWARE SocGholish Domain in DNS Lookup (pluralism .themancav .com)
- [x] ET MALWARE DNS Query to Teal Kurma Domain (anfturkce .news)
- [x] ET MALWARE DNS Query to Teal Kurma Domain (nmcbcd .live)
- [x] ET MALWARE DNS Query to Teal Kurma Domain (querryfiles .com)
- [x] ET MALWARE DNS Query to Teal Kurma Domain (ud .ybcd .tech)
- [x] ET MALWARE DNS Query to Teal Kurma Domain (alhurra .online)
- [x] ET MALWARE DNS Query to Teal Kurma Domain (lo0 .systemctl .network)
- [x] ET MALWARE DNS Query to Teal Kurma Domain (dhcp .systemctl .network)
- [x] ET MALWARE Observed Teal Kurma Domain (al-marsad .co in TLS SNI)
- [x] ET MALWARE Observed Teal Kurma Domain (alhurra .online in TLS SNI)
- [x] ET MALWARE Observed Teal Kurma Domain (ybcd .tech in TLS SNI)
- [x] ET MALWARE Observed Teal Kurma Domain (lo0 .systemctl .network in TLS SNI)
- [x] ET MALWARE Observed Teal Kurma Domain (aws .systemctl .network in TLS SNI)
- [x] ET MALWARE Observed Teal Kurma Domain (nmcbcd .live in TLS SNI)
- [x] ET MALWARE SnappyTCP Reverse Shell Header Value Observed
- [x] ET MALWARE SnappyTCP Reverse Shell Client Checkin M2
- [ ] ET MALWARE SocGholish CnC Domain in TLS SNI (* .cloudid .coffeeonboard .com)
- [x] ET MALWARE Win32/Asmodeasmo Bot CnC Checkin
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .settings .oysterfloats .org)
- [x] ET MALWARE Void Rabisu Related Loader Activity (GET)
- [x] ET MALWARE Observed TA430/Andariel APT Related Domain (tech .micrsofts .com in TLS SNI)
- [x] ET MALWARE Observed TA430/Andariel APT Related Domain (tech .micrsofts .tech in TLS SNI)
- [x] ET MALWARE JynxLoaderV2 CnC Server Command (NOTASK)
- [x] ET MALWARE Encoded JinxV2DEV User-Agent Observed (4a696e785632444556)
- [x] ET MALWARE RisePro CnC Activity (Inbound)
- [x] ET MALWARE TA430/Andariel APT HazyLoad Proxy Related Activity (POST)
- [x] ET MALWARE DNS Query to Axile Stealer Domain (axile .su)
- [x] ET MALWARE Axile Stealer CnC Activity (POST)
- [x] ET MALWARE Lazarus APT Related Loader Activity (GET)
- [x] ET MALWARE Win32/Spyder CnC Checkin
- [x] ET MALWARE Latrodectus Alive Response M2
- [x] ET MALWARE Latrodectus Alive Response M4
- [x] ET MALWARE Latrodectus Alive Response M6
- [x] ET MALWARE Latrodectus Alive Response M8
- [x] ET MALWARE Observed Malicious SSL Cert (TA577)
- [x] ET MALWARE Observed Malicious SSL Cert (TA577)
- [x] ET MALWARE Observed Malicious SSL Cert (TA577)
- [x] ET MALWARE Win32/GoPix Stealer Activity (POST)
- [x] ET MALWARE Win32/Blacklegion Ransomware CnC Checkin
- [x] ET MALWARE Observed Suspected TA453 Related Domain (metasupportmail .co in TLS SNI)
- [x] ET MALWARE Observed Suspected TA453 Related Domain (metaemailsecurity .com in TLS SNI)
- [x] ET MALWARE Observed Suspected TA453 Related Domain (igsecurity .email in TLS SNI)
- [x] ET MALWARE Observed Suspected TA453 Related Domain (metasupport .com in TLS SNI)
- [x] ET MALWARE [ANY.RUN] Socks5Systemz HTTP C2 Connection M2
- [x] ET MALWARE SocGholish Domain in TLS SNI (pluralism .themancav .com)
- [x] ET MALWARE DNS Query to Teal Kurma Domain (al-marsad .co)
- [x] ET MALWARE DNS Query to Teal Kurma Domain (aws .systemctl .network)
- [x] ET MALWARE DNS Query to Teal Kurma Domain (ybcd .tech)
- [x] ET MALWARE DNS Query to Teal Kurma Domain (systemctl .network)
- [x] ET MALWARE DNS Query to Teal Kurma Domain (upt .mcsoft .org)
- [x] ET MALWARE DNS Query to Teal Kurma Domain (eth0 .secrsys .net)
- [x] ET MALWARE Observed Teal Kurma Domain (anfturkce .news in TLS SNI)
- [x] ET MALWARE Observed Teal Kurma Domain (ud .ybcd .tech in TLS SNI)
- [x] ET MALWARE Observed Teal Kurma Domain (systemctl .network in TLS SNI)
- [x] ET MALWARE Observed Teal Kurma Domain (querryfiles .com in TLS SNI)
- [x] ET MALWARE Observed Teal Kurma Domain (upt .mcsoft .org in TLS SNI)
- [x] ET MALWARE Observed Teal Kurma Domain (dhcp .systemctl .network in TLS SNI)
- [x] ET MALWARE Observed Teal Kurma Domain (eth0 .secrsys .net in TLS SNI)
- [x] ET MALWARE SnappyTCP Reverse Shell Client Checkin M1
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .cloudid .coffeeonboard .com)
- [x] ET MALWARE Observed Malicious SSL Cert (Silver Keylogger)
- [x] ET MALWARE Observed Malicious SSL Cert (Brushaloader CnC) 2023-12-4
- [ ] ET MALWARE SocGholish CnC Domain in TLS SNI (* .settings .oysterfloats .org)
- [x] ET MALWARE TA430/Andariel APT Related CnC Domain in DNS Lookup (tech .micrsofts .com)
- [x] ET MALWARE TA430/Andariel APT Related CnC Domain in DNS Lookup (tech .micrsofts .tech)
- [x] ET MALWARE TA430/Andariel APT Related DLRAT Activity (POST)
- [x] ET MALWARE JynxLoaderV2 CnC Command (INSTALL)
- [x] ET MALWARE RisePro CnC Activity (Outbound)
- [x] ET MALWARE TA430/Andariel APT BottomLoader Activity (GET)
- [x] ET MALWARE Suspected Kimsuky APT RevClient Related Activity
- [x] ET MALWARE Observed Axile Stealer Domain (axile .su in TLS SNI)
- [x] ET MALWARE Suspected Lazarus APT Validator Related Activity (POST)
- [x] ET MALWARE Win32/Spyder Sending Info to CnC
- [x] ET MALWARE Win32/Spyder Successful CnC Checkin
- [x] ET MALWARE Latrodectus Alive Response M3
- [x] ET MALWARE Latrodectus Alive Response M5
- [x] ET MALWARE Latrodectus Alive Response M7
- [x] ET MALWARE IcedID CnC Domain in DNS Lookup
- [x] ET MALWARE Observed Malicious SSL Cert (TA577)
- [x] ET MALWARE Observed Malicious SSL Cert (TA577)
- [x] ET MALWARE Observed Malicious SSL Cert (TA577)
- [x] ET MALWARE Qbot Related Activity (POST)
- [x] ET MALWARE Win32/Blacklegion Ransomware CnC Response

- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .scheme .corycabana .net)
- [x] ET MALWARE CloudAtlas APT Related DNS Lookup (avito-service .net)
- [x] ET MALWARE CloudAtlas APT Related Maldoc Activity M1 (GET)
- [x] ET MALWARE Observed CloudAtlas APT Related Domain (network-list .com in TLS SNI)
- [x] ET MALWARE CloudAtlas APT Related Maldoc Activity M4 (GET)
- [x] ET MALWARE CloudAtlas APT Related Maldoc Activity M6 (GET)
- [x] ET MALWARE DNS Query to Suspected APT Domain (idf .pics)
- [x] ET MALWARE Observed Suspected APT Domain (idfleaks .info in TLS SNI)
- [x] ET MALWARE Observed Suspected APT Domain (idfinfo .pw in TLS SNI)
- [ ] ET MALWARE DNS Query to UAC-0177 Domain (ssl4 .site)
- [ ] ET MALWARE DNS Query to UAC-0177 Domain (personlog .in)
- [ ] ET MALWARE DNS Query to UAC-0177 Domain (authssl .online)
- [ ] ET MALWARE DNS Query to UAC-0177 Domain (hsts .online)
- [ ] ET MALWARE DNS Query to UAC-0177 Domain (ssl2 .online)
- [ ] ET MALWARE DNS Query to UAC-0177 Domain (goaccount .link)
- [ ] ET MALWARE DNS Query to UAC-0177 Domain (ssl1 .online)
- [ ] ET MALWARE DNS Query to UAC-0177 Domain (certifiedauth .in)
- [ ] ET MALWARE DNS Query to UAC-0177 Domain (connectssl .in)
- [ ] ET MALWARE DNS Query to UAC-0177 Domain (ssl3 .site)
- [ ] ET MALWARE DNS Query to UAC-0177 Domain (exmo .day)
- [ ] ET MALWARE DNS Query to UAC-0177 Domain (ssl4 .online)
- [ ] ET MALWARE Observed UAC-0177 Domain (ssl2 .in in TLS SNI)
- [ ] ET MALWARE Observed UAC-0177 Domain (getssl .ink in TLS SNI)
- [ ] ET MALWARE Observed UAC-0177 Domain (ssl2 .link in TLS SNI)
- [ ] ET MALWARE Observed UAC-0177 Domain (ssl1 .site in TLS SNI)
- [ ] ET MALWARE Observed UAC-0177 Domain (authssl .in in TLS SNI)
- [ ] ET MALWARE Observed UAC-0177 Domain (authssl .site in TLS SNI)
- [ ] ET MALWARE Observed UAC-0177 Domain (ssl2 .site in TLS SNI)
- [ ] ET MALWARE Observed UAC-0177 Domain (passport2 .zip in TLS SNI)
- [ ] ET MALWARE Observed UAC-0177 Domain (authssl .link in TLS SNI)
- [ ] ET MALWARE Observed UAC-0177 Domain (getssl .click in TLS SNI)
- [ ] ET MALWARE Observed UAC-0177 Domain (ssl3 .online in TLS SNI)
- [ ] ET MALWARE Observed UAC-0177 Domain (authcheck .in in TLS SNI)
- [ ] ET MALWARE Observed UAC-0177 Domain (authssl .org in TLS SNI)
- [x] ET MALWARE Possible KV Botnet CnC Checkin
- [x] ET MALWARE CloudAtlas APT Related Maldoc Activity M7 (GET)
- [x] ET MALWARE Malicious Loader Related Activity Response
- [x] ET MALWARE Win32/BlackRain CnC Activity
- [x] ET MALWARE Brute Ratel Framework Related Domain in DNS Lookup (azureclouder .com)
- [x] ET MALWARE YoroTrooper APT Related Activty (GET)
- [x] ET MALWARE Win32/Koi Loader CnC Checkin M1
- [x] ET MALWARE Win32/Koi Loader CnC Checkin M3
- [x] ET MALWARE Win32/Unknown Stealer Data Exfiltration Attempt
- [x] ET MALWARE Suspicious Domain (webvideoshareonline .com) in TLS SNI
- [x] ET MALWARE Observed Win32/Koi Loader/Stealer Domain (podologie-werne .de) in TLS SNI
- [x] ET MALWARE Suspected PrivateLoader Activity (POST)
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (agedelayglacierwe .pw)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (chincenterblandwka .pw in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (neighborhoodfeelsa .fun in TLS SNI)
- [ ] ET MALWARE SocGholish CnC Domain in TLS SNI (* .places .creeksidehuntingpreserve .com)
- [ ] ET MALWARE SocGholish CnC Domain in TLS SNI (* .scheme .corycabana .net)
- [x] ET MALWARE Observed CloudAtlas APT Related Domain (avito-service .net in TLS SNI)
- [x] ET MALWARE CloudAtlas APT Related Domain in DNS Lookup (network-list .com)
- [x] ET MALWARE CloudAtlas APT Related Maldoc Activity M3 (GET)
- [x] ET MALWARE CloudAtlas APT Related Maldoc Activity M5 (GET)
- [x] ET MALWARE DNS Query to Suspected APT Domain (idfleaks .info)
- [x] ET MALWARE DNS Query to Suspected APT Domain (idfinfo .pw)
- [x] ET MALWARE Observed Suspected APT Domain (idf .pics in TLS SNI)
- [ ] ET MALWARE DNS Query to UAC-0177 Domain (ssl2 .in)
- [ ] ET MALWARE DNS Query to UAC-0177 Domain (getssl .ink)
- [ ] ET MALWARE DNS Query to UAC-0177 Domain (ssl2 .link)
- [ ] ET MALWARE DNS Query to UAC-0177 Domain (ssl1 .site)
- [ ] ET MALWARE DNS Query to UAC-0177 Domain (authssl .in)
- [x] ET MALWARE DNS Query to UAC-0177 Domain (authssl .site)
- [ ] ET MALWARE DNS Query to UAC-0177 Domain (ssl2 .site)
- [x] ET MALWARE DNS Query to UAC-0177 Domain (passport2 .zip)
- [ ] ET MALWARE DNS Query to UAC-0177 Domain (authssl .link)
- [ ] ET MALWARE DNS Query to UAC-0177 Domain (getssl .click)
- [ ] ET MALWARE DNS Query to UAC-0177 Domain (ssl3 .online)
- [ ] ET MALWARE DNS Query to UAC-0177 Domain (authcheck .in)
- [ ] ET MALWARE DNS Query to UAC-0177 Domain (authssl .org)
- [ ] ET MALWARE Observed UAC-0177 Domain (ssl4 .site in TLS SNI)
- [ ] ET MALWARE Observed UAC-0177 Domain (personlog .in in TLS SNI)
- [ ] ET MALWARE Observed UAC-0177 Domain (authssl .online in TLS SNI)
- [ ] ET MALWARE Observed UAC-0177 Domain (hsts .online in TLS SNI)
- [ ] ET MALWARE Observed UAC-0177 Domain (ssl2 .online in TLS SNI)
- [ ] ET MALWARE Observed UAC-0177 Domain (goaccount .link in TLS SNI)
- [ ] ET MALWARE Observed UAC-0177 Domain (ssl1 .online in TLS SNI)
- [ ] ET MALWARE Observed UAC-0177 Domain (certifiedauth .in in TLS SNI)
- [ ] ET MALWARE Observed UAC-0177 Domain (connectssl .in in TLS SNI)
- [ ] ET MALWARE Observed UAC-0177 Domain (ssl3 .site in TLS SNI)
- [ ] ET MALWARE Observed UAC-0177 Domain (exmo .day in TLS SNI)
- [ ] ET MALWARE Observed UAC-0177 Domain (ssl4 .online in TLS SNI)
- [x] ET MALWARE Possible W4SP Stealer CnC Checkin
- [x] ET MALWARE CloudAtlas APT Related Maldoc Activity M2 (GET)
- [x] ET MALWARE Malicious Loader Related Activity (GET)
- [x] ET MALWARE JaskaGO CnC Host Profile Exfil
- [x] ET MALWARE BlackRain User-Agent Observed
- [x] ET MALWARE Observed Brute Ratel Framework Related Domain (azureclouder .com in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related Activity M2
- [x] ET MALWARE Win32/Koi Loader CnC Checkin M2
- [x] ET MALWARE Win32/Koi Stealer CnC Checkin
- [x] ET MALWARE Win32/Unknown Stealer CnC Domain in DNS Lookup (webvideoshareonline .com)
- [x] ET MALWARE Win32/Koi Loader/Stealer CnC Domain in DNS Lookup (podologie-werne .de)
- [x] ET MALWARE Lumma Stealer Related Activity
- [x] ET MALWARE Observed Lumma Stealer Related Domain (agedelayglacierwe .pw in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (chincenterblandwka .pw)
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (neighborhoodfeelsa .fun)
- [ ] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .places .creeksidehuntingpreserve .com)
- [x] ET MALWARE TA451 FalseFont Backdoor Related Domain in DNS Lookup (digitalcodecrafters .com)

- [x] ET MALWARE Observed TA451 FalseFont Backdoor Related Domain (digitalcodecrafters .com in TLS SNI)
- [x] ET MALWARE Suspected Turla APT Kazuar Backdoor Related Activity
- [x] ET MALWARE Observed DNS Query to FIN7/Carbanak Related Domain (sun876954 .space)
- [x] ET MALWARE Suspected FIN7/Carbanak Related Payload C2 Downloader (GET)
- [x] ET MALWARE Rezlt RDP Grabber - This is Not RDP
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (politefrightenpowoa .pw)
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (carstirgapcheatdeposwte .pw)
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (recessionconceptjetwe .pw)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (recessionconceptjetwe .pw in TLS SNI)
- [x] ET MALWARE BlueNoroff APT Related Activity M1 (POST)
- [x] ET MALWARE DNS Query to Malicious Domain (steam-install .run)
- [x] ET MALWARE Win32/Sfuzuan Variant Payload Fetch
- [x] ET MALWARE SocGholish Domain in TLS SNI (ebooks .ferrelljoe .com)
- [x] ET MALWARE Suspected Generic PHP Backdoor Activity M2
- [x] ET MALWARE Ducktail APT Style Payload Request
- [x] ET MALWARE Agrius Group ASPXSpy Webshell Connection Inbound M2
- [x] ET MALWARE Agrius Group Webshell Command Execution Attempt
- [x] ET MALWARE DNS Query to Gamaredon Domain (koroglugo .shop)
- [x] ET MALWARE Observed Gamaredon Domain (plutoniumo .ru in TLS SNI)
- [x] ET MALWARE Observed Gamaredon Domain (raidla .ru in TLS SNI)
- [ ] ET MALWARE Gamaredon APT Related Maldoc Activity (GET)
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (referralpublicationjk .pw)
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (latetemporarynuance .pw)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (latetemporarynuance .pw in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (blastechohackopeower .pw in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (reviveincapablewew .pw in TLS SNI)
- [x] ET MALWARE Sharp Panda APT Related Domain in DNS Lookup (openxmlformats .shop)
- [x] ET MALWARE SocGholish Domain in TLS SNI (retraining .allstardriving .org)
- [x] ET MALWARE Suspected TA451 Related FalseFont Backdoor Activity M2
- [x] ET MALWARE Observed Lumma Stealer Related Domain (evokenumberpottruckere .fun in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (goddirtybrilliancece .fun in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (maskmusicalproplemanw .pw in TLS SNI)
- [ ] ET MALWARE Test CnC Domain in DNS Lookup (test .com)
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (sideindexfollowragelrew .pw)
- [x] ET MALWARE TrollAgent CnC Domain in DNS Lookup (ar .kostin .p-e .kr)
- [x] ET MALWARE TrollAgent Checkin
- [x] ET MALWARE Observed Lumma Stealer Related Domain (ranchguarrelguidewa .pw in TLS SNI)
- [x] ET MALWARE TrollAgent CnC Domain in DNS Lookup (winters .r-e .kr)
- [x] ET MALWARE Observed TrollAgent Domain (winters .r-e .kr in TLS SNI)
- [x] ET MALWARE Turla APT Kazuar Backdoor Related Activity
- [x] ET MALWARE Generic Stealer Checkin
- [x] ET MALWARE Observed FIN7/Carbanak Related Domain (sun876954 .space in TLS SNI)
- [x] ET MALWARE Snake Keylogger HTTP Exfil
- [x] ET MALWARE Kimsuky APT Related Win32/RftRAT Activity
- [x] ET MALWARE Observed Lumma Stealer Related Domain (politefrightenpowoa .pw in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (carstirgapcheatdeposwte .pw in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (opposesicknessopw .pw)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (opposesicknessopw .pw in TLS SNI)
- [x] ET MALWARE BlueNoroff APT Related Activity M2 (POST)
- [x] ET MALWARE Win32/Sfuzuan Variant Payload Fetch
- [x] ET MALWARE SocGholish Domain in DNS Lookup (ebooks .ferrelljoe .com)
- [x] ET MALWARE Suspected Generic PHP Backdoor Activity M1
- [x] ET MALWARE Generic PHP Backdoor CnC Response
- [x] ET MALWARE Agrius Group ASPXSpy Webshell Connection Inbound M1
- [x] ET MALWARE Agrius Group Webshell File Upload Attempt
- [x] ET MALWARE DNS Query to Gamaredon Domain (plutoniumo .ru)
- [x] ET MALWARE DNS Query to Gamaredon Domain (raidla .ru)
- [x] ET MALWARE Observed Gamaredon Domain (koroglugo .shop in TLS SNI)
- [x] ET MALWARE Gamaredon APT Related Maldoc Activity (POST)
- [x] ET MALWARE Observed Lumma Stealer Related Domain in TLS SNI (referralpublicationjk .pw)
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (playerweighmailydailew .pw)
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (blastechohackopeower .pw)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (playerweighmailydailew .pw in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (reviveincapablewew .pw)
- [x] ET MALWARE Sharp Panda APT Related Activity M3
- [x] ET MALWARE SocGholish Domain in DNS Lookup (retraining .allstardriving .org)
- [x] ET MALWARE Suspected TA451 Related FalseFont Backdoor Activity M1
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (evokenumberpottruckere .fun)
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (goddirtybrilliancece .fun)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (maskmusicalproplemanw .pw)
- [ ] ET MALWARE TrollAgent CnC Domain in DNS Lookup (ar .kostin .p-e .kr)
- [ ] ET MALWARE X CnC Domain in DNS Lookup (test .com)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (sideindexfollowragelrew .pw in TLS SNI)
- [x] ET MALWARE Suspected TA451 Related FalseFont Backdoor Activity M3
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (ranchguarrelguidewa .pw)
- [x] ET MALWARE TrollAgent CnC Domain in DNS Lookup (ol .negapa .p-e .kr)
- [x] ET MALWARE TrollAgent CnC Domain in DNS Lookup (ai .kostin .p-e .kr)
- [x] ET MALWARE Observed TrollAgent Domain (ai .kostin .p-e .kr in TLS SNI)

- [x] ET MALWARE Observed TrollAgent Domain (ol .negapa .p-e .kr in TLS SNI)
- [x] ET MALWARE Observed TrollAgent Domain (ar .kostin .p-e .kr in TLS SNI)
- [x] ET MALWARE Sea Turtle APT Checkin
- [x] ET MALWARE Blister Loader Cobalt Strike C2 Profile M1
- [x] ET MALWARE Blister Loader Cobalt Strike C2 Profile M2
- [x] ET MALWARE Blister Loader Cobalt Strike C2 Profile M3
- [x] ET MALWARE Blister Loader Cobalt Strike C2 Profile M4
- [x] ET MALWARE Blister Loader Cobalt Strike C2 Profile M5
- [x] ET MALWARE Blister Loader Cobalt Strike C2 Profile M6
- [x] ET MALWARE Blister Loader Cobalt Strike C2 Profile M7
- [x] ET MALWARE Blister Loader Cobalt Strike C2 Profile M8
- [x] ET MALWARE Blister Loader Cobalt Strike C2 Profile M9
- [x] ET MALWARE Blister Loader Cobalt Strike C2 Profile M10
- [x] ET MALWARE Blister Loader Cobalt Strike C2 Profile M11
- [x] ET MALWARE Blister Loader Cobalt Strike C2 Profile M12
- [x] ET MALWARE Blister Loader Cobalt Strike C2 Profile M13
- [x] ET MALWARE Blister Loader Cobalt Strike C2 Profile M14
- [x] ET MALWARE Blister Loader Cobalt Strike C2 Profile M15
- [x] ET MALWARE Blister Loader Cobalt Strike C2 Profile M16
- [x] ET MALWARE Blister Loader Cobalt Strike C2 Profile M17
- [x] ET MALWARE Blister Loader Cobalt Strike C2 Profile M18
- [x] ET MALWARE Blister Loader Cobalt Strike C2 Profile M19
- [x] ET MALWARE Blister Loader Cobalt Strike C2 Profile M20
- [x] ET MALWARE Blister Loader Cobalt Strike C2 Profile M21
- [x] ET MALWARE Blister Loader Mythic C2 Profile M1
- [x] ET MALWARE Blister Loader Mythic C2 Profile M2
- [x] ET MALWARE Blister Loader Mythic C2 Profile M3
- [x] ET MALWARE Blister Loader Mythic C2 Profile M4
- [x] ET MALWARE Possible GIFTEDVISITOR Activity - Ivanti Connect Secure
- [x] ET MALWARE Suspected UTA0178 Domain in DNS Lookup
- [x] ET MALWARE Suspected UTA0178 Domain in DNS Lookup
- [x] ET MALWARE UTA0178 Domain in DNS Lookup
- [x] ET MALWARE Suspected UTA0178 Domain in TLS SNI
- [x] ET MALWARE Suspected UTA0178 Domain in TLS SNI
- [x] ET MALWARE UTA0178 Domain in TLS SNI
- [x] ET MALWARE OrbitalBeam CnC Token Request
- [x] ET MALWARE OrbitalBeam CnC Token Response
- [x] ET MALWARE OrbitalBeam CnC Activity (Info)
- [x] ET MALWARE OrbitalBeam CnC Response (Info)
- [x] ET MALWARE OrbitalBeam CnC Activity (Debug)
- [x] ET MALWARE Epsilon Stealer Domain in DNS Lookup (3ps1l0n .life)
- [x] ET MALWARE Observed Epsilon Stealer Domain (3ps1l0n .life) in TLS SNI
- [x] ET MALWARE SocGholish Domain in DNS Lookup (event .coachgreb .com)
- [x] ET MALWARE SocGholish Domain in TLS SNI (event .coachgreb .com)
- [ ] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (recessionconceptjetwe .pwc)
- [ ] ET MALWARE Observed Lumma Stealer Related Domain (recessionconceptjetwe .pwc in TLS SNI)
- [ ] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (recessionconceptjetwe .pwc)
- [ ] ET MALWARE Observed Lumma Stealer Related Domain (recessionconceptjetwe .pwc in TLS SNI)
- [ ] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (copyexpertisesausewaverw .site)
- [ ] ET MALWARE Observed Lumma Stealer Related Domain (copyexpertisesausewaverw .site in TLS SNI)
- [x] ET MALWARE Jupyter Stealer CnC Checkin M2
- [x] ET MALWARE Win32/Rust Miner CnC Activity
- [x] ET MALWARE HailBot CnC Domain in DNS Lookup (asdsdfjsdfsd .indy)
- [x] ET MALWARE HailBot CnC Domain in DNS Lookup (jiggaboo .oss)
- [x] ET MALWARE HailBot CnC Domain in DNS Lookup (pposdif .parody)
- [x] ET MALWARE HailBot CnC Domain in DNS Lookup (sfdopospdofpsdo .dyn)
- [x] ET MALWARE HailBot CnC Domain in DNS Lookup (wendykortiz .gopher)
- [x] ET MALWARE HailBot CnC Domain in DNS Lookup (yoursocuteong .dyn)
- [x] ET MALWARE Observed HailBot Domain (asdsdfjsdfsd .indy in TLS SNI)
- [x] ET MALWARE Observed HailBot Domain (jiggaboo .oss in TLS SNI)
- [x] ET MALWARE Observed HailBot Domain (pposdif .parody in TLS SNI)
- [x] ET MALWARE Observed HailBot Domain (sfdopospdofpsdo .dyn in TLS SNI)
- [x] ET MALWARE Observed HailBot Domain (wendykortiz .gopher in TLS SNI)
- [x] ET MALWARE Observed HailBot Domain (yoursocuteong .dyn in TLS SNI)
- [x] ET MALWARE HailBot Server Response
- [x] ET MALWARE Hailbot CnC Checkin
- [x] ET MALWARE SocGholish Domain in DNS Lookup (surprise .refillpantrysd .com)
- [x] ET MALWARE SocGholish Domain in TLS SNI (surprise .refillpantrysd .com)
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (contextsuffreintymore .fun)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (contextsuffreintymore .fun in TLS SNI)
- [x] ET MALWARE BackConnect CnC Activity (Set Sleep Timer)
- [x] ET MALWARE BackConnect CnC Activity (Bot Task Request) M1
- [x] ET MALWARE BackConnect CnC Activity (Bot Task Request) M2
- [x] ET MALWARE BackConnect CnC Activity (Bot Error) M1
- [x] ET MALWARE BackConnect CnC Activity (Bot Error) M2
- [x] ET MALWARE BackConnect CnC Activity (Bot Reconnect) M1
- [x] ET MALWARE BackConnect CnC Activity (Start SOCKS) M1
- [x] ET MALWARE BackConnect CnC Activity (Start SOCKS) M2
- [x] ET MALWARE BackConnect CnC Activity (Start VNC) M1
- [x] ET MALWARE BackConnect CnC Activity (Start VNC) M2
- [x] ET MALWARE BackConnect CnC Activity (Start VNC) M3
- [x] ET MALWARE BackConnect CnC Activity (Start VNC) M4
- [x] ET MALWARE BackConnect CnC Activity (Start File Manager) M1
- [x] ET MALWARE BackConnect CnC Activity (Start File Manager) M2
- [x] ET MALWARE BackConnect CnC Activity (Start Reverse Shell) M1
- [x] ET MALWARE BackConnect CnC Activity (Start Reverse Shell) M2
- [x] ET MALWARE BackConnect CnC Activity (Bot Reconnect) M2
- [x] ET MALWARE Win32/Neptune Loader Activity (GET)
- [x] ET MALWARE [ANY.RUN] Xeno-RAT TCP Check-In
- [x] ET MALWARE [ANY.RUN] Xeno-RAT TCP Keep-Alive
- [x] ET MALWARE [ANY.RUN] Socks5Systemz HTTP C2 Connection M2
- [x] ET MALWARE DNS Query to TA453 Domain (coral-polydactyl-dragonfruit .glitch .me)
- [x] ET MALWARE DNS Query to TA453 Domain (kwhfibejjyxregxmnpcs .supabase .co)
- [x] ET MALWARE DNS Query to TA453 Domain (cloud-document-edit .onrender .com)
- [x] ET MALWARE DNS Query to TA453 Domain (ndrrftqrlblfecpupppp .supabase .co)
- [x] ET MALWARE DNS Query to TA453 Domain (east-healthy-dress .glitch .me)
- [x] ET MALWARE DNS Query to TA453 Domain (epibvgvoszemkwjnplyc .supabase .co)
- [x] ET MALWARE Observed TA453 Domain (coral-polydactyl-dragonfruit .glitch .me in TLS SNI)

- [x] ET MALWARE Observed TA453 Domain (kwhfibejjyxregxmnpcs .supabase .co in TLS SNI)
- [x] ET MALWARE Observed TA453 Domain (ndrrftqrlblfecpupppp .supabase .co in TLS SNI)
- [x] ET MALWARE Observed TA453 Domain (epibvgvoszemkwjnplyc .supabase .co in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (worrystitchsounddywuwp .site)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (copyrightspareddcitwew .site)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (combinethemepiggerygoj .site)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (expenditureddisumilarwo .site)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (worrystitchsounddywuwp .site in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (weedpairfolkloredheryw .site in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (paperambiguonusphoterew .site)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (combinethemepiggerygoj .site in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (lendremindcenterpassew .site in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (accouncementdivecane .site in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (fleetconsciousnessjuiw .site in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (carpetcupboardtejjerew .site in TLS SNI)
- [x] ET MALWARE Win32/AdAptertrAin CnC Server Checkin
- [x] ET MALWARE Khepri CnC Domain in DNS Lookup (securecrt .cc)
- [x] ET MALWARE Khepri CnC Domain in DNS Lookup (securecrt .vip)
- [x] ET MALWARE Khepri CnC Domain in DNS Lookup (macnavicat .com)
- [x] ET MALWARE Khepri CnC Domain in DNS Lookup (ultraedit .vip)
- [x] ET MALWARE Khepri CnC Domain in DNS Lookup (finalshell .me)
- [x] ET MALWARE Khepri CnC Domain in DNS Lookup (xmindcn .cc)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (benddiscoleideasbridrew .site in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (lastbishopmultiplyeow .site in TLS SNI)
- [x] ET MALWARE [ANY.RUN] ZharkBOT HTTP CnC Checkin
- [x] ET MALWARE Brosql Stealer Browser Login Exfil
- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (app .documentoffice .club)
- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (benefitinfo .pro)
- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (careagency .online)
- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (crareceive .site)
- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (depositurl .lat)
- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (forex .traderfree .online)
- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (groceryrebate .site)
- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (instantreceive .org)
- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (receive .bio)
- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (rentsubsidy .help)
- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (tinyurlinstant .co)
- [x] ET MALWARE Observed TA453 Domain (cloud-document-edit .onrender .com in TLS SNI)
- [x] ET MALWARE Observed TA453 Domain (east-healthy-dress .glitch .me in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (groannysoapblockedstiw .site)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (weedpairfolkloredheryw .site)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (qualifiedbehaviorrykej .site)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (lendremindcenterpassew .site)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (groannysoapblockedstiw .site in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (paperambiguonusphoterew .site in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (copyrightspareddcitwew .site in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (expenditureddisumilarwo .site in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (qualifiedbehaviorrykej .site in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (accouncementdivecane .site)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (fleetconsciousnessjuiw .site)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (carpetcupboardtejjerew .site)
- [x] ET MALWARE Win32/AdAptertrAin CnC Server Response
- [x] ET MALWARE Trojanized Software Download Domain in DNS Lookup (macyy .cn)
- [x] ET MALWARE Khepri CnC Domain in DNS Lookup (ultraedit .info)
- [x] ET MALWARE Khepri CnC Domain in DNS Lookup (rdesktophub .com)
- [x] ET MALWARE Khepri CnC Domain in DNS Lookup (vscode .digital)
- [x] ET MALWARE Khepri CnC Domain in DNS Lookup (finallshell .cc)
- [x] ET MALWARE Khepri CnC Domain in DNS Lookup (rdesktopconnect .com)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (benddiscoleideasbridrew .site)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (lastbishopmultiplyeow .site)
- [x] ET MALWARE Atomic Stealer Related Activity (POST)
- [x] ET MALWARE Brosql Stealer Screenshot Exfil
- [x] ET MALWARE Brosql Stealer Browser Cookie Exfil
- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (benefitinfo .live)
- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (benefiturl .pro)
- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (cra-receivenow .online)
- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (depositurl .co)
- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (direct .traderfree .online)
- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (groceryrebate .online)
- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (gstcreceive .online)
- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (nav .offlinedocument .site)
- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (receiveinstant .online)
- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (rentsubsidy .online)
- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (urldepost .co)

- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (verifyca .online)
- [ ] ET MALWARE ScarCruft TA409 Domain in DNS Lookup (visiononline .store)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (app .documentoffice .club)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (benefitinfo .live)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (benefitinfo .pro)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (benefiturl .pro)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (careagency .online)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (cra-receivenow .online)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (crareceive .site)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (depositurl .co)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (depositurl .lat)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (direct .traderfree .online)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (forex .traderfree .online)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (groceryrebate .online)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (groceryrebate .site)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (gstcreceive .online)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (instantreceive .org)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (nav .offlinedocument .site)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (receive .bio)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (receiveinstant .online)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (rentsubsidy .help)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (rentsubsidy .online)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (tinyurlinstant .co)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (urldepost .co)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (verifyca .online)
- [ ] ET MALWARE ScarCruft TA409 Domain in TLS SNI (visiononline .store)
- [ ] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (demonstratorleasheropw .site)
- [ ] ET MALWARE Observed Lumma Stealer Related Domain (demonstratorleasheropw .site in TLS SNI)
- [x] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .colors .usajicgu .com)
- [x] ET MALWARE SocGholish CnC Domain in TLS SNI (* .colors .usajicgu .com)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (racerecessionrestrai .site)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (cooperatecliqueobstac .site)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (braidfadefriendklypk .site)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (vesselspeedcrosswakew .site)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (communicationinchoicer .site)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (carvewomanflavourwop .site)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (retainfactorypunishjkw .site)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (willpoweragreebokkskiew .site)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (willpoweragreebokkskiew .site in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (braidfadefriendklypk .site in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (racerecessionrestrai .site in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (vesselspeedcrosswakew .site in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (brickabsorptiondullyi .site in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (retainfactorypunishjkw .site in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (communicationinchoicer .site in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (willpoweragreebokkskiew .site in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (carvewomanflavourwop .site in TLS SNI)
- [ ] ET MALWARE Observed Lumma Stealer Related Domain (vesselspeedcrosswakew .site in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (cooperatecliqueobstac .site in TLS SNI)
- [ ] ET MALWARE Observed Lumma Stealer Related Domain (racerecessionrestrai .site in TLS SNI)
- [ ] ET MALWARE Observed Lumma Stealer Related Domain (braidfadefriendklypk .site in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (gearboomchocolateowfs .site)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (gearboomchocolateowfs .site in TLS SNI)
- [x] ET MALWARE [ANY.RUN] RadX RAT Check-In (POST)
- [x] ET MALWARE [ANY.RUN] RadX RAT Keep-Alive Activity (POST)
- [x] ET MALWARE Win32/Cobalt Strike CnC Activity M1
- [x] ET MALWARE Win32/Cobalt Strike CnC Activity M2
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (brickabsorptiondullyi .site)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (crisisestimatehealtwh .site)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (crisisestimatehealtwh .site in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (consciouosoepewmausj .site)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (consciouosoepewmausj .site in TLS SNI)
- [x] ET MALWARE nspx30 Backdoor Trigger Response Observed
- [x] ET MALWARE nspx30 Orchestrator CnC Checkin
- [x] ET MALWARE Earth Preta PUBLOAD Activity M2
- [x] ET MALWARE Earth Preta PUBLOAD Activity M3
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (mealroomrallpassiveer .shop)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (mealroomrallpassiveer .shop in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (tonguehypnothesislan .shop)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (tonguehypnothesislan .shop in TLS SNI)
- [x] ET MALWARE Allakore RAT CnC Domain in DNS Lookup (hhplaytom .com)
- [x] ET MALWARE Allakore RAT CnC Domain in DNS Lookup (uperrunplay .com)
- [x] ET MALWARE Allakore RAT CnC Domain in DNS Lookup (zulabra .com)
- [x] ET MALWARE Allakore RAT CnC Domain in DNS Lookup (uplayground .online)
- [x] ET MALWARE Allakore RAT CnC Domain in DNS Lookup (flapawer .com)
- [x] ET MALWARE Allakore RAT CnC Domain in DNS Lookup (chaucheneguer .com)

- [x] ET MALWARE SocGholish Domain in DNS Lookup (miner .eastestsite .com)
- [x] ET MALWARE SocGholish Domain in TLS SNI (miner .eastestsite .com)
- [x] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .honors .howamerica .com)
- [x] ET MALWARE SocGholish CnC Domain in TLS SNI (* .honors .howamerica .com)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (cultureskетchfinanciall .shop)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (secretionsuitcasenioise .shop)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (claimconcessionrebe .shop)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (liabilityarrangemenyit .shop)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (gemcreedarticulateod .shop)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (modestessayevenmilwek .shop)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (sofahuntingslidedine .shop)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (triangleseasonbenchwj .shop)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (triangleseasonbenchwj .shop in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (claimconcessionrebe .shop in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (cultureskетchfinanciall .shop in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (gemcreedarticulateod .shop in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (sofahuntingslidedine .shop in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (modestessayevenmilwek .shop in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (secretionsuitcasenioise .shop in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (liabilityarrangemenyit .shop in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (nationalistvetecanve .shop)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (nationalistvetecanve .shop in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (cakecoldsplurgrewe .pw)
- [ ] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (bombertublestylebanws .fun)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (diagramfiremonkeyowwa .fun)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (dayfarrichjwclik .fun)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (ratefacilityframw .fun)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (cakecoldsplurgrewe .pw in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (bombertublestylebanws .fun in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (diagramfiremonkeyowwa .fun in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (dayfarrichjwclik .fun in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (ratefacilityframw .fun in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (healthrankunderow .fun)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (healthrankunderow .fun in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (cakecoldsplurgrewe .pw)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (cakecoldsplurgrewe .pw in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (offerimagefancine .shop)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (offerimagefancine .shop in TLS SNI)
- [ ] ET MALWARE [ANY.RUN] ToneShell FakeTLS Check-In (APT Mustang Panda / Earth Preta) M1
- [ ] ET MALWARE [ANY.RUN] BACKDOOR [ANY.RUN] ToneShell FakeTLS Check-In (APT Mustang Panda / Earth Preta) M2
- [ ] ET MALWARE [ANY.RUN] ToneShell FakeTLS Response (APT Mustang Panda / Earth Preta) M1
- [ ] ET MALWARE [ANY.RUN] ToneShell FakeTLS Response (APT Mustang Panda / Earth Preta) M2
- [x] ET MALWARE [ANY.RUN] WhiteSnake Stealer HTTP Request
- [x] ET MALWARE [ANY.RUN] WhiteSnake Stealer HTTP POST Report Exfiltration
- [x] ET MALWARE Allakore RAT CnC Checkin M2
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (fantasticabnormally .shop)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (fantasticabnormally .shop in TLS SNI)
- [x] ET MALWARE DNS Query to Malicious Domain (pdfmicrosoft .ddns .net)
- [x] ET MALWARE Observed Malicious Domain (pdfmicrosoft .ddns .net in TLS SNI)
- [x] ET MALWARE KrustyLoader CnC Domain in DNS Lookup (farstream .org)
- [x] ET MALWARE KrustyLoader CnC Domain in DNS Lookup (sysupdates .org)
- [x] ET MALWARE Observed KrustyLoader Domain (farstream .org) in TLS SNI
- [x] ET MALWARE Observed KrustyLoader Domain (sysupdates .org) in TLS SNI
- [x] ET MALWARE KrustyLoader CnC Domain in DNS Lookup (be-at-home .s3 .ap-northeast-2 .amazonaws .com)
- [x] ET MALWARE KrustyLoader CnC Domain in DNS Lookup (bbr-promo .s3 .amazonaws .com)
- [x] ET MALWARE KrustyLoader CnC Domain in DNS Lookup (bigtimeassets .s3 .amazonaws .com)
- [x] ET MALWARE KrustyLoader CnC Domain in DNS Lookup (acapros-app .s3-us-west-2 .amazonaws .com)
- [x] ET MALWARE KrustyLoader CnC Domain in DNS Lookup (beansdeals-static .s3 .amazonaws .com)
- [x] ET MALWARE KrustyLoader CnC Domain in DNS Lookup (bringthenoiseappnew .s3 .amazonaws .com)
- [x] ET MALWARE KrustyLoader CnC Domain in DNS Lookup (2261992 .s3 .amazonaws .com)
- [x] ET MALWARE KrustyLoader CnC Domain in DNS Lookup (ahha-asset .s3 .ap-northeast-2 .amazonaws .com)
- [x] ET MALWARE KrustyLoader CnC Domain in DNS Lookup (breaknlinks .s3 .amazonaws .com)
- [x] ET MALWARE HTTP POST with Suspicious User-Agent Observed - Possible ZLoader Activity M1
- [x] ET MALWARE HTTP POST with Suspicious User-Agent Observed - Possible ZLoader Activity M2
- [x] ET MALWARE LIGHTWIRE Web Shell Activity Observed
- [x] ET MALWARE CHAINLINE Web Shell Activity Observed
- [x] ET MALWARE FRAMEREST Web Shell Activity Observed
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (knonkcdalfyhitt .shop)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (knonkcdalfyhitt .shop in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (birdvigorousedetertyw .shop)

- [x] ET MALWARE Observed Lumma Stealer Related Domain (birdvigorousedetertyw .shop in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (telldruggcommitetter .shop in TLS SNI)
- [x] ET MALWARE Suspected TA451 Related FalseFont Backdoor Activity M5
- [x] ET MALWARE RubySleet APT TrollAgent CnC Checkin
- [x] ET MALWARE RubySleet APT TrollAgent CnC Domain in DNS Lookup (ai .kostin .p-e .kr)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (feturepoudbicchteo .shop in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (pavementpreferencewjiao .site in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (despairphtsograpgp .shop in TLS SNI)
- [x] ET MALWARE Mispadu Stealer CnC Checkin M2
- [x] ET MALWARE SocGholish CnC Domain in TLS SNI (* .our .openarmscv .org)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (samplepoisonbarryntj .shop in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (decorousnumerousieo .shop in TLS SNI)
- [x] ET MALWARE DNS Query to XWORM Domain (sponsored-ate .gl .at .ply .gg)
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (resergvearyinitiani .shop)
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (landgateindirectdangre .shop)
- [x] ET MALWARE FormBook CnC Checkin (GET) M5
- [x] ET MALWARE Observed Lumma Stealer Related Domain (flexibleagttypoceo .shop in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (exitassumebangpastcone .shop in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (vatleaflettrusteeooj .shop in TLS SNI)
- [x] ET MALWARE SocGholish CnC Domain in TLS SNI (* .day .50adayplan .com)
- [x] ET MALWARE MacOS RustDoor Related Activity M2 (POST)
- [x] ET MALWARE Observed MacOS RustDoor Related Domain (serviceicloud .com in TLS SNI)
- [x] ET MALWARE [ANY.RUN] Meduza Stealer Exfiltration M2
- [x] ET MALWARE Synapse/Lambda Ransomware CnC Checkin
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (bicyclesunhygenico .fun)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (antiuncontemporary .fun)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (unexaminablespectrall .fun)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (fishboatnurrybeauti .fun)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (bicyclesunhygenico .fun in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (antiuncontemporary .fun in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (unexaminablespectrall .fun in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (fishboatnurrybeauti .fun in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (bleednumberrottern .home)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (bleednumberrottern .home in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (lawwormroleveinn .mom)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (telldruggcommitetter .shop)
- [x] ET MALWARE Suspected TA451 Related FalseFont Backdoor Activity M4
- [ ] ET MALWARE Suspected TA451 Related FalseFont Backdoor Response
- [x] ET MALWARE RubySleet APT TrollAgent CnC Domain in DNS Lookup (ol .negapa .p-e .kr)
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (feturepoudbicchteo .shop)
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (pavementpreferencewjiao .site)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (despairphtsograpgp .shop)
- [x] ET MALWARE Mispadu Stealer CnC Checkin M1
- [x] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .our .openarmscv .org)
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (samplepoisonbarryntj .shop)
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (decorousnumerousieo .shop)
- [x] ET MALWARE DNS Query to Malware Delivery Domain (a0917004 .xsph .ru)
- [x] ET MALWARE Observed Malware Delivery Domain (a0917004 .xsph .ru in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (resergvearyinitiani .shop in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (landgateindirectdangre .shop in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (flexibleagttypoceo .shop)
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (exitassumebangpastcone .shop)
- [x] ET MALWARE Lumma Stealer Related Domain in DNS Lookup (vatleaflettrusteeooj .shop)
- [x] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .day .50adayplan .com)
- [x] ET MALWARE MacOS RustDoor Related Activity M1 (POST)
- [x] ET MALWARE MacOS RustDoor Related CnC Domain in DNS Lookup (serviceicloud .com)
- [x] ET MALWARE Observed Malicious Domain (ewbjr2h375tjz5fh3wvohsetk .com in TLS SNI)
- [x] ET MALWARE [ANY.RUN] Possible Meduza Stealer Exfiltration (TCP)
- [x] ET MALWARE PikaBot Java Loader CnC Checkin
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (reechoingkaolizationp .fun)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (pielumchalotpostwo .fun)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (muggierdragstemmio .fun)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (mazumaponyanthus .fun)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (reechoingkaolizationp .fun in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (pielumchalotpostwo .fun in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (muggierdragstemmio .fun in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (mazumaponyanthus .fun in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (brakesummitfiightre .pics)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (brakesummitfiightre .pics in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (baresoakopiniocowe .fun)

- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (baketransparentadw .pics)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (mercyaloofprincipleo .pics)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (hunterstrawmersp .home)
- ET MALWARE Observed Lumma Stealer Related Domain (baresoakopiniocowe .fun in TLS SNI)
- ET MALWARE Observed Lumma Stealer Related Domain (legislationdictater .mom in TLS SNI)
- ET MALWARE Observed Lumma Stealer Related Domain (developmentalveiop .home in TLS SNI)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (ironshottallinko .funu)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (lawwormroleveinn .momu)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (scshemevalleywelferw .site)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (snuggleapplicationswo .fun)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (theoryapparatusjuko .fun)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (punchtelephoneverdi .store)
- ET MALWARE Observed Lumma Stealer Related Domain (snuggleapplicationswo .fun in TLS SNI)
- ET MALWARE Observed Lumma Stealer Related Domain (theoryapparatusjuko .fun in TLS SNI)
- ET MALWARE Observed Lumma Stealer Related Domain (punchtelephoneverdi .store in TLS SNI)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (fossillandscapefewkew .site)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (townsfolkhiwoeko .fun)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (colonmoonmushroo .mom)
- ET MALWARE Pikabot Related Activity M5 (POST)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (cattilecodereowop .pw)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (thinrecordsunrjisow .pw)
- ET MALWARE BunnyLoader 3.0 Initial Checkin
- ET MALWARE BunnyLoader 3.0 Heartbeat Checkin
- ET MALWARE BunnyLoader 3.0 Tasking Checkin
- ET MALWARE BunnyLoader 3.0 Echo Checkin
- ET MALWARE BunnyLoader 3.0 CID Checkin
- ET MALWARE JS/GootLoader Activity M2 (GET)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (theoryapparatusjuko .funr)
- ET MALWARE Observed Lumma Stealer Related Domain (theoryapparatusjuko .funr in TLS SNI)
- ET MALWARE TinyTurlaNG Turla APT GetTask Request
- ET MALWARE DNS Query to TinyTurla Domain (jeepcarlease .com)
- ET MALWARE DNS Query to TinyTurla Domain (buy-new-car .com)
- ET MALWARE DNS Query to TinyTurla Domain (hanagram .jp)
- ET MALWARE Observed TinyTurla Domain (jeepcarlease .com in TLS SNI)
- ET MALWARE Observed TinyTurla Domain (buy-new-car .com in TLS SNI)
- ET MALWARE Observed TinyTurla Domain (hanagram .jp in TLS SNI)
- ET MALWARE SocGholish CnC Domain in TLS SNI (* .members .openarmscv .com)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (pooreveningfuseor .pw)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (problemregardybuiwo .fun)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (legislationdictater .mom)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (developmentalveiop .home)
- ET MALWARE Observed Lumma Stealer Related Domain (lawwormroleveinn .mom in TLS SNI)
- ET MALWARE Observed Lumma Stealer Related Domain (baketransparentadw .pics in TLS SNI)
- ET MALWARE Observed Lumma Stealer Related Domain (mercyaloofprincipleo .pics in TLS SNI)
- ET MALWARE Observed Lumma Stealer Related Domain (hunterstrawmersp .home in TLS SNI)
- ET MALWARE Observed Lumma Stealer Related Domain (ironshottallinko .funu in TLS SNI)
- ET MALWARE Observed Lumma Stealer Related Domain (lawwormroleveinn .momu in TLS SNI)
- ET MALWARE Observed Lumma Stealer Related Domain (scshemevalleywelferw .site in TLS SNI)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (strainriskpropos .store)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (telephoneverdictyow .site)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (smallrabbitcrossing .site)
- ET MALWARE Observed Lumma Stealer Related Domain (strainriskpropos .store in TLS SNI)
- ET MALWARE Observed Lumma Stealer Related Domain (telephoneverdictyow .site in TLS SNI)
- ET MALWARE Observed Lumma Stealer Related Domain (smallrabbitcrossing .site in TLS SNI)
- ET MALWARE Observed Lumma Stealer Related Domain (fossillandscapefewkew .site in TLS SNI)
- ET MALWARE Observed Lumma Stealer Related Domain (townsfolkhiwoeko .fun in TLS SNI)
- ET MALWARE Observed Lumma Stealer Related Domain (colonmoonmushroo .mom in TLS SNI)
- ET MALWARE Possible PikaBot Java Loader CnC Checkin
- ET MALWARE Observed Lumma Stealer Related Domain (cattilecodereowop .pw in TLS SNI)
- ET MALWARE Observed Lumma Stealer Related Domain (thinrecordsunrjisow .pw in TLS SNI)
- ET MALWARE BunnyLoader 3.0 Initial Checkin Response
- ET MALWARE BunnyLoader 3.0 Heartbeat Response
- ET MALWARE BunnyLoader 3.0 Tasking Response
- ET MALWARE BunnyLoader 3.0 DBID Checkin
- ET MALWARE DOILoader Activity M2 (GET)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (healthproline .pro)
- ET MALWARE Observed Lumma Stealer Related Domain (healthproline .pro in TLS SNI)
- ET MALWARE TinyTurlaNG Turla APT Initial Client Beacon
- ET MALWARE DNS Query to TinyTurla Domain (caduff-sa .ch)
- ET MALWARE DNS Query to TinyTurla Domain (carleasingguru .com)
- ET MALWARE DNS Query to TinyTurla Domain (thefinetreats .com)
- ET MALWARE Observed TinyTurla Domain (caduff-sa .ch in TLS SNI)
- ET MALWARE Observed TinyTurla Domain (carleasingguru .com in TLS SNI)
- ET MALWARE Observed TinyTurla Domain (thefinetreats .com in TLS SNI)
- ET MALWARE SocGholish CnC Domain in DNS Lookup (* .members .openarmscv .com)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (associationokeo .shop)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (chocolatedepressofw .fun)
- ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (turkeyunlikelyofw .shop)

- [x] ET MALWARE Observed Lumma Stealer Related Domain (associationokeo .shop in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (chocolatedepressofw .fun in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (turkeyunlikelyofw .shop in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (theoryapparatusjuko .funy in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (greenbowelsustainny .fun in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (theoryapparatusjuko .funl in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (fikkeropendorwiw .pw in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (numberlesswortheiwol .shop in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (superiorhardwaerw .pw in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (villagemagneticcsa .fun)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (villagemagneticcsa .fun in TLS SNI)
- [x] ET MALWARE Win/Ghostlocker Ransomware Activity M2 (POST)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (woodfeetumhblefepoj .shop)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (detectordiscusser .shop in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (technologyenterdo .shop in TLS SNI)
- [x] ET MALWARE Lazarus Group Backdoor CnC Checkin M1
- [x] ET MALWARE Lazarus Group Domain in DNS Lookup (sifucanva .com)
- [x] ET MALWARE Lazarus Group Domain in DNS Lookup (chrysalisc .com)
- [x] ET MALWARE Lazarus Group Domain in DNS Lookup (thefrostery .co .uk)
- [x] ET MALWARE Observed Lazarus Group Domain (rginfotechnology .com) in TLS SNI
- [x] ET MALWARE Observed Lazarus Group Domain (thefrostery .co .uk) in TLS SNI
- [x] ET MALWARE Observed Lazarus Group Domain (chrysalisc .com) in TLS SNI
- [x] ET MALWARE Lazarus Group Domain in DNS Lookup (updating .dothome .co .kr)
- [x] ET MALWARE SocGholish Domain in TLS SNI (stake .libertariancounterpoint .com)
- [x] ET MALWARE DNS Query to Malicious Domain (kakaoteam .site)
- [x] ET MALWARE DNS Query to Malicious Domain (mofamail .shop)
- [x] ET MALWARE DNS Query to Malicious Domain (cloudown .store)
- [x] ET MALWARE DNS Query to Malicious Domain (nidnaver .info)
- [x] ET MALWARE DNS Query to Malicious Domain (naveralarm .com)
- [x] ET MALWARE DNS Query to Malicious Domain (naveralert .com)
- [x] ET MALWARE DNS Query to Malicious Domain (navercafe .info)
- [x] ET MALWARE DNS Query to Malicious Domain (upbit-service .pe .kr)
- [x] ET MALWARE DNS Query to Malicious Domain (taxservice .pe .kr)
- [x] ET MALWARE DNS Query to Malicious Domain (kakaoaccouts .store)
- [x] ET MALWARE DNS Query to Malicious Domain (nsvc .mail .server .korea)
- [x] ET MALWARE Observed Malicious Domain (kakaoteam .site in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (mofamail .shop in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (cloudown .store in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (pooreveningfuseor .pw in TLS SNI)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (problemregardybuiwo .fun in TLS SNI)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (theoryapparatusjuko .funy)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (greenbowelsustainny .fun)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (theoryapparatusjuko .funl)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (fikkeropendorwiw .pw)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (numberlesswortheiwol .shop)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (superiorhardwaerw .pw)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (pooreveningfuseor .pwl)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (pooreveningfuseor .pwl in TLS SNI)
- [x] ET MALWARE Win/Ghostlocker Ransomware Activity M1 (POST)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (detectordiscusser .shop)
- [x] ET MALWARE Lumma Stealer Related CnC Domain in DNS Lookup (technologyenterdo .shop)
- [x] ET MALWARE Observed Lumma Stealer Related Domain (woodfeetumhblefepoj .shop in TLS SNI)
- [x] ET MALWARE [ANY.RUN] SilentCryptoMiner Check-in POST Request
- [x] ET MALWARE Lazarus Group Backdoor CnC Checkin M2
- [x] ET MALWARE Lazarus Group Domain in DNS Lookup (contact .rgssm .in)
- [x] ET MALWARE Lazarus Group Domain in DNS Lookup (rginfotechnology .com)
- [x] ET MALWARE Lazarus Group Domain in DNS Lookup (job4writers .com)
- [x] ET MALWARE Observed Lazarus Group Domain (sifucanva .com) in TLS SNI
- [x] ET MALWARE Observed Lazarus Group Domain (contact .rgssm .in) in TLS SNI
- [x] ET MALWARE Observed Lazarus Group Domain (job4writers .com) in TLS SNI
- [x] ET MALWARE SocGholish Domain in DNS Lookup (stake .libertariancounterpoint .com)
- [x] ET MALWARE DNS Query to Malicious Domain (countrysvc .pe .kr)
- [x] ET MALWARE DNS Query to Malicious Domain (naverscorp .shop)
- [x] ET MALWARE DNS Query to Malicious Domain (ned .newnotification .server .korea)
- [x] ET MALWARE DNS Query to Malicious Domain (navigation .cc)
- [x] ET MALWARE DNS Query to Malicious Domain (nmail .navermail .online .korea)
- [x] ET MALWARE DNS Query to Malicious Domain (navecorps .com)
- [x] ET MALWARE DNS Query to Malicious Domain (nidnaver .help)
- [x] ET MALWARE DNS Query to Malicious Domain (civilizations .store)
- [x] ET MALWARE DNS Query to Malicious Domain (akites .site)
- [x] ET MALWARE DNS Query to Malicious Domain (mofamail .homes)
- [x] ET MALWARE DNS Query to Malicious Domain (upbit2024 .re .kr)
- [x] ET MALWARE Observed Malicious Domain (countrysvc .pe .kr in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (naverscorp .shop in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (ned .newnotification .server .korea in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (navigation .cc in TLS SNI)

- [x] ET MALWARE Observed Malicious Domain (nidnaver .info in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (naveralarm .com in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (naveralert .com in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (navercafe .info in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (upbit-service .pe .kr in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (taxservice .pe .kr in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (kakaoaccouts .store in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (nsvc .mail .server .korea in TLS SNI)
- [x] ET MALWARE Win32/AsyncRAT CnC Checkin (GET)
- [x] ET MALWARE PyRation Variant - Action Sent to Client
- [x] ET MALWARE PyRation Variant - Configuration Request
- [x] ET MALWARE DNS Query to Lactrodectus Domain
- [x] ET MALWARE Observed Lactrodectus Domain in TLS SNI
- [x] ET MALWARE Malvertising Domain in DNS Lookup (reclaimmycredit .com)
- [x] ET MALWARE Observed Malvertising Domain (reclaimmycredit .com) in TLS SNI
- [x] ET MALWARE SocGholish CnC Domain in DNS Lookup (* .collection .aixpirts .com)
- [x] ET MALWARE Win32/MarioLoader CnC Activity (POST) M1
- [x] ET MALWARE Win32/MarioLoader CnC Activity (POST) M2
- [x] ET MALWARE Malvertising Related Domain in DNS Lookup (hmgcyberschools .com)
- [x] ET MALWARE Malvertising Related Domain in DNS Lookup (legit .onelink .me)
- [x] ET MALWARE Observed Malvertising Related Domain (hmgcyberschools .com) in TLS SNI
- [x] ET MALWARE Observed Malvertising Related Domain (legit .onelink .me) in TLS SNI
- [x] ET MALWARE TA421 Wineloader CnC Checkin
- [x] ET MALWARE Suspected TA430/Andariel AndarLoader Related Domain in TLS SNI
- [x] ET MALWARE TA430/Andariel Related Domain in DNS Lookup
- [x] ET MALWARE TA430/Andariel AndarLoader Related Activity M3
- [x] ET MALWARE DNS Query to Ducktail APT Domain (123online .uk)
- [x] ET MALWARE DNS Query to Ducktail APT Domain (mafiakorea .com)
- [x] ET MALWARE Observed Ducktail Domain (123online .uk in TLS SNI)
- [x] ET MALWARE Observed Ducktail Domain (mafiakorea .com in TLS SNI)
- [x] ET MALWARE Lazarus Group Comebacker Backdoor CnC Checkin
- [x] ET MALWARE Lazarus Group Combacker CnC Domain in DNS Lookup (chaingrown .com)
- [x] ET MALWARE TA430/Andariel NukeSped Backdoor Variant Activity M1
- [x] ET MALWARE TA430/Andariel NukeSped Backdoor Variant Server Response M1
- [x] ET MALWARE DNS Query to TA455 Domain (xboxplayservice .com)
- [x] ET MALWARE Observed TA455 Domain in TLS SNI (xboxplayservice .com)
- [x] ET MALWARE Observed TA455 Domain in TLS SNI (1stemployer .com)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (vscodeupdater .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (airconnectionsapi .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (nmail .navermail .online .korea in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (navecorps .com in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (nidnaver .help in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (civilizations .store in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (akites .site in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (mofamail .homes in TLS SNI)
- [x] ET MALWARE Observed Malicious Domain (upbit2024 .re .kr in TLS SNI)
- [x] ET MALWARE Elusive Stealer CnC Exfil via Telegram
- [x] ET MALWARE PyRation Variant - Command Sent to Client
- [x] ET MALWARE PyRation Variant - Configuration Response
- [x] ET MALWARE DNS Query to Lactrodectus Domain
- [x] ET MALWARE Observed Lactrodectus Domain in TLS SNI
- [x] ET MALWARE Malvertising Domain in DNS Lookup (parsic .org)
- [x] ET MALWARE Observed Malvertising Domain (parsic .org) in TLS SNI
- [x] ET MALWARE Unknown Malvertising Payload CnC Checkin (PSecWin)
- [x] ET MALWARE SocGholish CnC Domain in TLS SNI (* .collection .aixpirts .com)
- [x] ET MALWARE Win32/MarioLoader Payload Request (GET)
- [x] ET MALWARE Unknown Powershell Malvertising Payload CnC Checkin
- [x] ET MALWARE Malvertising Related Domain in DNS Lookup (darknetlinks .wiki)
- [x] ET MALWARE Malvertising Related Domain in DNS Lookup (healthbeautycosmetics .com)
- [x] ET MALWARE Observed Malvertising Related Domain (darknetlinks .wiki) in TLS SNI
- [x] ET MALWARE Observed Malvertising Related Domain (healthbeautycosmetics .com) in TLS SNI
- [x] ET MALWARE Suspected TA430/Andariel AndarLoader Related CnC Domain in DNS Lookup
- [x] ET MALWARE TA430/Andariel AndarLoader Related Activity M1
- [x] ET MALWARE TA430/Andariel AndarLoader Related Activity M2
- [x] ET MALWARE DuckTail APT CnC Activity (GET)
- [x] ET MALWARE DNS Query to Ducktail APT Domain (mountainseagroup3 .top)
- [x] ET MALWARE DNS Query to Ducktail APT Domain (dailyfasterauto .info)
- [x] ET MALWARE Observed Ducktail Domain (mountainseagroup3 .top in TLS SNI)
- [x] ET MALWARE Observed Ducktail Domain (dailyfasterauto .info in TLS SNI)
- [x] ET MALWARE Lazarus Group Combacker CnC Domain in DNS Lookup (blockchain-newtech .com)
- [x] ET MALWARE Lazarus Group Combacker CnC Domain in DNS Lookup (fasttet .com)
- [x] ET MALWARE TA430/Andariel NukeSped Backdoor Variant Activity M2
- [x] ET MALWARE TA430/Andariel NukeSped Backdoor Variant Server Response M2
- [x] ET MALWARE Observed TA455 Domain in TLS SNI (vsliveagent .com)
- [x] ET MALWARE Observed TA455 Domain in TLS SNI (teledyneflir.com .de)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (qaquestionsapi .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (helicoptersahtests .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (regionuaequestions .azurewebsites .net in TLS SNI)

- ET MALWARE Observed UNC1549/TA455 Domain (testmanagementapisjson .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (iaidevrssfeed .cloudapp .azure .com in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (apphrquizapi .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (notebooktextchecking .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (questionsapplicationbackup .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (customercareservice .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (blogvolleyballstatus .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (emiratescheckapi .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (questionsurveyapp .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (manpowerfeedapijson .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (airconnectionapi .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (coffeeonlineshop .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (javaruntimestestapi .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (iaidevrssfeedp .cloudapp .azure .com in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (roadmapselector .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (engineeringssfeed .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (integratedblognewsapi .azurewebsites .com in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (airgadgetsolutions .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (qaquestionapi .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (iaidevrssfeed .centrualus .cloudapp .azure .com in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (boeisurveyapplications .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (helicopterahtest .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (altnametestapi .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (ilengineeringrssfeed .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (integratedblognewfeed .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (javaruntimeversionchecking .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (connectairapijson .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (integratedblognewsapi .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (notebooktextcheckings .com in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (surveyonlinetest .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (questionsapplicationapijson .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (openapplicationcheck .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (workersquestionsjson .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (checkapicountryquestionsjson .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (blognewsalphaapijson .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (notebooktextcheckings .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (onequestionsapi .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (onequestionsapicheck .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (arquestionsapi .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (uaeaircheckon .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (iaidevrssfeed .centralus .cloudapp .azure .com in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (notebooktexts .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (quiztestapplication .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (engineeringrssfeed .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (javaruntime .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (onequestions .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (logupdatemanagementapijson .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (qaquestions .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (homefurniture .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (blogvolleyballstatusapi .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (technewsblogapi .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (emiratescheckapijson .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (airgadgetsolution .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (surveyappquery .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (jupyternotebookcollection .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (hrapplicationtest .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (identifycheckapplication .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (manpowerfeedapi .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (workersquestionsapi .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (optionalapplication .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (flighthelicopterahtest .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (customercareserviceapi .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (exchtestcheckingapihealth .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (questionsdatabases .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (humanresourcesapijson .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (logsapimanagement .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (browsercheckap .azurewebsites .net in TLS SNI)
- ET MALWARE Observed UNC1549/TA455 Domain (integratedblognews .azurewebsites .net in TLS SNI)

- [x] ET MALWARE Observed UNC1549/TA455 Domain (changequestionstypeapi .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (cashcloudservices .com in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (questionsurveyappserver .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (audiomanagerapi .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (coffeeonlineshoping .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (exchtestcheckingapi .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (surveyonlinetestapi .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (personalizationsurvey .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (questionsapplicationapi .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (turkairline .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (identifycheckingapplications .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (testquestionapplicationapi .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (tnlsowki .westus3 .cloudapp .azure .com in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (registerinsurance .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (hiringarabicregion .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (countrybasedquestions .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (apphrquestion .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (javaruntimetestapi .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (browsercheckingapi .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (logupdatemanagementapi .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (qaquestionsapijson .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (sportblogs .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (changequestiontypesapi .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (intergratedblognewsapi .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (queryfindquestions .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (queryquestions .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (checkapicountryquestions .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (audioservicetestapi .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (workersquestions .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (uaeairchecks .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (jupyternotebookscollection .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (refaeldevrssfeed .centralus .cloudapp .azure .com in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (apphrquestions .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (personalitytestquestionapi .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (tnlsowkis .westus3 .cloudapp .azure .com in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (humanresourcesapi .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (checkservicecustomerapi .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (testtesttes .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (humanresourcesapiquiz .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (jupyternotebookcollections .com in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (jupyternotebookcollections .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (helicopterahtests .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (changequestiontypes .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (testmanagementapi1 .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (browsercheckjson .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (answerssurveytest .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (airconnectionsapijson .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (changequestionstypejsonapi .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (marineblogapi .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (logsapimanagements .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (javaruntimeversioncheckingapi .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (identifycheckapplications .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (connectionhandlerapi .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (testmanagementapis .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (tiappschecktest .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (arquestions .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (roadmapselectorapi .azurewebsites .net in TLS SNI)
- [x] ET MALWARE Observed UNC1549/TA455 Domain (birngthemhomenow .co .il in TLS SNI)
- [ ] GPL MALWARE BackOrifice access

- [x] **emerging-misc.rules** Hide

- [ ] ET MISC HP Web JetAdmin ExecuteFile admin access
- [ ] GPL MISC Teardrop attack
- [ ] GPL MISC Ascend Route
- [ ] GPL MISC Finger remote command execution attempt
- [ ] GPL MISC Finger remote command pipe execution attempt
- [ ] GPL MISC Finger bomb attempt
- [ ] GPL MISC Time-To-Live Exceeded in Transit
- [ ] GPL MISC Connection Closed MSG from Port 80
- [ ] GPL MISC source route ssrr
- [ ] GPL MISC Source Port 20 to <1024
- [ ] GPL MISC source port 53 to <1024
- [x] GPL MISC Invalid PCAnywhere Login
- [ ] GPL MISC xdmcp query
- [ ] GPL MISC ip reserved bit set
- [x] GPL MISC rlogin bin
- [x] GPL MISC rlogin echo++

- [x] GPL MISC rlogin root
- [x] GPL MISC rsh froot
- [x] GPL MISC ident version request
- [x] GPL MISC rwhoisd format string attempt
- [x] GPL MISC UPnP Location overflow
- [ ] GPL MISC Unassigned/Reserved IP protocol
- [ ] GPL MISC UPnP service discover attempt
- [ ] GPL MISC bootp invalid hardware type
- [x] GPL MISC CVS invalid repository response
- [x] GPL MISC CVS invalid directory response
- [x] GPL MISC CVS invalid module response
- [ ] GPL MISC BGP invalid length
- [ ] GPL MISC IP Proto 53 SWIPE
- [ ] GPL MISC IP Proto 77 Sun ND
- [x] GPL MISC CVS non-relative path error response
- [ ] GPL MISC NNTP senduuname overflow attempt
- [ ] GPL MISC NNTP checkgroups overflow attempt
- [ ] GPL MISC NNTP sendme overflow attempt
- [ ] GPL MISC Nntp rmgroup overflow attempt
- [x] GPL MISC HP Web JetAdmin remote file upload attempt
- [x] GPL MISC HP Web JetAdmin file write attempt
- [ ] GPL MISC NNTP XPAT pattern overflow attempt
- [ ] GPL MISC squid WCCP I_SEE_YOU message overflow attempt
- [x] GPL MISC rsh echo + +
- [x] GPL MISC rsh root
- [ ] GPL MISC 0 ttl
- [x] GPL MISC UPnP malformed advertisement
- [ ] GPL MISC AUTHINFO USER overflow attempt
- [ ] GPL MISC return code buffer overflow attempt
- [ ] GPL MISC bootp hardware address length overflow
- [x] GPL MISC CVS invalid user authentication response
- [x] GPL MISC CVS double free exploit attempt response
- [x] GPL MISC CVS missing cvsroot response
- [ ] GPL MISC rsyncd overflow attempt
- [ ] GPL MISC BGP invalid type 0
- [ ] GPL MISC IP Proto 55 IP Mobility
- [ ] GPL MISC IP Proto 103 PIM
- [ ] GPL MISC NNTP sendsys overflow attempt
- [ ] GPL MISC NNTP version overflow attempt
- [ ] GPL MISC NNTP ihave overflow attempt
- [ ] GPL MISC NNTP newgroup overflow attempt
- [ ] GPL MISC NNTP article post without path attempt
- [x] GPL MISC HP Web JetAdmin setinfo access
- [ ] GPL MISC rsync backup-dir directory traversal attempt
- [ ] GPL MISC nntp SEARCH pattern overflow attempt

- [x] **emerging-mobile_malware.rules** Hide

- [ ] ET MOBILE_MALWARE Android Trojan Command and Control Communication
- [ ] ET MOBILE_MALWARE Android Trojan DroidDream Command and Control Communication
- [x] ET MOBILE_MALWARE Android Trojan Fake10086 checkin 2
- [ ] ET MOBILE_MALWARE SymbOS SuperFairy.D BackgroundUpdata.ini Missing File HTTP Request
- [ ] ET MOBILE_MALWARE SymbOS/Yxes.B/E CnC Checkin Request
- [ ] ET MOBILE_MALWARE SymbOS/Yxes CnC Checkin Request 2
- [ ] ET MOBILE_MALWARE Possible Mobile Malware POST of IMEI International Mobile Equipment Identity in URI
- [ ] ET MOBILE_MALWARE SymbOS/Yxes.I PropertyFile.jsp CnC Server Communication
- [ ] ET MOBILE_MALWARE SymbOS/Yxes.I NumberFile.jsp CnC Server Communication
- [ ] ET MOBILE_MALWARE SPR/MobileSpy Mobile Spyware Sending Geographic Location Logs To Remote Server
- [ ] ET MOBILE_MALWARE SPR/MobileSpy Mobile Spyware Sending SMS Logs to Remote Server
- [ ] ET MOBILE_MALWARE SymbOS.Sagasi.a Worm Sending Data to Server
- [ ] ET MOBILE_MALWARE SslCrypt Server Communication
- [ ] ET MOBILE_MALWARE SslCrypt Server Communication
- [x] ET MOBILE_MALWARE Android/Smspacem CnC Communication Attempt
- [ ] ET MOBILE_MALWARE DroidKungFu Checkin
- [ ] ET MOBILE_MALWARE DroidKungFu Checkin 2
- [ ] ET MOBILE_MALWARE DNS Query For Known Mobile Malware Control Server (waplove .cn)
- [ ] ET MOBILE_MALWARE DNS Query For Known Mobile Malware Control Server (searchwebmobile .com)
- [ ] ET MOBILE_MALWARE Android.Plankton/Tonclank Control Server Responding With JAR Download URL
- [x] ET MOBILE_MALWARE Android.HongTouTou Checkin
- [x] ET MOBILE_MALWARE Android.YzhcSms URL for Possible File Download
- [x] ET MOBILE_MALWARE XML Style POST Of IMSI International Mobile Subscriber Identity
- [ ] ET MOBILE_MALWARE SymbOS/Yxes Plugucsrv.sisx File Download
- [x] ET MOBILE_MALWARE Android Trojan MSO.PJApps checkin 2
- [ ] ET MOBILE_MALWARE Android Trojan Fake10086 checkin 1
- [ ] ET MOBILE_MALWARE SymbOS SuperFairy.D StartUpdata.ini Missing File HTTP Request
- [ ] ET MOBILE_MALWARE SymbOS SuperFairy.D active.txt Missing File HTTP Request
- [ ] ET MOBILE_MALWARE SymbOS/Yxes CnC Checkin Request
- [ ] ET MOBILE_MALWARE SymbOS/Yxes.F CnC Checkin Request 3
- [ ] ET MOBILE_MALWARE SymbOS.Flexispy.a Commercial Spying App Sending User Information to Server
- [ ] ET MOBILE_MALWARE SymbOS/Yxes.I TipFile.jsp CnC Server Communication
- [ ] ET MOBILE_MALWARE SymbOS/Merogo User Agent
- [ ] ET MOBILE_MALWARE SPR/MobileSpy Mobile Spyware Sending Call Logs to Remote Server
- [ ] ET MOBILE_MALWARE SymbOS.Sagasi.a Worm Sending Data to Server
- [ ] ET MOBILE_MALWARE SymbOS.Sagasi.a User Agent LARK/1.3.0
- [x] ET MOBILE_MALWARE SslCrypt Server Communication
- [ ] ET MOBILE_MALWARE SymbOS/SuperFairy.D Bookmarked Connection to Server
- [ ] ET MOBILE_MALWARE Iphone iKee.B Checkin
- [ ] ET MOBILE_MALWARE Possible Post of Infected Mobile Device Location Information
- [x] ET MOBILE_MALWARE DNS Query for gongfu-android.com DroidKungFu CnC Server
- [x] ET MOBILE_MALWARE Android.Tonclank JAR File Download
- [x] ET MOBILE_MALWARE Android.Plankton/Tonclank Successful Installation Device Information POST
- [ ] ET MOBILE_MALWARE DroidKungFu Checkin 3
- [x] ET MOBILE_MALWARE Android.YzhcSms CnC Keepalive Message
- [x] ET MOBILE_MALWARE XML Style POST Of IMEI International Mobile Equipment Identity
- [ ] ET MOBILE_MALWARE SymbOS/Yxes CnC Checkin Message
- [ ] ET MOBILE_MALWARE SymbOS/Yxes Jump.jsp CnC Checkin Message

- [ ] ET MOBILE_MALWARE SymbOS/Yxes KernelPara.jsp CnC Checkin Message
- [ ] ET MOBILE_MALWARE Android.CruseWin XML Configuration File Sent From CnC Server
- [x] ET MOBILE_MALWARE Android.Bgserv POST of Data to CnC Server
- [x] ET MOBILE_MALWARE Android/GoldDream Task Information Retrieval
- [ ] ET MOBILE_MALWARE SymbOS/CommDN Downloading Second Stage Malware Binary
- [ ] ET MOBILE_MALWARE SymbOS/SymGam Receiving SMS Message Template from CnC Server
- [x] ET MOBILE_MALWARE Android.AdSms Retrieving XML File from CnC Server
- [x] ET MOBILE_MALWARE Android.Zitmo Forwarding SMS Message to CnC Server
- [x] ET MOBILE_MALWARE Android/SndApp.B Sending Device Information
- [x] ET MOBILE_MALWARE Android/KungFu Package Delete Command
- [x] ET MOBILE_MALWARE Android/SndApps.SM Sending Information to CnC
- [ ] ET MOBILE_MALWARE iOS Keylogger iKeyMonitor access
- [x] ET MOBILE_MALWARE Android/CoolPaperLeak Sending Information To CnC
- [x] ET MOBILE_MALWARE Android TrojanFakeLookout.A
- [ ] ET MOBILE_MALWARE DroidKungFu Variant
- [x] ET MOBILE_MALWARE Android/Smsilence.A Sending SMS Messages CnC Beacon
- [x] ET MOBILE_MALWARE signed-unsigned integer mismatch code-verification bypass
- [x] ET MOBILE_MALWARE Android/Opfake.A GetTask CnC Beacon
- [x] ET MOBILE_MALWARE Possible Android InMobi SDK SideDoor Access takeCameraPicture
- [x] ET MOBILE_MALWARE Possible Android InMobi SDK SideDoor Access makeCall
- [x] ET MOBILE_MALWARE Possible Android InMobi SDK SideDoor Access sendMail
- [x] ET MOBILE_MALWARE Possible Android InMobi SDK SideDoor Access registerMicListener
- [x] ET MOBILE_MALWARE Android.KorBanker Successful Fake Banking App Install CnC Server Acknowledgement
- [x] ET MOBILE_MALWARE Android/HeHe.Spy RegisterRequest CnC Beacon
- [x] ET MOBILE_MALWARE Android/HeHe.Spy ReportRequest CnC Beacon
- [ ] ET MOBILE_MALWARE Android/HeHe.Spy ReportMessageRequest CnC Beacon
- [x] ET MOBILE_MALWARE Android/FakeKakao checkin 1
- [x] ET MOBILE_MALWARE Android/FakeKakao checkin 3
- [x] ET MOBILE_MALWARE AndroidOS/Lotoor.Q
- [x] ET MOBILE_MALWARE Andr/com.sdwiurse
- [x] ET MOBILE_MALWARE Android Spyware Dowgin Checkin
- [ ] ET MOBILE_MALWARE Android ScarePakage checkin 2
- [x] ET MOBILE_MALWARE Worm.AndroidOS.Selfmite.a Checkin
- [x] ET MOBILE_MALWARE Android/Spy.Kasandra.A Checkin
- [x] ET MOBILE_MALWARE Android/Locker.B Checkin 2
- [ ] ET MOBILE_MALWARE iOS/AppBuyer Checkin 1
- [ ] ET MOBILE_MALWARE Possible Android CVE-2014-6041
- [x] ET MOBILE_MALWARE iOS/Xsser Checkin
- [x] ET MOBILE_MALWARE iOS/Xsser sending files
- [x] ET MOBILE_MALWARE Android/Koler.C Checkin
- [ ] ET MOBILE_MALWARE CoolReaper CnC Beacon 1
- [x] ET MOBILE_MALWARE CoolReaper User-Agent
- [x] ET MOBILE_MALWARE Android/SMSThief.F Banker CnC Beacon
- [x] ET MOBILE_MALWARE IOS_XAGENT UA
- [x] ET MOBILE_MALWARE Possible Android CVE-2014-6041
- [ ] ET MOBILE_MALWARE Android.Trojan.SLocker.DZ Checkin
- [ ] ET MOBILE_MALWARE Android.CruseWin Retriving XML File from Hard Coded CnC
- [x] ET MOBILE_MALWARE Android.Walkinwat Sending Data to CnC Server
- [x] ET MOBILE_MALWARE Android/GoldDream Infected Device Registration
- [x] ET MOBILE_MALWARE Android/GoldDream Uploading Watch Files
- [ ] ET MOBILE_MALWARE SymbOS/SymGam CnC Checkin
- [x] ET MOBILE_MALWARE Android/HippoSms Method Request to CnC
- [ ] ET MOBILE_MALWARE Android.AdSms XML File From CnC Server
- [x] ET MOBILE_MALWARE Android/Netisend.A Posting Information to CnC
- [x] ET MOBILE_MALWARE Android/Ozotshielder.A Checkin
- [x] ET MOBILE_MALWARE Android/FakeTimer.A Reporting to CnC
- [x] ET MOBILE_MALWARE Android/Plankton.P Commands Request to CnC Server
- [x] ET MOBILE_MALWARE Android/Updtkiller Sending Device Information
- [ ] ET MOBILE_MALWARE Android/Ksapp.A Checkin
- [ ] ET MOBILE_MALWARE Android/Fakelash.A!tr.spy Checkin
- [x] ET MOBILE_MALWARE Android/Smsilence.A Successful Install Report
- [x] ET MOBILE_MALWARE DNS Query Targeted Tibetan Android Malware C2 Domain
- [x] ET MOBILE_MALWARE Android/FakeAhnAV.A CnC Beacon
- [x] ET MOBILE_MALWARE Android/Opfake.A Country CnC Beacon
- [x] ET MOBILE_MALWARE Possible Android InMobi SDK SideDoor Access getGalleryImage
- [x] ET MOBILE_MALWARE Possible Android InMobi SDK SideDoor Access postToSocial
- [x] ET MOBILE_MALWARE Possible Android InMobi SDK SideDoor Access sendSMS
- [x] ET MOBILE_MALWARE Android.KorBanker Fake Banking App Install CnC Beacon
- [ ] ET MOBILE_MALWARE Android/HeHe.Spy getLastVersion CnC Beacon
- [x] ET MOBILE_MALWARE Android/HeHe.Spy LoginRequest CnC Beacon
- [x] ET MOBILE_MALWARE Android/HeHe.Spy GetTaskRequest CnC Beacon
- [x] ET MOBILE_MALWARE Android/DwnlAPK-A Configuration File Request
- [x] ET MOBILE_MALWARE Android/FakeKakao checkin 2
- [x] ET MOBILE_MALWARE SMSSend Fake flappy bird APK
- [ ] ET MOBILE_MALWARE Android.Adware.Wapsx.A
- [x] ET MOBILE_MALWARE Android/Comll.Banker RAT CnC Beacon
- [ ] ET MOBILE_MALWARE Android ScarePakage checkin
- [ ] ET MOBILE_MALWARE AndroidOS.Simplocker Checkin
- [ ] ET MOBILE_MALWARE Android/Trogle.A Possible Exfiltration of SMS via SMTP
- [x] ET MOBILE_MALWARE Android/Locker.B Checkin 1
- [ ] ET MOBILE_MALWARE Android/Youmi.Adware Install Report CnC Beacon
- [ ] ET MOBILE_MALWARE iOS/AppBuyer Checkin 2
- [x] ET MOBILE_MALWARE Android/Code4hk.A Checkin
- [x] ET MOBILE_MALWARE iOS/Xsser sending GPS info
- [x] ET MOBILE_MALWARE iOS/Xsser checking library version
- [x] ET MOBILE_MALWARE Android.Stealthgenie Checkin
- [x] ET MOBILE_MALWARE CoolReaper CnC Beacon 2
- [x] ET MOBILE_MALWARE Android Syria-Twitter Checkin
- [x] ET MOBILE_MALWARE Operation Pawn Storm IOS_XAGENT Checkin
- [x] ET MOBILE_MALWARE Possible Android CVE-2014-6041
- [x] ET MOBILE_MALWARE Android.Trojan.SMSSend.Y
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Wroba.m Checkin

- [x] ET MOBILE_MALWARE Android BatteryBotPro Checkin
- [x] ET MOBILE_MALWARE Android BatteryBotPro Checkin 2
- [ ] ET MOBILE_MALWARE Android Gunpoder Checkin
- [x] ET MOBILE_MALWARE DNS Android/Spy.Feabme.A Query
- [ ] ET MOBILE_MALWARE Android.Trojan.SLocker.DZ Checkin 2
- [ ] ET MOBILE_MALWARE Trojan.iPhoneOS.KeyRaider Checkin
- [ ] ET MOBILE_MALWARE Trojan.iPhoneOS.KeyRaider Checkin 2
- [ ] ET MOBILE_MALWARE YiSpecter Activity M1
- [ ] ET MOBILE_MALWARE YiSpecter Activity M2
- [x] ET MOBILE_MALWARE Android/Kemoge DNS Lookup
- [x] ET MOBILE_MALWARE Android/Kemoge Checkin
- [x] ET MOBILE_MALWARE Android/Kemoge Checkin 2
- [x] ET MOBILE_MALWARE Android Trojan Cloudsota HTTP Host
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Acecard.c Checkin
- [x] ET MOBILE_MALWARE Android/TrojanDropper.Agent.EP HTTP Host
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.SmForw/SlemBunk/SLocker Checkin
- [x] ET MOBILE_MALWARE Android/SlemBunk.Banker Phished Credentials Upload
- [ ] ET MOBILE_MALWARE Android/Fakeinst.KD .onion Proxy Domain
- [ ] ET MOBILE_MALWARE Backdoor.AndroidOS.Torec.a .onion Proxy Domain
- [ ] ET MOBILE_MALWARE Backdoor.AndroidOS.Torec.a .onion Proxy Domain 2
- [x] ET MOBILE_MALWARE DNS Trojan-Banker.AndroidOS.Marcher.i Query
- [x] ET MOBILE_MALWARE iOS DualToy Checkin
- [x] ET MOBILE_MALWARE AndroRAT Bitter DNS Lookup (info2t .com)
- [x] ET MOBILE_MALWARE Adware.Adwo.A
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Marcher Sending Credit Card Info
- [x] ET MOBILE_MALWARE Possible iOS WebView Auto Dialer 1
- [x] ET MOBILE_MALWARE Possible iOS WebView Auto Dialer 2
- [x] ET MOBILE_MALWARE Android.Trojan.HiddenApp.OU Checkin
- [ ] ET MOBILE_MALWARE Android.Trojan.HiddenApp.OU Checkin 2
- [ ] ET MOBILE_MALWARE Android.Trojan.HiddenApp.OU SSL CnC Cert
- [x] ET MOBILE_MALWARE Unknown Redirector Nov 17 2016
- [ ] ET MOBILE_MALWARE Unknown Landing URI Nov 17 2016
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Marcher.a Checkin
- [x] ET MOBILE_MALWARE Android Fancy Bear Checkin
- [x] ET MOBILE_MALWARE Android Fancy Bear Checkin 2
- [x] ET MOBILE_MALWARE Android Fancy Bear Checkin 3
- [x] ET MOBILE_MALWARE Android Fancy Bear Checkin 4
- [x] ET MOBILE_MALWARE Android Fancy Bear Checkin 5
- [x] ET MOBILE_MALWARE Android Fancy Bear Checkin 6
- [ ] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Marcher SSL CnC Cert
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Marcher DNS Lookup
- [ ] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Marcher DNS Lookup
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Femas.b CnC Beacon
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Femas.b Apps List Exfil
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Femas.b DNS Lookup
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Femas.b DNS Lookup
- [ ] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Femas.b DNS Lookup
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Femas.b DNS Lookup
- [x] ET MOBILE_MALWARE Android.C2P.Qd!c Ransomware CnC Beacon
- [ ] ET MOBILE_MALWARE Android Trojan Pegasus CnC Beacon
- [ ] ET MOBILE_MALWARE Android Trojan Pegasus CnC Beacon M2
- [x] ET MOBILE_MALWARE AdWare.AndroidOS.Ewind.cd Checkin
- [x] ET MOBILE_MALWARE AdWare.AndroidOS.Ewind.cd Response
- [x] ET MOBILE_MALWARE Android.Dropper.Abd Checkin
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Marcher.a CnC Beacon
- [x] ET MOBILE_MALWARE ANDROIDOS_LEAKERLOCKER.HRX DNS Lookup
- [x] ET MOBILE_MALWARE WireX Botnet DNS Lookup
- [x] ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup
- [x] ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 2
- [x] ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 3
- [x] ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 4
- [x] ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 5
- [x] ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 6
- [x] ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 7
- [x] ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 8
- [x] ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 9
- [x] ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 10
- [x] ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 11
- [x] ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 12
- [x] ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 13
- [x] ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 14
- [x] ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 15
- [x] ET MOBILE_MALWARE Android/Bankbot.HH!tr DNS Lookup 16
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.RedAlert CnC Beacon
- [x] ET MOBILE_MALWARE Android JadeRAT CnC Beacon
- [ ] ET MOBILE_MALWARE Android JadeRAT CnC Beacon 2
- [x] ET MOBILE_MALWARE Android Marcher Trojan Download - Raiffeisen Bank Targeting (set)
- [x] ET MOBILE_MALWARE Android Marcher Trojan Download - Sparkasse Bank Targeting (set)
- [x] ET MOBILE_MALWARE Android Marcher Trojan Download - BankAustria Targeting (set)
- [x] ET MOBILE_MALWARE Android Marcher Trojan Download - Austrian Bank Targeting
- [x] ET MOBILE_MALWARE Android/TrojanDropper.Agent.BKY DNS Lookup 1
- [x] ET MOBILE_MALWARE Android/TrojanDropper.Agent.BKY DNS Lookup 2
- [x] ET MOBILE_MALWARE Android/TrojanDropper.Agent.BKY DNS Lookup 3
- [x] ET MOBILE_MALWARE Android/TrojanDropper.Agent.BKY DNS Lookup 4
- [x] ET MOBILE_MALWARE Android.Trojan.Marcher.U DNS Lookup
- [x] ET MOBILE_MALWARE Android/Spy.Agent.AON / Glancelove DNS Lookup 1 (goldncup .com)
- [x] ET MOBILE_MALWARE Android/Spy.Agent.AON / Glancelove DNS Lookup 2 (glancelove .com)
- [x] ET MOBILE_MALWARE Android/Spy.Agent.AON / Glancelove DNS Lookup 3 (autoandroidup .website)
- [x] ET MOBILE_MALWARE Android/Spy.Agent.AON / Glancelove DNS Lookup 4 (mobilestoreupdate .website)
- [x] ET MOBILE_MALWARE Android/Spy.Agent.AON / Glancelove DNS Lookup 5 (updatemobapp .website)
- [x] ET MOBILE_MALWARE iOS/Bahamut DNS Lookup
- [x] ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 2
- [x] ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 3
- [x] ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 4
- [x] ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 5
- [x] ET MOBILE_MALWARE Android Golden Rat Checkin
- [x] ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 6
- [x] ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 7
- [x] ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 8
- [x] ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 9
- [x] ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 10
- [x] ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 11
- [x] ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 12
- [x] ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 13
- [x] ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 14

- [x] ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 15
- [x] ET MOBILE_MALWARE iOS/Bahamut DNS Lookup 16
- [x] ET MOBILE_MALWARE NSO Related Domain 1
- [x] ET MOBILE_MALWARE NSO Related Domain 2
- [x] ET MOBILE_MALWARE NSO Related Domain 3
- [x] ET MOBILE_MALWARE NSO Related Domain 4
- [x] ET MOBILE_MALWARE NSO Related Domain 5
- [x] ET MOBILE_MALWARE NSO Related Domain 6
- [x] ET MOBILE_MALWARE NSO Related Domain 7
- [x] ET MOBILE_MALWARE NSO Related Domain 8
- [x] ET MOBILE_MALWARE NSO Related Domain 9
- [x] ET MOBILE_MALWARE NSO Related Domain 10
- [x] ET MOBILE_MALWARE NSO Related Domain 11
- [x] ET MOBILE_MALWARE NSO Related Domain 12
- [x] ET MOBILE_MALWARE NSO Related Domain 13
- [x] ET MOBILE_MALWARE NSO Related Domain 14
- [x] ET MOBILE_MALWARE NSO Related Domain 15
- [x] ET MOBILE_MALWARE NSO Related Domain 16
- [x] ET MOBILE_MALWARE NSO Related Domain 17
- [x] ET MOBILE_MALWARE NSO Related Domain 18
- [x] ET MOBILE_MALWARE NSO Related Domain 19
- [x] ET MOBILE_MALWARE NSO Related Domain 20
- [x] ET MOBILE_MALWARE NSO Related Domain 21
- [x] ET MOBILE_MALWARE NSO Related Domain 22
- [x] ET MOBILE_MALWARE NSO Related Domain 24
- [x] ET MOBILE_MALWARE NSO Related Domain 25
- [x] ET MOBILE_MALWARE NSO Related Domain 26
- [x] ET MOBILE_MALWARE NSO Related Domain 27
- [x] ET MOBILE_MALWARE NSO Related Domain 28
- [x] ET MOBILE_MALWARE NSO Related Domain 29
- [x] ET MOBILE_MALWARE NSO Related Domain 30
- [x] ET MOBILE_MALWARE NSO Related Domain 31
- [x] ET MOBILE_MALWARE NSO Related Domain 32
- [x] ET MOBILE_MALWARE NSO Related Domain 33
- [x] ET MOBILE_MALWARE NSO Related Domain 34
- [x] ET MOBILE_MALWARE NSO Related Domain 35
- [x] ET MOBILE_MALWARE NSO Related Domain 36
- [x] ET MOBILE_MALWARE NSO Related Domain 37
- [x] ET MOBILE_MALWARE NSO Related Domain 38
- [x] ET MOBILE_MALWARE NSO Related Domain 39
- [x] ET MOBILE_MALWARE NSO Related Domain 40
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.CrazyMango.a Checkin
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.CrazyMango.a CnC Beacon
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.CrazyMango.a Checkin 2
- [x] ET MOBILE_MALWARE [PTsecurity] Spyware.BondPath (PathCall/ Dingwe) Check-in
- [x] ET MOBILE_MALWARE Android APT-C-23 (1jve .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (1jve .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (clarke-taylor .life in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (clarke-taylor .life in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (hcttmail .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (hcttmail .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (mail-presidency .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (mail-presidency .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (aamir-khan .site in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (aamir-khan .site in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (daario-naharis .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (daario-naharis .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (help-live .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (help-live .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (margaery-tyrell .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (margaery-tyrell .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (accaunts-googlc .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (accaunts-googlc .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (dachfunny .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (dachfunny .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (help-sec .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (help-sec .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (maria-bouchard .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (maria-bouchard .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (account-gocgle .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (account-gocgle .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (dachfunny .us in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (dachfunny .us in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (heyapp .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (heyapp .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (marklavi .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (marklavi .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (account-googlc .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (account-googlc .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (dardash .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (dardash .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (hitmesanjjoy .pro in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (hitmesanjjoy .pro in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (mary-crawley .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (mary-crawley .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (accountforuser .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (accountforuser .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (dardash .fun in DNS Lookup)

- [x] ET MOBILE_MALWARE Android APT-C-23 (dardash .fun in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (hoopoechat .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (masuka .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (accountforusers .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (dardash .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (hotimael .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (matthew-stevens .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (accounts-gocgle .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (dardash .live in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (hotmailme .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (mauricefischer .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (accounts-googlc .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (david-mclean .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (italk-chat .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (max-eleanor .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (accountusers .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (david-moris .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (italk-chat .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (max-mayfield .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (accuant-googlc .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (davina-claire .xyz in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (jack-wagner .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (maxlight .us in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (activedardash .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (davos-seaworth .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (james-charles .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (mediauploader .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (alain .ps in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (debra-morgan .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (jimmykudo .online in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (meet-me .chat in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (alisonparker .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (donna-paulsen .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (android-settings .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (hoopoechat .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (masuka .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (accountforusers .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (dardash .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (hotimael .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (matthew-stevens .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (accounts-gocgle .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (dardash .live in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (hotmailme .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (mauricefischer .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (accounts-googlc .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (david-mclean .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (italk-chat .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (max-eleanor .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (accountusers .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (david-moris .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (italk-chat .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (max-mayfield .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (accuant-googlc .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (davina-claire .xyz in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (jack-wagner .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (maxlight .us in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (activedardash .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (davos-seaworth .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (james-charles .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (mediauploader .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (alain .ps in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (debra-morgan .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (jimmykudo .online in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (meet-me .chat in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (alisonparker .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (donna-paulsen .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (android-settings .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (easyshow .fun in DNS Lookup)

- [x] ET MOBILE_MALWARE Android APT-C-23 (easyshow .fun in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (jon-snow .pro in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (men-ana .fun in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (apkapps .pro in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (eleanor-guthrie .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (jorah-mormont .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (michael-keaton .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (apkapps .site in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (eleanorguthrie .site in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (joycebyers .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (miranda-barlow .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (appchecker .us in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (engin-altan .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (juana .fun in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (miwakosato .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (appuree .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (esofiezo .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (kaniel-outis .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (mofa-help .site in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (arthursaito .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (everyservices .space in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (karenwheeler .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (moneymotion .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (aryastark .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (exvsnomy .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (kate-austen .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (myboon .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (aslaug-sigurd .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (ezofiezo .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (katesacker .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (mygift .site in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (assets-acc .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (face-book-support .email in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (katie .party in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (mygift .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (jon-snow .pro in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (men-ana .fun in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (apkapps .pro in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (eleanor-guthrie .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (jorah-mormont .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (michael-keaton .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (apkapps .site in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (eleanorguthrie .site in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (joycebyers .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (miranda-barlow .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (appchecker .us in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (engin-altan .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (juana .fun in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (miwakosato .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (appuree .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (esofiezo .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (kaniel-outis .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (mofa-help .site in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (arthursaito .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (everyservices .space in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (karenwheeler .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (moneymotion .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (aryastark .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (exvsnomy .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (kate-austen .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (myboon .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (aslaug-sigurd .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (ezofiezo .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (katesacker .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (mygift .site in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (assets-acc .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (face-book-support .email in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (katie .party in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (mygift .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (bbc-learning .com in DNS Lookup)

- [x] ET MOBILE_MALWARE Android APT-C-23 (bbc-learning .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (fasebcck .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (kik-com .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (namybotter .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (bellamy-bob .life in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (fasebock .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (kristy-milligan .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (namyyeatop .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (bestbitloly .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (fasebook .cam in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (lagertha-lothbrok .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (natemunson .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (billy-bones .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (fasebookvideo .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (leonard-kim .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (new .filetea .me in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (bitgames .world in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (fatehmedia .site in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (leslie-barnes .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (nightchat .fun in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (black-honey .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (firesky .site in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (lets-see .site in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (nightchat .live in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (bob-turco .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (flirtymania .fun in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (lexi-branson .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (nissour-beton .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (buymicrosft .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (freya .miranda-barlow .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (lincoln-blake .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (octavia-blake .world in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (camilleoconnell .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (geny-wise .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (fasebcck .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (kik-com .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (namybotter .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (bellamy-bob .life in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (fasebock .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (kristy-milligan .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (namyyeatop .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (bestbitloly .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (fasebook .cam in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (lagertha-lothbrok .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (natemunson .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (billy-bones .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (fasebookvideo .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (leonard-kim .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (new .filetea .me in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (bitgames .world in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (fatehmedia .site in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (leslie-barnes .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (nightchat .fun in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (black-honey .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (firesky .site in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (lets-see .site in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (nightchat .live in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (bob-turco .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (flirtymania .fun in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (lexi-branson .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (nissour-beton .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (buymicrosft .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (freya .miranda-barlow .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (lincoln-blake .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (octavia-blake .world in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (camilleoconnell .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (geny-wise .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (lindamullins .info in DNS Lookup)

- [x] ET MOBILE_MALWARE Android APT-C-23 (lindamullins .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (olivia-hartman .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (caroline-nina .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (gmailservice .us in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (liz-keen .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (oriential .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (cassy-gray .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (graceygretchen .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (login-yohoo .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (ososezo .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (cecilia-dobrev .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (hareyupnow .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (lord-varys .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (ososezo .site in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (cecilia-gilbert .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (harper-monty .site in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (lyanna-stark .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (parrotchat .co in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (cerseilannister .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (harrykane .online in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (mail-accout .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (pmi-pna .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (chat-often .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (harvey-ross .info in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (mail-goog1e .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (pml-help .site in TLS SNI)
- [x] ET MOBILE_MALWARE Android APT-C-23 (christopher .fun in TLS SNI)
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (areadozemode .space in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (twethujsnu .cc in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (taiprotectsq .xyz in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (projectpredator .space in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (aserogeege .space in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (dingpsounda .space in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (privateanbshouse .space in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (olivia-hartman .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (caroline-nina .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (gmailservice .us in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (liz-keen .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (oriential .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (cassy-gray .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (graceygretchen .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (login-yohoo .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (ososezo .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (cecilia-dobrev .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (hareyupnow .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (lord-varys .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (ososezo .site in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (cecilia-gilbert .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (harper-monty .site in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (lyanna-stark .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (parrotchat .co in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (cerseilannister .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (harrykane .online in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (mail-accout .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (pmi-pna .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (chat-often .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (harvey-ross .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (mail-goog1e .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (pml-help .site in DNS Lookup)
- [x] ET MOBILE_MALWARE Android APT-C-23 (christopher .fun in DNS Lookup)
- [x] ET MOBILE_MALWARE Android/GPlayed (sub1 .tdsworker .ru in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (selectnew25mode .space in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (project2anub .xyz in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (uwannaplaygame .space in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (nihaobrazzzahit .top in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (hdfuckedin18 .top in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (wantddantiprot .space in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (seconddoxed .space in DNS Lookup)

- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (firstdoxed .space in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (oauth3 .html5100 .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (dosandiq .space in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (protect4juls .space in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (wijariief .space in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.d (scradm .in in DNS Lookup)
- [x] ET MOBILE_MALWARE Android/Xnore Fake Facebook Login Credentials Collected
- [x] ET MOBILE_MALWARE Android/BasBanke CnC Checkin
- [x] ET MOBILE_MALWARE Observed Malicious SSL Cert (DonotGroup Android CnC)
- [x] ET MOBILE_MALWARE Windows Phone PUA.Redpher (myservicessapps .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android/Spy.Agent.ANA (androidsmedia .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android/Spy.Agent.ANA (androidssystem .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android/Spy.Agent.ANA (secandroid .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android/Spy.Agent.ANA (mediadownload .space in DNS Lookup)
- [x] ET MOBILE_MALWARE Android/Spy.Agent.ANA (mediamobilereg .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android/Spy.Agent.ANA (sharpion .org in DNS Lookup)
- [x] ET MOBILE_MALWARE Android/Spy.Agent.ANA (shileyfetwell .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan.AndroidOS.TimpDoor Module Download Request
- [x] ET MOBILE_MALWARE Trojan.AndroidOS.TimpDoor (purple .itraffic .click in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan.AndroidOS.TimpDoor (purple .m-ads .net in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan.AndroidOS.TimpDoor (drproxy .pro in DNS Lookup)
- [x] ET MOBILE_MALWARE Android/Spy.Agent.AOX Checkin
- [x] ET MOBILE_MALWARE Apple iPhone Implant - Boundary Observed
- [x] ET MOBILE_MALWARE Apple iPhone Implant - Upload Files
- [x] ET MOBILE_MALWARE Apple iPhone Implant - Command Executed
- [x] ET MOBILE_MALWARE Evil Eye Android Malware Beacon
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Joker Checkin
- [x] ET MOBILE_MALWARE MOONSHINE payload C2 activity
- [x] ET MOBILE_MALWARE Android/Geost CnC Checkin
- [ ] ET MOBILE_MALWARE Suspected SandCat Related CnC
- [x] ET MOBILE_MALWARE Suspected Android Youzicheng Proxy Activity
- [ ] ET MOBILE_MALWARE Android Lightspy Implant CnC
- [x] ET MOBILE_MALWARE Android/TrojanDropper.Agent.EQO Variant CnC Activity
- [x] ET MOBILE_MALWARE Android Trojan MSO.PJApps checkin 1
- [x] ET MOBILE_MALWARE Android PHONEMONITOR RAT CnC (getsettings)
- [x] ET MOBILE_MALWARE Suspected PROJECTSPY CnC (video)
- [x] ET MOBILE_MALWARE Suspected PROJECTSPY Cookie
- [x] ET MOBILE_MALWARE NSO Group CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE NSO Group CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE NSO Group CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE PHANTOMLANCE CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE PHANTOMLANCE CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE SSL/TLS Certificate Observed (Betcity CnC)
- [x] ET MOBILE_MALWARE Android/xDrop Ransomware CnC Checkin
- [x] ET MOBILE_MALWARE Android Malvertising Communication
- [ ] ET MOBILE_MALWARE ActionSpy CnC (POST)
- [x] ET MOBILE_MALWARE NSO Group Domain in DNS Lookup (urlpush .net)
- [x] ET MOBILE_MALWARE NSO Group Domain in DNS Lookup (free247downloads .com)
- [x] ET MOBILE_MALWARE NSO Group CnC Domain in DNS Lookup (chretiendaujoudhui .com)
- [x] ET MOBILE_MALWARE NSO Group CnC Domain in DNS Lookup (leprotestant .com)
- [x] ET MOBILE_MALWARE NSO Group CnC Domain in DNS Lookup (vie-en-islam .com)
- [x] ET MOBILE_MALWARE NSO Group CnC Domain in DNS Lookup (viedechretien .org)
- [x] ET MOBILE_MALWARE Backdoor.AndroidOS.Ahmyth.f (DNS Lookup)
- [x] ET MOBILE_MALWARE Android Joker CnC Configuration Retrieval
- [x] ET MOBILE_MALWARE TransparentTribe AhMyth RAT Variant Activity (POST)
- [x] ET MOBILE_MALWARE Android.Trojan.Rana.A (wherisdomaintv .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android.Trojan.Rana.A (whoisdomainpc .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android.Trojan.Rana.A (fullplayersoftware .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android.Trojan.Rana.A (softwareplayertop .com in DNS Lookup)
- [ ] ET MOBILE_MALWARE Observed NSO Group CnC Domain in TLS SNI (img565vv6 .holdmydoor .com)
- [ ] ET MOBILE_MALWARE Observed NSO Group CnC Domain in TLS SNI (crashparadox .net)
- [ ] ET MOBILE_MALWARE Observed NSO Group CnC Domain in TLS SNI (f15fwd322 .regularhours .net)
- [x] ET MOBILE_MALWARE Observed NSO Group CnC Domain in TLS SNI (bananakick .net)
- [x] ET MOBILE_MALWARE Observed NSO Group CnC Domain in TLS SNI (stilloak .net)
- [x] ET MOBILE_MALWARE Observed NSO Group CnC Domain in TLS SNI (flowersarrows .com)
- [x] ET MOBILE_MALWARE Android Flubot / LIKEACHARM Stealer Exfil (POST)
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Hawkshaw.a (bald-panel .firebaseio .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Hawkshaw.a (hawkshaw-cae48 .firebaseio .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Hawkshaw.a (spitfirepanel .firebaseio .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Hawkshaw.a (phoenix-panel .firebaseio .com in DNS Lookup)
- [x] ET MOBILE_MALWARE ITW Android Post-Exploit Downloader CnC Activity
- [x] ET MOBILE_MALWARE Android GolfSpy (services4me .net in TLS SNI)
- [x] ET MOBILE_MALWARE Possible Phenakite User-Agent
- [x] ET MOBILE_MALWARE Phenakite Audio Upload CnC
- [x] ET MOBILE_MALWARE Phenakite Image Upload CnC activity
- [x] ET MOBILE_MALWARE Arid Viper (dash-chat-c02b3 .firebaseio .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (dash-chat-c02b3 .appspot .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (hidden-chat-e58d7 .firebaseio .com in DNS Lookup)

- [x] ET MOBILE_MALWARE Arid Viper (hidden-chat-e58d7 .appspot .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (calculator-1e016 .appspot .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (samehnew-10a7c .appspot .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (play-store-51182 .appspot .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (stand-by-97c5c .appspot .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (es-last-telegram .appspot .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (fasibauik .co in DNS Lookup)
- [ ] ET MOBILE_MALWARE Arid Viper (fasebcck .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (fasebcak .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (fasebaak .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (fasebaook .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (log-yoahao .co in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (kevin-good .top in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (anna-sanchez .online in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (jennifer-marler .pw in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (stacks-zadar .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (richardbeman .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (moggfelicio .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (kentporter .site in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (lordblackwood .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (tim-jordan .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android Flubot / LIKEACHARM Stealer Exfil (POST) 2
- [x] ET MOBILE_MALWARE Kimsuky AppleSeed CnC Checkin
- [x] ET MOBILE_MALWARE PJobRat CnC Checkin
- [x] ET MOBILE_MALWARE NSO Pegasus iOS CnC Domain in DNS Lookup (opposedarrangement .net)
- [x] ET MOBILE_MALWARE NSO Pegasus iOS Megalodon Gatekeeper Activity (GET)
- [x] ET MOBILE_MALWARE Observed Malicious SSL Cert (Android/FakeAdBlocker CnC)
- [x] ET MOBILE_MALWARE Observed Malicious SSL Cert (Android/FakeAdBlocker CnC)
- [x] ET MOBILE_MALWARE Observed Malicious SSL Cert (Android/FakeAdBlocker CnC)
- [x] ET MOBILE_MALWARE Observed Malicious SSL Cert (Android/FakeAdBlocker CnC)
- [x] ET MOBILE_MALWARE Observed Malicious SSL Cert (Android/FakeAdBlocker CnC)
- [x] ET MOBILE_MALWARE Observed Oscorp/UBEL CnC Domain (quantumbots .xyz in TLS SNI)
- [x] ET MOBILE_MALWARE Observed Oscorp/UBEL CnC Domain (montanatony .xyz in TLS SNI)
- [x] ET MOBILE_MALWARE Observed Oscorp/UBEL CnC Domain (omegabots .xyz in TLS SNI)
- [x] ET MOBILE_MALWARE Observed Oscorp/UBEL CnC Domain (callbinary .xyz in TLS SNI)
- [x] ET MOBILE_MALWARE APT33/Charming Kitten Android/LittleLooter Activity (POST)
- [x] ET MOBILE_MALWARE APT33/Charming Kitten Android/LittleLooter Activity (POST) M3
- [x] ET MOBILE_MALWARE Android Vultr Checkin
- [x] ET MOBILE_MALWARE Android/SOVA Banking Trojan Activity (bot update)
- [x] ET MOBILE_MALWARE Android/SOVA Banking Trojan Activity (session cookie delete)
- [x] ET MOBILE_MALWARE Android/SOVA Banking Trojan Activity (log post)
- [x] ET MOBILE_MALWARE Arid Viper (calculator-1e016 .firebaseio .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (samehnew-10a7c .firebaseio .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (play-store-51182 .firebaseio .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (stand-by-97c5c .firebaseio .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (es-last-telegram .firebaseio .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (margarita-smith .host in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (fasebcak .co in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (fasebcoki .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (fasbcaok .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (fasebaok .co in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (fasebaok .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (log-yoheo .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (marty-colvard .top in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (wendy-johnston .pw in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (goerge-amper .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (joe-rumley .pw in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (vickeryduncan .site in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (stevensmalley .pro in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (chad-jessie .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (julie-parker .top in DNS Lookup)
- [x] ET MOBILE_MALWARE Arid Viper (hannah-parsons .info in DNS Lookup)
- [x] ET MOBILE_MALWARE Android Flubot / LIKEACHARM Stealer Exfil (POST) 3
- [x] ET MOBILE_MALWARE PJobRat System Exfil to CnC
- [x] ET MOBILE_MALWARE NSO Pegasus iOS Activity (GET)
- [x] ET MOBILE_MALWARE NSO Pegasus iOS Megalodon Activity (GET)
- [x] ET MOBILE_MALWARE Observed Malicious SSL Cert (Android/FakeAdBlocker CnC)
- [x] ET MOBILE_MALWARE Observed Malicious SSL Cert (Android/FakeAdBlocker CnC)
- [x] ET MOBILE_MALWARE Observed Malicious SSL Cert (Android/FakeAdBlocker CnC)
- [x] ET MOBILE_MALWARE Observed Malicious SSL Cert (Android/FakeAdBlocker CnC)
- [x] ET MOBILE_MALWARE Observed Malicious SSL Cert (Android/FakeAdBlocker CnC)
- [x] ET MOBILE_MALWARE Observed Oscorp/UBEL CnC Domain (marcobrando .xyz in TLS SNI)
- [x] ET MOBILE_MALWARE Observed Oscorp/UBEL CnC Domain (smoothcbots .xyz in TLS SNI)
- [x] ET MOBILE_MALWARE Observed Oscorp/UBEL CnC Domain (gogleadser .xyz in TLS SNI)
- [x] ET MOBILE_MALWARE Oscorp/UBEL Activity
- [x] ET MOBILE_MALWARE APT33/Charming Kitten Android/LittleLooter Activity (POST) M2
- [ ] ET MOBILE_MALWARE APT33/Charming Kitten Android/LittleLooter Activity (POST) M4
- [x] ET MOBILE_MALWARE Android/FlyTrap Activity (POST)
- [x] ET MOBILE_MALWARE Android/SOVA Banking Trojan Activity (number update)
- [x] ET MOBILE_MALWARE Android/SOVA Banking Trojan Activity (bot registration)
- [x] ET MOBILE_MALWARE Android/Spy.Agent.BEH Variant Activity (POST)

- [x] ET MOBILE_MALWARE Observed APT-C-23 Related Domain (linda-gaytan .website in TLS SNI)
- [x] ET MOBILE_MALWARE APT-C-23 Related CnC Domain in DNS Lookup (javan-demsky .website)
- [x] ET MOBILE_MALWARE Kimsuky AppleSeed CnC Checkin M2
- [x] ET MOBILE_MALWARE Possible Trojan-Banker.AndroidOS.Sharkbot Activity (DNS Lookup) 2
- [x] ET MOBILE_MALWARE Android Brunhilda Dropper (protectionguardapp .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android Brunhilda Dropper (readyqrscanner .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android Brunhilda Dropper (flowdivison .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android Brunhilda Dropper (multifuctionscanner .club in DNS Lookup)
- [x] ET MOBILE_MALWARE Android Brunhilda Dropper (multifuctionscanner .club in TLS SNI)
- [ ] ET MOBILE_MALWARE Coper Banking Trojan Related Domain in DNS Lookup
- [x] ET MOBILE_MALWARE AndroidOS/Basbanke.A Activity (POST)
- [x] ET MOBILE_MALWARE Android.BankBot.11270 (TLS SNI)
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.t (DNS Lookup)
- [x] ET MOBILE_MALWARE Android/SharkBot Related Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup) 2
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup) 3
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup) 4
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup) 5
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup) 6
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup) 7
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup) 8
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup) 9
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup) 10
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup) 11
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (DNS Lookup) 12
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI)
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 3
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 5
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 7
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 9
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 11
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 20
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 14
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 16
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 18
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 21
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 23
- [x] ET MOBILE_MALWARE Android Spy APT-C-23 (frances-thomas .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android Spy APT-C-23 (scott-chapin .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android Spy APT-C-23 (linda-gaytan .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android Spy APT-C-23 (david-gardiner .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android Spy APT-C-23 (amanda-hart .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Android Spy APT-C-23 (javan-demsky .website in DNS Lookup)
- [x] ET MOBILE_MALWARE Observed Android ExobotCompact.D/Octo Domain (ifn1h8ag1g .com in TLS SNI)
- [x] ET MOBILE_MALWARE Observed Android ExobotCompact.D/Octo Domain (equisdeperson .space in TLS SNI)
- [x] ET MOBILE_MALWARE APT-C-23 Related CnC Domain in DNS Lookup (linda-gaytan .website)
- [ ] ET MOBILE_MALWARE Gamaredon/Armageddon Related Domain in DNS Lookup (google-play .serveftp .com)
- [x] ET MOBILE_MALWARE Possible Trojan-Banker.AndroidOS.Sharkbot Activity (DNS Lookup)
- [x] ET MOBILE_MALWARE Trojan-Dropper.AndroidOS.Anatsa Checkin
- [x] ET MOBILE_MALWARE Android Brunhilda Dropper (protectionguardapp .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android Brunhilda Dropper (readyqrscanner .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android Brunhilda Dropper (flowdivison .club in TLS SNI)
- [x] ET MOBILE_MALWARE Android Gymdrop Dropper (onlinefitnessanalysis .com in DNS Lookup)
- [x] ET MOBILE_MALWARE Android Gymdrop Dropper (onlinefitnessanalysis .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android/FluBot Trojan Sending Information (POST)
- [x] ET MOBILE_MALWARE Android.BankBot.11270 (DNS Lookup)
- [x] ET MOBILE_MALWARE Android/TrojanDropper.Agent.GWO Checkin
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Anubis.t (TLS SNI)
- [x] ET MOBILE_MALWARE Android.Trojan.AndroRAT.CE Checkin
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI)
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI) 2
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI) 3
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI) 4
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI) 5
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI) 6
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI) 7
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI) 8
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI) 9
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI) 10
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI) 11
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Realrat.c (TLS SNI) 12
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 2
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 4
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 6
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 8
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 10
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 12
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 13
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 15
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 17
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 19
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 22
- [x] ET MOBILE_MALWARE Android/FakeWallet.AH!tr (TLS SNI) 24
- [x] ET MOBILE_MALWARE Android Spy APT-C-23 (frances-thomas .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android Spy APT-C-23 (scott-chapin .com in TLS SNI)
- [x] ET MOBILE_MALWARE Android Spy APT-C-23 (linda-gaytan .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android Spy APT-C-23 (david-gardiner .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android Spy APT-C-23 (amanda-hart .website in TLS SNI)
- [x] ET MOBILE_MALWARE Android Spy APT-C-23 (javan-demsky .website in TLS SNI)
- [x] ET MOBILE_MALWARE Observed Android ExobotCompact.D/Octo Domain (s22231232fdnsjds .top in TLS SNI)
- [x] ET MOBILE_MALWARE Observed Android ExobotCompact.D/Octo Domain (xipxesip .design in TLS SNI)

☑ ET MOBILE_MALWARE Observed Android/SpyLoan.9ef8bf95 Domain (api .dreamloan .cc in TLS SNI)
☑ ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Wroba Lure (Package Delivery)
☑ ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Origami.b / Donot DNS Lookup
☑ ET MOBILE_MALWARE Android ERMAC Banker (PL) Related Domain in DNS Lookup (bolt-food .site)
☑ ET MOBILE_MALWARE Android Spy Hermit CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy Hermit CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy Hermit CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy Hermit CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy Hermit CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy Hermit CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy Hermit CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy Hermit CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy Hermit CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Banker Octo CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Banker Octo CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Banker Octo CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Banker Octo CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Banker Octo CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Banker Octo CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Banker Octo CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Banker Octo CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Dropper Checkin Activity (POST)
☑ ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Ermak.a Checkin
☑ ET MOBILE_MALWARE Android/IRATA CnC Domain (rimotgozaran .tk) in DNS Lookup
☑ ET MOBILE_MALWARE Observed Android/IRATA Domain (rimotgozaran .tk) in TLS SNI
☑ ET MOBILE_MALWARE Android/IRATA Data Exfiltration Attempt
☑ ET MOBILE_MALWARE XX-Net VPN Client CnC Checkin
☑ ET MOBILE_MALWARE Trojan-Ransom.AndroidOS.Agent.bi CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Trojan-Dropper.AndroidOS.Guerrilla.h CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android/Drinik Activity (POST)
☑ ET MOBILE_MALWARE Android/Drinik CnC Domain (gia .3utilities .com) in DNS Lookup
☐ ET MOBILE_MALWARE Android/RatMilad CnC Domain (api .numrent .shop) in DNS Lookup
☐ ET MOBILE_MALWARE Bahamut Group Fake VPN Payload Delivery Domain (thesecurevpn .com) in DNS Lookup
☑ ET MOBILE_MALWARE Android/LoanBee Data Stealer Data Exfiltration Domain (api .loanbee .tech) in DNS Lookup
☑ ET MOBILE_MALWARE Backdoor.AndroidOS.Xhunter.a CnC Domain in DNS Lookup

☑ ET MOBILE_MALWARE Observed Trojan-Spy.AndroidOS.Agent.abe Domain in TLS SNI
☐ ET MOBILE_MALWARE Android/FakeWallet.D Activity (GET)
☑ ET MOBILE_MALWARE Observed Trojan-Spy.AndroidOS.Origami.b / Donot Domain in TLS SNI
☑ ET MOBILE_MALWARE Observed Android ERMAC Banker (PL) Domain (bolt-food .site in TLS SNI)
☑ ET MOBILE_MALWARE Android Spy Hermit CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy Hermit CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy Hermit CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy Hermit CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy Hermit CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy Hermit CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy Hermit CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy Hermit CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android/Revive Banking Trojan Initial Checkin Activity (POST)
☑ ET MOBILE_MALWARE Android Banker Octo CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Banker Octo CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Banker Octo CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Banker Octo CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Banker Octo CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Banker Octo CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Banker Octo CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Banker Octo CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android.Trojan.Banker.XJ Activity
☑ ET MOBILE_MALWARE Trojan-Dropper.AndroidOS.Hqwar.hf Checkin
☑ ET MOBILE_MALWARE Android/IRATA CnC Domain (rimot-anitain .tk) in DNS Lookup
☑ ET MOBILE_MALWARE Observed Android/IRATA Domain (rimot-anitain .tk) in TLS SNI
☑ ET MOBILE_MALWARE Android/Zanubis CnC Domain (fullcircleteam .com) in DNS Lookup
☑ ET MOBILE_MALWARE Trojan-Spy.AndroidOS.Agent.aam CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Trojan-Ransom.AndroidOS.Agent.bi CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android/Drinik Checkin Activity (POST)
☑ ET MOBILE_MALWARE Android/Drinik Activity M2 (POST)
☑ ET MOBILE_MALWARE Android/RatMilad CnC Checkin
☐ ET MOBILE_MALWARE Android/ShartBot CNC Domain (cdopea .store) in DNS Lookup
☐ ET MOBILE_MALWARE Bahamut Group Fake VPN CnC Domain (ft8hua063okwfdcu21pw .de) in DNS Lookup
☑ ET MOBILE_MALWARE Android/Spy.Agent.AKS CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Agent.ld CnC Domain in DNS Lookup

- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Agent.ld CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android/Spy.Vultur.A CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Trojan-Spy.AndroidOS.SmsThief.ta CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Banbra.aa CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Rewardsteal.e CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android/Spy.SmsSpy.XC CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android/Spy.Banker.BOF CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android.Backdoor.866.origin CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.Rewardsteal.e CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android/Gigabud CnC Domain (lionaiothai .com) in DNS Lookup
- [x] ET MOBILE_MALWARE Android/Gigabud CnC Domain (cmnb9 .cc) in DNS Lookup
- [x] ET MOBILE_MALWARE Android/Gigabud CnC Domain (bweri6 .cc) in DNS Lookup
- [x] ET MOBILE_MALWARE Android/Gigabud CnC Check-in M1
- [x] ET MOBILE_MALWARE Android/Gigabud CnC Check-in M2
- [x] ET MOBILE_MALWARE Android/Gigabud CnC Check-in M3
- [x] ET MOBILE_MALWARE Android/Gigabud CnC Check-in M4
- [x] ET MOBILE_MALWARE Android/Gigabud CnC Check-in M5
- [x] ET MOBILE_MALWARE Android/Gigabud CnC Check-in M6
- [x] ET MOBILE_MALWARE Android/Gigabud CnC Check-in M7
- [x] ET MOBILE_MALWARE Android/Gigabud CnC Check-in M8
- [x] ET MOBILE_MALWARE Android/Gigabud CnC Check-in M9
- [x] ET MOBILE_MALWARE Android/Gigabud CnC Check-in M10
- [x] ET MOBILE_MALWARE Android/Gigabud CnC Check-in M11
- [x] ET MOBILE_MALWARE Android/Gigabud CnC Check-in M12
- [x] ET MOBILE_MALWARE Android/FakeCalls CnC Server Response
- [x] ET MOBILE_MALWARE Android/Spy.Banker.BTO CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android/Harly.AO CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Trojan-Banker.AndroidOS.GoatRat CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Trojan-Ransom.AndroidOS.CryCrypt.c Checkin
- [x] ET MOBILE_MALWARE Trojan/iOS Operation Triangulation CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Trojan/iOS Operation Triangulation CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Trojan/iOS Operation Triangulation CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Trojan/iOS Operation Triangulation CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Trojan/iOS Operation Triangulation CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Trojan/iOS Operation Triangulation CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Trojan/iOS Operation Triangulation CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Trojan/iOS Operation Triangulation CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Trojan/iOS Operation Triangulation CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Trojan/iOS Operation Triangulation CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Trojan/iOS Operation Triangulation CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Trojan/iOS Operation Triangulation CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Trojan/iOS Operation Triangulation CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android/Spy.Bahamut.I CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup

- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup

- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
- [x] ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup

☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup

☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup

☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android/MMRAT Data Exfiltration Attempt
☑ ET MOBILE_MALWARE Android/MMRAT CnC Checkin M2
☑ ET MOBILE_MALWARE Fake Rocket Alerts App Sending Phone Information (POST)
☑ ET MOBILE_MALWARE GoldDigger CnC Domain in DNS Lookup (ks8cb .cc)
☑ ET MOBILE_MALWARE GoldDigger CnC Domain in DNS Lookup (bv8k .xyz)
☑ ET MOBILE_MALWARE GoldDigger CnC Domain in DNS Lookup (hzc5 .xyz)

☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☐ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android Spy PREDATOR CnC Domain in DNS Lookup
☑ ET MOBILE_MALWARE Android/InfamousChisel.InfoStealer APT28/SANDWORM Data Exfiltration
☑ ET MOBILE_MALWARE Android/MMRAT CnC Checkin M1
☑ ET MOBILE_MALWARE Android Nexus Banking Botnet Activity (GET)
☑ ET MOBILE_MALWARE Android FastViewer Variant Check-In (GET)
☑ ET MOBILE_MALWARE Observed GoldDigger Domain (ks8cb .cc in TLS SNI)
☑ ET MOBILE_MALWARE GoldDigger CnC Domain in DNS Lookup (t8bc .xyz)
☑ ET MOBILE_MALWARE GoldDigger CnC Domain in DNS Lookup (ms2ve .cc)

- [x] ET MOBILE_MALWARE GoldDigger CnC Domain in DNS Lookup (zu7kt .cc)
- [x] ET MOBILE_MALWARE Observed GoldDigger Domain (bv8k .xyz in TLS SNI)
- [x] ET MOBILE_MALWARE Observed GoldDigger Domain (t8bc .xyz in TLS SNI)
- [x] ET MOBILE_MALWARE Observed GoldDigger Domain (hzc5 .xyz in TLS SNI)
- [x] ET MOBILE_MALWARE Observed GoldDigger Domain (ms2ve .cc in TLS SNI)
- [x] ET MOBILE_MALWARE Observed GoldDigger Domain (zu7kt .cc in TLS SNI)
- [x] ET MOBILE_MALWARE Gigabud CnC Domain in DNS Lookup (blsdk5 .cc)
- [x] ET MOBILE_MALWARE Gigabud CnC Domain in DNS Lookup (nnzf1 .cc)
- [x] ET MOBILE_MALWARE Gigabud CnC Domain in DNS Lookup (bweri6 .cc)
- [x] ET MOBILE_MALWARE Gigabud CnC Domain in DNS Lookup (bc2k .xyz)
- [x] ET MOBILE_MALWARE Gigabud CnC Domain in DNS Lookup (re6s .xyz)
- [x] ET MOBILE_MALWARE Gigabud CnC Domain in DNS Lookup (js6kk .xyz)
- [x] ET MOBILE_MALWARE Observed Gigabud Domain (re6s .xyz in TLS SNI)
- [x] ET MOBILE_MALWARE Observed Gigabud Domain (js6kk .xyz in TLS SNI)
- [x] ET MOBILE_MALWARE Observed Gigabud Domain (bc2k .xyz in TLS SNI)
- [x] ET MOBILE_MALWARE Observed Gigabud Domain (bweri6 .cc in TLS SNI)
- [x] ET MOBILE_MALWARE Observed Gigabud Domain (nnzf1 .cc in TLS SNI)
- [x] ET MOBILE_MALWARE Observed Gigabud Domain (blsdk5 .cc in TLS SNI)
- [x] ET MOBILE_MALWARE Android Kamran Malware Related CnC Domain in DNS Lookup

- [x] **emerging-netbios.rules** Hide

- [ ] ET NETBIOS NII Microsoft ASN.1 Library Buffer Overflow Exploit
- [ ] ET NETBIOS LSA exploit
- [ ] ET NETBIOS MS04011 Lsasrv.dll RPC exploit (WinXP)
- [ ] ET NETBIOS MS04011 Lsasrv.dll RPC exploit (Win2k)
- [ ] ET NETBIOS MS04-007 Kill-Bill ASN1 exploit attempt
- [ ] ET NETBIOS ms05-011 exploit
- [ ] ET NETBIOS SMB-DS Microsoft Windows 2000 Plug and Play Vulnerability
- [ ] ET NETBIOS SMB-DS DCERPC PnP HOD bind attempt
- [ ] ET NETBIOS SMB-DS DCERPC PnP bind attempt
- [ ] ET NETBIOS SMB-DS DCERPC PnP QueryResConfList exploit attempt
- [ ] ET NETBIOS SMB DCERPC PnP bind attempt
- [ ] ET NETBIOS SMB DCERPC PnP QueryResConfList exploit attempt
- [ ] ET NETBIOS NETBIOS SMB DCERPC NetrpPathCanonicalize request (possible MS06-040)
- [ ] ET NETBIOS NETBIOS SMB-DS DCERPC NetrpPathCanonicalize request (possible MS06-040)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (1)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (2)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (3)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (4)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (5)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (7)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (8)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (9)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (10)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 - Known Exploit Instance
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (11)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (12)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (13)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (14)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (15)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (16)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (17)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (18)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (19)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (20)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (22)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (23)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (24)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (25)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (27)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (28)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (29)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (30)
- [x] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 - Known Exploit Instance (2)
- [ ] ET NETBIOS Remote SMB2.0 DoS Exploit
- [ ] ET NETBIOS windows recycler request - suspicious
- [ ] ET NETBIOS windows recycler .exe request - suspicious
- [x] ET NETBIOS Microsoft Windows SMB Client Race Condition Remote Code Execution
- [x] ET NETBIOS SMB Trans2 Query_Fs_Attribute_Info SrvSmbQueryFsInformation Pool Buffer Overflow
- [x] ET NETBIOS Microsoft Windows Server 2003 Active Directory Pre-Auth BROWSER ELECTION Heap Overflow Attempt
- [ ] ET NETBIOS Tree Connect AndX Request IPC$ Unicode
- [x] ET NETBIOS PolarisOffice Insecure Library Loading - SMB ASCII
- [x] ET NETBIOS PolarisOffice Insecure Library Loading - SMB Unicode
- [x] ET NETBIOS Microsoft Windows RRAS SMB Remote Code Execution
- [ ] ET NETBIOS DCERPC WMI Remote Process Execution

- [x] ET NETBIOS DCERPC DCOM ExecuteShellCommand Call - Likely Lateral Movement
- [ ] ET NETBIOS DCERPC DCOM ShellExecute - Likely Lateral Movement
- [ ] GPL NETBIOS x86 Linux samba overflow
- [x] GPL NETBIOS DOS RFPoison
- [x] GPL NETBIOS NT NULL session
- [x] GPL NETBIOS SMB ADMIN$ share access
- [x] GPL NETBIOS SMB C$ share access
- [x] GPL NETBIOS SMB CD..
- [x] GPL NETBIOS SMB CD...
- [x] GPL NETBIOS SMB D$ share access
- [x] GPL NETBIOS SMB IPC$ share access
- [x] GPL NETBIOS SMB IPC$ unicode share access
- [x] GPL NETBIOS xp_reg* - registry access
- [x] GPL NETBIOS xp_reg* registry access
- [x] GPL NETBIOS RFParalyze Attempt
- [ ] GPL NETBIOS SMB SMB_COM_TRANSACTION Max Parameter and Max Count of 0 DOS Attempt
- [ ] GPL NETBIOS SMB SMB_COM_TRANSACTION Max Data Count of 0 DOS Attempt
- [x] GPL NETBIOS SMB trans2open buffer overflow attempt
- [x] GPL NETBIOS SMB winreg create tree attempt
- [x] GPL NETBIOS SMB winreg unicode create tree attempt
- [x] GPL NETBIOS SMB startup folder access
- [x] GPL NETBIOS SMB startup folder unicode access
- [x] GPL NETBIOS DCERPC invalid bind attempt
- [x] GPL NETBIOS SMB DCERPC invalid bind attempt
- [ ] GPL NETBIOS DCERPC ISystemActivator bind attempt
- [x] GPL NETBIOS SMB-DS DCERPC ISystemActivator bind attempt
- [x] GPL NETBIOS DCERPC Remote Activation bind attempt
- [x] GPL NETBIOS SMB-DS DCERPC Remote Activation bind attempt
- [x] GPL NETBIOS DCERPC Messenger Service buffer overflow attempt
- [x] GPL NETBIOS SMB-DS DCERPC Messenger Service buffer overflow attempt
- [x] GPL NETBIOS SMB DCERPC Workstation Service unicode bind attempt
- [x] GPL NETBIOS SMB DCERPC Workstation Service bind attempt
- [x] GPL NETBIOS SMB-DS DCERPC Workstation Service unicode bind attempt
- [x] GPL NETBIOS SMB-DS DCERPC Workstation Service bind attempt
- [x] GPL NETBIOS DCERPC Workstation Service direct service bind attempt
- [x] GPL NETBIOS DCERPC Workstation Service direct service access attempt
- [ ] GPL NETBIOS SMB-DS DCERPC print spool bind attempt
- [ ] GPL NETBIOS SMB-DS DCERPC enumerate printers request attempt
- [ ] GPL NETBIOS SMB Session Setup NTMLSSP asn1 overflow attempt
- [x] GPL NETBIOS SMB-DS Session Setup NTMLSSP asn1 overflow attempt
- [x] GPL NETBIOS SMB NTLMSSP invalid mechlistMIC attempt
- [x] GPL NETBIOS SMB-DS DCERPC NTLMSSP invalid mechlistMIC attempt
- [x] GPL NETBIOS SMB Session Setup AndX request username overflow attempt
- [x] GPL NETBIOS SMB-DS Session Setup AndX request username overflow attempt
- [ ] GPL NETBIOS SMB Session Setup AndX request unicode username overflow attempt
- [ ] GPL NETBIOS SMB-DS Session Setup AndX request unicode username overflow attempt
- [x] GPL NETBIOS SMB-DS IPC$ share access
- [x] GPL NETBIOS SMB-DS IPC$ unicode share access
- [x] GPL NETBIOS SMB D$ unicode share access
- [x] GPL NETBIOS SMB-DS D$ share access
- [x] GPL NETBIOS SMB-DS D$ unicode share access
- [x] GPL NETBIOS SMB C$ unicode share access
- [x] GPL NETBIOS SMB-DS C$ share access
- [x] GPL NETBIOS SMB-DS C$ unicode share access
- [x] GPL NETBIOS SMB ADMIN$ unicode share access
- [x] GPL NETBIOS SMB-DS ADMIN$ share access
- [x] GPL NETBIOS SMB-DS ADMIN$ unicode share access
- [x] GPL NETBIOS SMB-DS winreg create tree attempt
- [x] GPL NETBIOS SMB-DS winreg unicode create tree attempt
- [x] GPL NETBIOS SMB-DS winreg bind attempt
- [x] GPL NETBIOS SMB-DS winreg unicode bind attempt
- [x] GPL NETBIOS SMB-DS InitiateSystemShutdown unicode attempt
- [x] GPL NETBIOS SMB-DS InitiateSystemShutdown unicode little endian attempt
- [x] GPL NETBIOS SMB-DS InitiateSystemShutdown attempt
- [x] GPL NETBIOS SMB-DS InitiateSystemShutdown little endian attempt
- [x] GPL NETBIOS SMB-DS DCERPC ISystemActivator unicode bind attempt
- [x] GPL NETBIOS SMB-DS DCEPRC ORPCThis request flood attempt
- [x] GPL NETBIOS DCERPC LSASS bind attempt
- [ ] GPL NETBIOS DCERPC LSASS DsRolerUpgradeDownlevelServer Exploit attempt
- [ ] GPL NETBIOS SMB DCERPC LSASS unicode bind attempt
- [x] GPL NETBIOS SMB DCERPC LSASS bind attempt
- [x] GPL NETBIOS SMB DCERPC LSASS DsRolerUpgradeDownlevelServer exploit attempt
- [x] GPL NETBIOS SMB-DS DCERPC LSASS bind attempt
- [x] GPL NETBIOS SMB-DS DCERPC LSASS unicode bind attempt
- [ ] GPL NETBIOS SMB-DS DCERPC LSASS DsRolerUpgradeDownlevelServer exploit attempt
- [x] GPL NETBIOS DCERPC LSASS direct bind attempt
- [x] GPL NETBIOS SMB DCERPC LSASS direct bind attempt
- [x] GPL NETBIOS SMB-DS DCERPC LSASS direct bind attempt
- [ ] GPL NETBIOS NS lookup response name overflow attempt
- [x] GPL NETBIOS SMB repeated logon failure
- [x] GPL NETBIOS SMB-DS repeated logon failure
- [x] GPL NETBIOS SMB nddeapi create tree attempt
- [x] GPL NETBIOS SMB nddeapi unicode create tree attempt
- [x] GPL NETBIOS SMB-DS nddeapi create tree attempt
- [x] GPL NETBIOS SMB-DS nddeapi unicode create tree attempt
- [x] GPL NETBIOS SMB nddeapi bind attempt
- [x] GPL NETBIOS SMB nddeapi unicode bind attempt
- [x] GPL NETBIOS SMB-DS nddeapi bind attempt
- [x] GPL NETBIOS SMB-DS nddeapi unicode bind attempt
- [x] GPL NETBIOS SMB NDdeSetTrustedShareW overflow attempt
- [x] GPL NETBIOS SMB NDdeSetTrustedShareW unicode overflow attempt
- [x] GPL NETBIOS SMB-DS NDdeSetTrustedShareW overflow attempt
- [x] GPL NETBIOS SMB-DS NDdeSetTrustedShareW unicode overflow attempt
- [x] GPL NETBIOS SMB winreg bind attempt
- [x] GPL NETBIOS SMB winreg unicode bind attempt
- [x] GPL NETBIOS SMB InitiateSystemShutdown attempt
- [x] GPL NETBIOS SMB InitiateSystemShutdown little endian attempt
- [x] GPL NETBIOS SMB InitiateSystemShutdown unicode attempt
- [x] GPL NETBIOS SMB InitiateSystemShutdown unicode little endian attempt
- [x] GPL NETBIOS SMB NDdeSetTrustedShareW little endian overflow attempt
- [x] GPL NETBIOS SMB NDdeSetTrustedShareW unicode little endian overflow attempt
- [x] GPL NETBIOS SMB-DS NDdeSetTrustedShareW little endian overflow attempt

- [x] GPL NETBIOS SMB-DS NDdeSetTrustedShareW unicode little endian overflow attempt
- [ ] GPL NETBIOS SMB too many stacked requests
- [ ] GPL NETBIOS SMB-DS too many stacked requests
- [x] GPL NETBIOS SMB-DS IPC$ andx share access
- [x] GPL NETBIOS SMB-DS IPC$ unicode andx share access
- [x] GPL NETBIOS SMB nddeapi andx create tree attempt
- [x] GPL NETBIOS SMB nddeapi unicode andx create tree attempt
- [x] GPL NETBIOS SMB-DS nddeapi andx create tree attempt
- [x] GPL NETBIOS SMB-DS nddeapi unicode andx create tree attempt
- [x] GPL NETBIOS SMB nddeapi andx bind attempt
- [x] GPL NETBIOS SMB nddeapi unicode andx bind attempt
- [x] GPL NETBIOS SMB-DS nddeapi andx bind attempt
- [x] GPL NETBIOS SMB-DS nddeapi unicode andx bind attempt
- [x] GPL NETBIOS SMB NDdeSetTrustedShareW andx overflow attempt
- [x] GPL NETBIOS SMB NDdeSetTrustedShareW little endian andx overflow attempt
- [x] GPL NETBIOS SMB NDdeSetTrustedShareW unicode andx overflow attempt
- [x] GPL NETBIOS SMB NDdeSetTrustedShareW unicode little endian andx overflow attempt
- [x] GPL NETBIOS SMB-DS NDdeSetTrustedShareW andx overflow attempt
- [x] GPL NETBIOS SMB-DS NDdeSetTrustedShareW little endian andx overflow attempt
- [x] GPL NETBIOS SMB-DS NDdeSetTrustedShareW unicode andx overflow attempt
- [x] GPL NETBIOS SMB-DS NDdeSetTrustedShareW unicode little endian andx overflow attempt
- [ ] GPL NETBIOS SMB-DS D$ andx share access
- [x] GPL NETBIOS SMB-DS D$ unicode andx share access
- [ ] GPL NETBIOS SMB-DS C$ andx share access
- [x] GPL NETBIOS SMB-DS C$ unicode andx share access
- [x] GPL NETBIOS SMB-DS ADMIN$ andx share access
- [x] GPL NETBIOS SMB-DS ADMIN$ unicode andx share access
- [x] GPL NETBIOS SMB winreg andx create tree attempt
- [x] GPL NETBIOS SMB winreg unicode andx create tree attempt
- [x] GPL NETBIOS SMB-DS winreg andx create tree attempt
- [x] GPL NETBIOS SMB-DS winreg unicode andx create tree attempt
- [x] GPL NETBIOS SMB winreg andx bind attempt
- [x] GPL NETBIOS SMB winreg unicode andx bind attempt
- [x] GPL NETBIOS SMB-DS winreg andx bind attempt
- [x] GPL NETBIOS SMB-DS winreg unicode andx bind attempt
- [x] GPL NETBIOS SMB InitiateSystemShutdown andx attempt
- [x] GPL NETBIOS SMB InitiateSystemShutdown little endian andx attempt
- [x] GPL NETBIOS SMB InitiateSystemShutdown unicode andx attempt
- [x] GPL NETBIOS SMB InitiateSystemShutdown unicode little endian andx attempt
- [x] GPL NETBIOS SMB-DS InitiateSystemShutdown andx attempt
- [x] GPL NETBIOS SMB-DS InitiateSystemShutdown little endian andx attempt
- [x] GPL NETBIOS SMB-DS InitiateSystemShutdown unicode andx attempt
- [x] GPL NETBIOS SMB-DS InitiateSystemShutdown unicode little endian andx attempt
- [ ] GPL NETBIOS SMB Session Setup NTMLSSP unicode asn1 overflow attempt
- [x] GPL NETBIOS SMB Session Setup NTMLSSP andx asn1 overflow attempt
- [x] GPL NETBIOS SMB Session Setup NTMLSSP unicode andx asn1 overflow attempt
- [x] GPL NETBIOS SMB-DS Session Setup NTMLSSP unicode asn1 overflow attempt
- [ ] GPL NETBIOS SMB-DS Session Setup NTMLSSP andx asn1 overflow attempt
- [ ] GPL NETBIOS SMB-DS Session Setup NTMLSSP unicode andx asn1 overflow attempt
- [x] GPL NETBIOS SMB NT Trans NT CREATE oversized Security Descriptor attempt
- [x] GPL NETBIOS SMB NT Trans NT CREATE andx oversized Security Descriptor attempt
- [x] GPL NETBIOS SMB NT Trans NT CREATE unicode oversized Security Descriptor attempt
- [ ] GPL NETBIOS SMB NT Trans NT CREATE unicode andx oversized Security Descriptor attempt
- [x] GPL NETBIOS SMB-DS NT Trans NT CREATE oversized Security Descriptor attempt
- [ ] GPL NETBIOS SMB-DS NT Trans NT CREATE andx oversized Security Descriptor attempt
- [x] GPL NETBIOS SMB-DS NT Trans NT CREATE unicode oversized Security Descriptor attempt
- [ ] GPL NETBIOS SMB-DS NT Trans NT CREATE unicode andx oversized Security Descriptor attempt
- [x] GPL NETBIOS SMB NT Trans NT CREATE SACL overflow attempt
- [x] GPL NETBIOS SMB NT Trans NT CREATE andx SACL overflow attempt
- [x] GPL NETBIOS SMB NT Trans NT CREATE unicode SACL overflow attempt
- [x] GPL NETBIOS SMB NT Trans NT CREATE unicode andx SACL overflow attempt
- [x] GPL NETBIOS SMB-DS NT Trans NT CREATE SACL overflow attempt
- [ ] GPL NETBIOS SMB-DS NT Trans NT CREATE andx SACL overflow attempt
- [x] GPL NETBIOS SMB-DS NT Trans NT CREATE unicode SACL overflow attempt
- [ ] GPL NETBIOS SMB-DS NT Trans NT CREATE unicode andx SACL overflow attempt
- [x] GPL NETBIOS SMB NT Trans NT CREATE DACL overflow attempt
- [x] GPL NETBIOS SMB NT Trans NT CREATE andx DACL overflow attempt
- [x] GPL NETBIOS SMB NT Trans NT CREATE unicode DACL overflow attempt
- [ ] GPL NETBIOS SMB NT Trans NT CREATE unicode andx DACL overflow attempt
- [x] GPL NETBIOS SMB-DS NT Trans NT CREATE DACL overflow attempt
- [ ] GPL NETBIOS SMB-DS NT Trans NT CREATE andx DACL overflow attempt
- [x] GPL NETBIOS SMB-DS NT Trans NT CREATE unicode DACL overflow attempt
- [ ] GPL NETBIOS SMB-DS NT Trans NT CREATE unicode andx DACL overflow attempt
- [x] GPL NETBIOS SMB NT Trans NT CREATE invalid SACL ace size dos attempt
- [ ] GPL NETBIOS SMB NT Trans NT CREATE andx invalid SACL ace size dos attempt
- [x] GPL NETBIOS SMB NT Trans NT CREATE unicode invalid SACL ace size dos attempt
- [ ] GPL NETBIOS SMB NT Trans NT CREATE unicode andx invalid SACL ace size dos attempt
- [x] GPL NETBIOS SMB-DS NT Trans NT CREATE invalid SACL ace size dos attempt
- [ ] GPL NETBIOS SMB-DS NT Trans NT CREATE andx invalid SACL ace size dos attempt
- [x] GPL NETBIOS SMB-DS NT Trans NT CREATE unicode invalid SACL ace size dos attempt
- [ ] GPL NETBIOS SMB-DS NT Trans NT CREATE unicode andx invalid SACL ace size dos attempt
- [x] GPL NETBIOS SMB NT Trans NT CREATE invalid SACL ace size dos attempt

- [ ] GPL NETBIOS SMB NT Trans NT CREATE andx invalid SACL ace size dos attempt
- [ ] GPL NETBIOS SMB NT Trans NT CREATE unicode andx invalid SACL ace size dos attempt
- [ ] GPL NETBIOS SMB-DS NT Trans NT CREATE andx invalid SACL ace size dos attempt
- [ ] GPL NETBIOS SMB-DS NT Trans NT CREATE unicode andx invalid SACL ace size dos attempt
- [ ] GPL NETBIOS SMB llsrpc unicode create tree attempt
- [ ] GPL NETBIOS SMB llsrpc unicode andx create tree attempt
- [ ] GPL NETBIOS SMB-DS llsrpc unicode create tree attempt
- [x] GPL NETBIOS SMB-DS llsrpc unicode andx create tree attempt
- [x] GPL NETBIOS SMB llsrpc little endian bind attempt
- [x] GPL NETBIOS SMB llsrpc unicode little endian bind attempt
- [x] GPL NETBIOS SMB llsrpc little endian andx bind attempt
- [x] GPL NETBIOS SMB llsrpc unicode little endian andx bind attempt
- [x] GPL NETBIOS SMB-DS llsrpc little endian bind attempt
- [x] GPL NETBIOS SMB-DS llsrpc unicode little endian bind attempt
- [x] GPL NETBIOS SMB-DS llsrpc little endian andx bind attempt
- [x] GPL NETBIOS SMB-DS llsrpc unicode little endian andx bind attempt
- [x] GPL NETBIOS SMB llsrconnect little endian overflow attempt
- [x] GPL NETBIOS SMB llsrconnect unicode little endian overflow attempt
- [x] GPL NETBIOS SMB llsrconnect little endian andx overflow attempt
- [x] GPL NETBIOS SMB llsrconnect unicode little endian andx overflow attempt
- [x] GPL NETBIOS SMB-DS llsrconnect little endian overflow attempt
- [x] GPL NETBIOS SMB-DS llsrconnect unicode little endian overflow attempt
- [x] GPL NETBIOS SMB-DS llsrconnect little endian andx overflow attempt
- [x] GPL NETBIOS SMB-DS llsrconnect unicode little endian andx overflow attempt
- [ ] GPL NETBIOS SMB Trans2 QUERY_FILE_INFO andx attempt
- [ ] GPL NETBIOS SMB-DS Trans2 QUERY_FILE_INFO andx attempt
- [ ] GPL NETBIOS SMB Trans2 FIND_FIRST2 andx attempt
- [ ] GPL NETBIOS SMB-DS Trans2 FIND_FIRST2 andx attempt
- [ ] GPL NETBIOS SMB Trans2 FIND_FIRST2 response andx overflow attempt
- [ ] GPL NETBIOS SMB-DS Trans2 FIND_FIRST2 response andx overflow attempt
- [x] GPL NETBIOS DCERPC msqueue little endian bind attempt
- [x] GPL NETBIOS DCERPC CoGetInstanceFromFile overflow attempt
- [x] GPL NETBIOS SMB msqueue little endian bind attempt
- [x] GPL NETBIOS SMB msqueue unicode little endian bind attempt
- [x] GPL NETBIOS SMB msqueue little endian andx bind attempt
- [x] GPL NETBIOS SMB msqueue unicode little endian andx bind attempt
- [x] GPL NETBIOS SMB-DS msqueue little endian bind attempt
- [x] GPL NETBIOS SMB-DS msqueue unicode little endian bind attempt
- [x] GPL NETBIOS SMB-DS msqueue little endian andx bind attempt
- [x] GPL NETBIOS SMB-DS msqueue unicode little endian andx bind attempt
- [x] GPL NETBIOS SMB CoGetInstanceFromFile little endian overflow attempt
- [x] GPL NETBIOS SMB CoGetInstanceFromFile unicode little endian overflow attempt
- [x] GPL NETBIOS SMB CoGetInstanceFromFile little endian andx overflow attempt
- [x] GPL NETBIOS SMB CoGetInstanceFromFile unicode little endian andx overflow attempt
- [x] GPL NETBIOS SMB-DS CoGetInstanceFromFile little endian overflow attempt
- [x] GPL NETBIOS SMB-DS CoGetInstanceFromFile unicode little endian overflow attempt
- [x] GPL NETBIOS SMB-DS CoGetInstanceFromFile little endian andx overflow attempt
- [x] GPL NETBIOS SMB-DS CoGetInstanceFromFile unicode little endian andx overflow attempt
- [x] GPL NETBIOS SMB NT Trans NT CREATE unicode invalid SACL ace size dos attempt
- [x] GPL NETBIOS SMB-DS NT Trans NT CREATE invalid SACL ace size dos attempt
- [x] GPL NETBIOS SMB-DS NT Trans NT CREATE unicode invalid SACL ace size dos attempt
- [x] GPL NETBIOS SMB llsrpc create tree attempt
- [ ] GPL NETBIOS SMB llsrpc andx create tree attempt
- [ ] GPL NETBIOS SMB-DS llsrpc create tree attempt
- [ ] GPL NETBIOS SMB-DS llsrpc andx create tree attempt
- [x] GPL NETBIOS SMB llsrpc bind attempt
- [x] GPL NETBIOS SMB llsrpc unicode bind attempt
- [x] GPL NETBIOS SMB llsrpc andx bind attempt
- [x] GPL NETBIOS SMB llsrpc unicode andx bind attempt
- [x] GPL NETBIOS SMB-DS llsrpc bind attempt
- [x] GPL NETBIOS SMB-DS llsrpc unicode bind attempt
- [x] GPL NETBIOS SMB-DS llsrpc andx bind attempt
- [x] GPL NETBIOS SMB-DS llsrpc unicode andx bind attempt
- [x] GPL NETBIOS SMB llsrconnect overflow attempt
- [x] GPL NETBIOS SMB llsrconnect unicode overflow attempt
- [x] GPL NETBIOS SMB llsrconnect andx overflow attempt
- [x] GPL NETBIOS SMB llsrconnect unicode andx overflow attempt
- [x] GPL NETBIOS SMB-DS llsrconnect overflow attempt
- [x] GPL NETBIOS SMB-DS llsrconnect unicode overflow attempt
- [x] GPL NETBIOS SMB-DS llsrconnect andx overflow attempt
- [x] GPL NETBIOS SMB-DS llsrconnect unicode andx overflow attempt
- [ ] GPL NETBIOS SMB Trans2 QUERY_FILE_INFO attempt
- [ ] GPL NETBIOS SMB-DS Trans2 QUERY_FILE_INFO attempt
- [ ] GPL NETBIOS SMB Trans2 FIND_FIRST2 attempt
- [ ] GPL NETBIOS SMB-DS Trans2 FIND_FIRST2 attempt
- [ ] GPL NETBIOS SMB Trans2 FIND_FIRST2 response overflow attempt
- [ ] GPL NETBIOS SMB-DS Trans2 FIND_FIRST2 response overflow attempt
- [x] GPL NETBIOS DCERPC msqueue bind attempt
- [x] GPL NETBIOS DCERPC CoGetInstanceFromFile little endian overflow attempt
- [x] GPL NETBIOS SMB msqueue bind attempt
- [x] GPL NETBIOS SMB msqueue unicode bind attempt
- [x] GPL NETBIOS SMB msqueue andx bind attempt
- [x] GPL NETBIOS SMB msqueue unicode andx bind attempt
- [x] GPL NETBIOS SMB-DS msqueue bind attempt
- [x] GPL NETBIOS SMB-DS msqueue unicode bind attempt
- [x] GPL NETBIOS SMB-DS msqueue andx bind attempt
- [x] GPL NETBIOS SMB-DS msqueue unicode andx bind attempt
- [x] GPL NETBIOS SMB CoGetInstanceFromFile overflow attempt
- [x] GPL NETBIOS SMB CoGetInstanceFromFile unicode overflow attempt
- [x] GPL NETBIOS SMB CoGetInstanceFromFile andx overflow attempt
- [x] GPL NETBIOS SMB CoGetInstanceFromFile unicode andx overflow attempt
- [x] GPL NETBIOS SMB-DS CoGetInstanceFromFile overflow attempt
- [x] GPL NETBIOS SMB-DS CoGetInstanceFromFile unicode overflow attempt
- [x] GPL NETBIOS SMB-DS CoGetInstanceFromFile andx overflow attempt
- [x] GPL NETBIOS SMB-DS CoGetInstanceFromFile unicode andx overflow attempt
- [ ] GPL NETBIOS name query overflow attempt TCP

- [ ] GPL NETBIOS name query overflow attempt UDP
- [ ] GPL NETBIOS DCERPC ISystemActivator path overflow attempt little endian
- [ ] GPL NETBIOS DCERPC ISystemActivator path overflow attempt big endian
- [ ] GPL NETBIOS WINS name query overflow attempt UDP
- [x] GPL NETBIOS SMB winreg bind attempt
- [x] GPL NETBIOS SMB winreg little endian bind attempt
- [x] GPL NETBIOS SMB winreg unicode bind attempt
- [x] GPL NETBIOS SMB winreg unicode little endian bind attempt
- [x] GPL NETBIOS SMB winreg andx bind attempt
- [x] GPL NETBIOS SMB winreg little endian andx bind attempt
- [x] GPL NETBIOS SMB winreg unicode andx bind attempt
- [x] GPL NETBIOS SMB winreg unicode little endian andx bind attempt
- [x] GPL NETBIOS SMB-DS winreg bind attempt
- [x] GPL NETBIOS SMB-DS winreg little endian bind attempt
- [x] GPL NETBIOS SMB-DS winreg unicode bind attempt
- [x] GPL NETBIOS SMB-DS winreg unicode little endian bind attempt
- [ ] GPL NETBIOS SMB-DS winreg andx bind attempt
- [x] GPL NETBIOS SMB-DS winreg little endian andx bind attempt
- [x] GPL NETBIOS SMB-DS winreg unicode andx bind attempt
- [x] GPL NETBIOS SMB-DS winreg unicode little endian andx bind attempt
- [x] GPL NETBIOS SMB OpenKey overflow attempt
- [x] GPL NETBIOS SMB OpenKey little endian overflow attempt
- [x] GPL NETBIOS SMB OpenKey unicode overflow attempt
- [x] GPL NETBIOS SMB OpenKey unicode little endian overflow attempt
- [x] GPL NETBIOS SMB OpenKey andx overflow attempt
- [x] GPL NETBIOS SMB OpenKey little endian andx overflow attempt
- [x] GPL NETBIOS SMB OpenKey unicode andx overflow attempt
- [x] GPL NETBIOS SMB OpenKey unicode little endian andx overflow attempt
- [x] GPL NETBIOS SMB-DS OpenKey overflow attempt
- [x] GPL NETBIOS SMB-DS OpenKey little endian overflow attempt
- [x] GPL NETBIOS SMB-DS OpenKey unicode overflow attempt
- [x] GPL NETBIOS SMB-DS OpenKey unicode little endian overflow attempt
- [x] GPL NETBIOS SMB-DS OpenKey andx overflow attempt
- [x] GPL NETBIOS SMB-DS OpenKey little endian andx overflow attempt
- [x] GPL NETBIOS SMB-DS OpenKey unicode andx overflow attempt
- [x] GPL NETBIOS SMB-DS OpenKey unicode little endian andx overflow attempt
- [ ] GPL NETBIOS Messenger message little endian overflow attempt
- [ ] GPL NETBIOS Messenger message overflow attempt
- [x] GPL NETBIOS DCERPC irot bind attempt
- [x] GPL NETBIOS DCERPC irot little endian bind attempt
- [x] GPL NETBIOS DCERPC IrotIsRunning attempt
- [x] GPL NETBIOS DCERPC IrotIsRunning little endian attempt
- [x] GPL NETBIOS SMB irot bind attempt
- [x] GPL NETBIOS SMB irot little endian bind attempt
- [x] GPL NETBIOS SMB irot unicode bind attempt
- [x] GPL NETBIOS SMB irot unicode little endian bind attempt
- [x] GPL NETBIOS SMB irot andx bind attempt
- [x] GPL NETBIOS SMB irot little endian andx bind attempt
- [x] GPL NETBIOS SMB irot unicode andx bind attempt
- [x] GPL NETBIOS SMB irot unicode little endian andx bind attempt
- [x] GPL NETBIOS SMB-DS irot bind attempt
- [x] GPL NETBIOS SMB-DS irot little endian bind attempt
- [x] GPL NETBIOS SMB-DS irot unicode bind attempt
- [x] GPL NETBIOS SMB-DS irot unicode little endian bind attempt
- [x] GPL NETBIOS SMB-DS irot andx bind attempt
- [x] GPL NETBIOS SMB-DS irot little endian andx bind attempt
- [x] GPL NETBIOS SMB-DS irot unicode andx bind attempt
- [x] GPL NETBIOS SMB-DS irot unicode little endian andx bind attempt
- [x] GPL NETBIOS SMB IrotIsRunning attempt
- [x] GPL NETBIOS SMB IrotIsRunning little endian attempt
- [x] GPL NETBIOS SMB IrotIsRunning unicode attempt
- [x] GPL NETBIOS SMB IrotIsRunning unicode little endian attempt
- [x] GPL NETBIOS SMB IrotIsRunning andx attempt
- [x] GPL NETBIOS SMB IrotIsRunning little endian andx attempt
- [x] GPL NETBIOS SMB IrotIsRunning unicode andx attempt
- [x] GPL NETBIOS SMB IrotIsRunning unicode little endian andx attempt
- [x] GPL NETBIOS SMB-DS IrotIsRunning attempt
- [x] GPL NETBIOS SMB-DS IrotIsRunning little endian attempt
- [x] GPL NETBIOS SMB-DS IrotIsRunning unicode attempt
- [x] GPL NETBIOS SMB-DS IrotIsRunning unicode little endian attempt
- [x] GPL NETBIOS SMB-DS IrotIsRunning andx attempt
- [x] GPL NETBIOS SMB-DS IrotIsRunning little endian andx attempt
- [x] GPL NETBIOS SMB-DS IrotIsRunning unicode andx attempt
- [x] GPL NETBIOS SMB-DS IrotIsRunning unicode little endian andx attempt
- [x] GPL NETBIOS DCERPC IActivation bind attempt
- [x] GPL NETBIOS DCERPC IActivation little endian bind attempt
- [x] GPL NETBIOS SMB IActivation bind attempt
- [x] GPL NETBIOS SMB IActivation little endian bind attempt
- [x] GPL NETBIOS SMB IActivation unicode bind attempt
- [x] GPL NETBIOS SMB IActivation unicode little endian bind attempt
- [x] GPL NETBIOS SMB IActivation andx bind attempt
- [x] GPL NETBIOS SMB IActivation little endian andx bind attempt
- [x] GPL NETBIOS SMB IActivation unicode andx bind attempt
- [x] GPL NETBIOS SMB IActivation unicode little endian andx bind attempt
- [x] GPL NETBIOS SMB-DS IActivation bind attempt
- [x] GPL NETBIOS SMB-DS IActivation little endian bind attempt
- [x] GPL NETBIOS SMB-DS IActivation unicode bind attempt
- [x] GPL NETBIOS SMB-DS IActivation unicode little endian bind attempt
- [x] GPL NETBIOS SMB-DS IActivation andx bind attempt
- [x] GPL NETBIOS SMB-DS IActivation little endian andx bind attempt
- [x] GPL NETBIOS SMB-DS IActivation unicode andx bind attempt
- [x] GPL NETBIOS SMB-DS IActivation unicode little endian andx bind attempt
- [x] GPL NETBIOS SMB ISystemActivator bind attempt
- [x] GPL NETBIOS SMB ISystemActivator little endian bind attempt
- [x] GPL NETBIOS SMB ISystemActivator unicode bind attempt
- [x] GPL NETBIOS SMB ISystemActivator unicode little endian bind attempt
- [x] GPL NETBIOS SMB ISystemActivator andx bind attempt
- [x] GPL NETBIOS SMB ISystemActivator little endian andx bind attempt
- [x] GPL NETBIOS SMB ISystemActivator unicode andx bind attempt
- [x] GPL NETBIOS SMB ISystemActivator unicode little endian andx bind attempt
- [x] GPL NETBIOS SMB-DS ISystemActivator bind attempt
- [x] GPL NETBIOS SMB-DS ISystemActivator little endian bind attempt
- [x] GPL NETBIOS SMB-DS ISystemActivator unicode bind attempt
- [x] GPL NETBIOS SMB-DS ISystemActivator unicode little endian bind attempt
- [x] GPL NETBIOS SMB-DS ISystemActivator andx bind attempt
- [x] GPL NETBIOS SMB-DS ISystemActivator little endian andx bind attempt
- [x] GPL NETBIOS SMB-DS ISystemActivator unicode andx bind attempt
- [x] GPL NETBIOS SMB-DS ISystemActivator unicode little endian andx bind attempt

- [x] GPL NETBIOS SMB RemoteActivation attempt
- [x] GPL NETBIOS SMB RemoteActivation little endian attempt
- [x] GPL NETBIOS SMB RemoteActivation unicode attempt
- [x] GPL NETBIOS SMB RemoteActivation unicode little endian attempt
- [x] GPL NETBIOS SMB RemoteActivation andx attempt
- [x] GPL NETBIOS SMB RemoteActivation little endian andx attempt
- [x] GPL NETBIOS SMB RemoteActivation unicode andx attempt
- [x] GPL NETBIOS SMB RemoteActivation unicode little endian andx attempt
- [x] GPL NETBIOS SMB-DS RemoteActivation attempt
- [x] GPL NETBIOS SMB-DS RemoteActivation little endian attempt
- [x] GPL NETBIOS SMB-DS RemoteActivation unicode attempt
- [x] GPL NETBIOS SMB-DS RemoteActivation unicode little endian attempt
- [x] GPL NETBIOS SMB-DS RemoteActivation andx attempt
- [x] GPL NETBIOS SMB-DS RemoteActivation little endian andx attempt
- [x] GPL NETBIOS SMB-DS RemoteActivation unicode andx attempt
- [x] GPL NETBIOS SMB-DS RemoteActivation unicode little endian andx attempt
- [x] GPL NETBIOS SMB CoGetInstanceFromFile attempt
- [x] GPL NETBIOS SMB CoGetInstanceFromFile little endian attempt
- [x] GPL NETBIOS SMB CoGetInstanceFromFile unicode attempt
- [x] GPL NETBIOS SMB CoGetInstanceFromFile unicode little endian attempt
- [x] GPL NETBIOS SMB CoGetInstanceFromFile andx attempt
- [x] GPL NETBIOS SMB CoGetInstanceFromFile little endian andx attempt
- [x] GPL NETBIOS SMB CoGetInstanceFromFile unicode andx attempt
- [x] GPL NETBIOS SMB CoGetInstanceFromFile unicode little endian andx attempt
- [x] GPL NETBIOS SMB-DS CoGetInstanceFromFile attempt
- [x] GPL NETBIOS SMB-DS CoGetInstanceFromFile little endian attempt
- [x] GPL NETBIOS SMB-DS CoGetInstanceFromFile unicode attempt
- [x] GPL NETBIOS SMB-DS CoGetInstanceFromFile unicode little endian attempt
- [x] GPL NETBIOS SMB-DS CoGetInstanceFromFile andx attempt
- [x] GPL NETBIOS SMB-DS CoGetInstanceFromFile little endian andx attempt
- [x] GPL NETBIOS SMB-DS CoGetInstanceFromFile unicode andx attempt
- [x] GPL NETBIOS SMB-DS CoGetInstanceFromFile unicode little endian andx attempt

- [ ] **emerging-p2p.rules** Show

- [x] **emerging-phishing.rules** Hide

- [ ] ET PHISHING Paypal Phishing victim POSTing data
- [ ] ET PHISHING Potential Paypal Phishing Form Attachment
- [ ] ET PHISHING Potential ACH Transaction Phishing Attachment
- [x] ET PHISHING Successful Generic Credit Card Information Phish
- [x] ET PHISHING Successful Generic PII Phish
- [x] ET PHISHING Successful Bank of America Phish M1 Oct 01 2012
- [x] ET PHISHING Possible Successful AOL Phish Nov 21 2012
- [x] ET PHISHING Possible Successful Yahoo Phish Nov 21 2012
- [x] ET PHISHING Possible Successful Gmail Phish Nov 21 2012
- [x] ET PHISHING Possible Successful Hotmail Phish Nov 21 2012
- [x] ET PHISHING Possible Successful Phish - Other Credentials Nov 21 2012
- [ ] ET PHISHING Spam Campaign JPG CnC Link
- [x] ET PHISHING Chase/Bank of America Phishing Landing Uri Structure Nov 27 2012
- [x] ET PHISHING Possible Successful Generic SSN Phish
- [ ] ET PHISHING PHISH Generic - Bank and Routing
- [x] ET PHISHING Successful PayPal Phish Nov 30 2012
- [x] ET PHISHING Successful Google Account Phish Dec 04 2012
- [ ] ET PHISHING PHISH Bank - York - Creds Phished
- [x] ET PHISHING Successful PayPal Phish Dec 19 2012
- [x] ET PHISHING Possible Successful Phish - Generic POST to myform.php Feb 01 2013
- [x] ET PHISHING Possible Generic Phishing Landing Jul 12 2013
- [x] ET PHISHING Possible Successful AOL Phish Nov 25 2013
- [x] ET PHISHING Possible Successful Yahoo Phish Nov 25 2013
- [x] ET PHISHING Possible Successful Gmail Phish Nov 25 2013
- [x] ET PHISHING Possible Successful Remax Phish - Hotmail Creds Nov 25 2013
- [x] ET PHISHING Possible Successful Phish - Other Credentials Nov 25 2013
- [x] ET PHISHING Apple Phishing Landing Jan 30 2014
- [ ] ET PHISHING PHISH Visa - Landing Page
- [x] ET PHISHING Possible Successful Verified by Visa Phish Jan 30 2014
- [x] ET PHISHING Possible Phish - Mirrored Website Comment Observed
- [x] ET PHISHING Possible iTunes Phishing Landing - Title over non SSL
- [x] ET PHISHING Successful iTunes Phish Mar 21 2014
- [x] ET PHISHING Successful iTunes Phish Mar 21 2014
- [x] ET PHISHING Possible Phish - Saved Website Comment Observed
- [ ] ET PHISHING Possible Phishing E-ZPass Email Toll Notification July 30 2014
- [ ] ET PHISHING Potential Sofacy Phishing Redirect
- [ ] ET PHISHING Operation Huyao Landing Page Nov 07 2014
- [ ] ET PHISHING Operation Huyao Phishing Page Nov 07 2014
- [x] ET PHISHING Successful AOL/PayPal Phish Nov 24 2014
- [x] ET PHISHING Successful PayPal Phish Nov 24 2014
- [x] ET PHISHING Successful Paypal Phish Nov 24 2014
- [x] ET PHISHING Successful Paypal Phish Nov 24 2014
- [x] ET PHISHING PayPal Phishing Landing Nov 24 2014
- [x] ET PHISHING Possible Dropbox Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible Tsukuba Banker Edwards Packed proxy.pac
- [x] ET PHISHING Successful Adobe Phish Jun 17 2015
- [x] ET PHISHING Successful Google Drive Phish June 17 2015
- [x] ET PHISHING Successful Dropbox Phish June 17 2015
- [x] ET PHISHING Possible Successful Remax Phish - AOL Creds Jun 23 2015
- [x] ET PHISHING Possible Successful Yahoo Phish Jun 23 2015
- [x] ET PHISHING Possible Successful Remax Phish - Other Creds Jun 23 2015
- [x] ET PHISHING Possible Google Drive/Dropbox Phishing Landing Jul 10 2015
- [x] ET PHISHING Google Drive Phishing Landing M1 July 24 2015
- [x] ET PHISHING Google Drive Phishing Landing M2 July 24 2015
- [x] ET PHISHING Possible Generic Phishing Landing Jul 28 2015
- [x] ET PHISHING Possible Generic Phishing Landing Jul 28 2015
- [x] ET PHISHING Possible Generic Phishing Landing Jul 28 2015
- [x] ET PHISHING Possible Generic Phishing Landing Jul 28 2015
- [x] ET PHISHING Possible Successful Generic Phish - Credit Card
- [x] ET PHISHING Possible Successful Generic Phish - Three Security Questions
- [x] ET PHISHING Possible Successful Phish - Generic Status Messages Sept 11 2015
- [x] ET PHISHING Successful Phish Outlook Credentials Oct 01 2015
- [x] ET PHISHING Potential Data URI Phishing Oct 02 2015
- [x] ET PHISHING Successful Paypal Account Phish Oct 30
- [x] ET PHISHING Successful Paypal Account Phish 2015-10-30 2
- [x] ET PHISHING Successful Paypal Account Phish 2015-10-30 3

- [ ] ET PHISHING Jimdo.com Phishing PDF via HTTP
- [x] ET PHISHING Mailbox Renewal Phish Landing Nov 13
- [ ] ET PHISHING Jimdo Outlook Web App Phishing Landing Nov 16
- [ ] ET PHISHING Generic Phishing Landing Uri Nov 25 2015
- [ ] ET PHISHING Chrome Extension Phishing DNS Request
- [x] ET PHISHING Suspicious LastPass URI Structure - Possible Phishing
- [x] ET PHISHING Successful Phishing Attempt via GetGoPhish Phishing Tool
- [x] ET PHISHING Successful Apple Phish M2 Feb 06 2016
- [x] ET PHISHING JS Obfuscation - Possible Phishing 2016-03-01
- [ ] ET PHISHING Successful Enom Phish Mar 08 2016
- [x] ET PHISHING Possible Apple Phishing Domain Mar 14 2016
- [x] ET PHISHING Possible Paypal Phishing Domain Mar 14 2016
- [x] ET PHISHING PhishMe.com Phishing Landing Exercise
- [x] ET PHISHING Successful Google Drive/Dropbox Phish Nov 20 2016
- [x] ET PHISHING Successful Bank of Oklahoma Phish M2 Jul 21 2016
- [x] ET PHISHING Successful Apple Suspended Account Phish M2 Aug 09 2016
- [x] ET PHISHING Excel Online Phishing Landing Aug 09 2016
- [ ] ET PHISHING Successful Generic Adobe Shared Document Phish Aug 11 2016
- [x] ET PHISHING Email Storage Upgrade Phishing Landing 2016-08-15
- [ ] ET PHISHING Successful Credit Agricole Phish Aug 15 2016 M2
- [x] ET PHISHING Possible Bank of America Phishing Domain Aug 15 2016
- [x] ET PHISHING Netflix Phishing Landing 2016-08-17
- [x] ET PHISHING Possible Successful Phish to .tk domain Aug 26 2016
- [ ] ET PHISHING DNS Query to Ebay Phishing Domain
- [ ] ET PHISHING Successful Tesco Bank Phish M1 Nov 08 2016
- [x] ET PHISHING Possible Cartasi Phishing Domain Nov 08 2016
- [x] ET PHISHING Successful XBOOMBER Paypal Phish Nov 28 2016
- [x] ET PHISHING Possible Linkedin Phishing Domain Dec 09 2016
- [x] ET PHISHING Microsoft Edge SmartScreen Page Spoof Attempt Dec 16 2016
- [x] ET PHISHING Successful Bradesco Bank Phish M2 Jan 05 2017
- [x] ET PHISHING Paypal Phishing Landing Jan 09 2017
- [x] ET PHISHING Successful Paypal Phish Jan 23 2017
- [x] ET PHISHING Possible Ebay Phishing Domain Jan 30 2017
- [x] ET PHISHING Possible Discover Phishing Domain Feb 02 2017
- [x] ET PHISHING Possible Successful Apple Phishing Domain Feb 02 2017
- [x] ET PHISHING Possible Successful Paypal Phishing Domain Feb 02 2017
- [x] ET PHISHING Possible Successful Google Drive Phishing Domain Feb 02 2017
- [x] ET PHISHING Possible Successful Linkedin Phishing Domain Feb 02 2017
- [x] ET PHISHING Possible Successful Discover Phish Feb 02 2017
- [ ] ET PHISHING DNS Request to NilePhish Domain 02
- [ ] ET PHISHING DNS Request to NilePhish Domain 04
- [ ] ET PHISHING DNS Request to NilePhish Domain 06
- [ ] ET PHISHING DNS Request to NilePhish Domain 08
- [ ] ET PHISHING DNS Request to NilePhish Domain 10
- [ ] ET PHISHING DNS Request to NilePhish Domain 12
- [ ] ET PHISHING DNS Request to NilePhish Domain 14
- [ ] ET PHISHING DNS Request to NilePhish Domain 16
- [ ] ET PHISHING DNS Request to NilePhish Domain 18
- [ ] ET PHISHING DNS Request to NilePhish Domain 20
- [ ] ET PHISHING DNS Request to NilePhish Domain 22
- [ ] ET PHISHING DNS Request to NilePhish Domain 24
- [ ] ET PHISHING DNS Request to NilePhish Domain 26
- [ ] ET PHISHING DNS Request to NilePhish Domain 28
- [ ] ET PHISHING DNS Request to NilePhish Domain 30
- [ ] ET PHISHING DNS Request to NilePhish Domain 32
- [ ] ET PHISHING Google Drive (Remax) Phish Landing Nov 4
- [x] ET PHISHING Revalidation Phish Landing Nov 13 2015
- [x] ET PHISHING Netsolhost SSL Proxying - Possible Phishing Nov 24 2015
- [x] ET PHISHING Successful Google Drive Phish Dec 4 2015 M1
- [x] ET PHISHING Chrome Extension Phishing HTTP Request
- [x] ET PHISHING Possible Phishing Landing via GetGoPhish Phishing Tool
- [x] ET PHISHING Successful Apple Phish M1 Feb 06 2016
- [x] ET PHISHING Successful Apple Phish M3 Feb 06 2016
- [x] ET PHISHING Possible Phishing Landing - Data URI Inline Javascript Mar 07 2016
- [x] ET PHISHING Possible Chase Phishing Domain Mar 14 2016
- [x] ET PHISHING Possible USAA Phishing Domain Mar 14 2016
- [x] ET PHISHING PhishMe.com Phishing Exercise - Client Plugins
- [ ] ET PHISHING Suspicious Hidden Javascript Redirect - Possible Phishing Jun 17
- [x] ET PHISHING Successful Bank of Oklahoma Phish M1 Jul 21 2016
- [ ] ET PHISHING Successful Apple Suspended Account Phish M1 Aug 09 2016
- [x] ET PHISHING Apple Suspended Account Phishing Landing Aug 09 2016
- [x] ET PHISHING Adobe Shared Document Phishing Landing Nov 19 2015
- [x] ET PHISHING Successful Excel Phish Aug 15 2016
- [ ] ET PHISHING Successful Credit Agricole Phish Aug 15 2016 M1
- [x] ET PHISHING Possible Square Enix Phishing Domain 2016-08-15
- [ ] ET PHISHING Successful Netflix Phish Aug 17 2016
- [x] ET PHISHING Possible Google Drive Phishing Domain Aug 25 2016
- [x] ET PHISHING Form Data Submitted to yolasite.com - Possible Phishing
- [ ] ET PHISHING Possible Fake AV Phone Scam Long Domain Sept 15 2016
- [ ] ET PHISHING Successful Tesco Bank Phish M2 Nov 08 2016
- [ ] ET PHISHING XBOOMBER Paypal Phishing Landing Nov 28 2016
- [x] ET PHISHING Successful iCloud Phish Oct 10 2016
- [x] ET PHISHING Possible Phishing Redirect Dec 13 2016
- [x] ET PHISHING Successful Bradesco Bank Phish M1 Jan 05 2017
- [x] ET PHISHING Successful National Bank Phish Jan 05 2017
- [x] ET PHISHING Possible Successful Generic Paypal Phish Jan 23 2016
- [x] ET PHISHING Successful RBC Royal Bank Phish Jan 30 2017
- [x] ET PHISHING Possible Successful Ebay Phish Jan 30 2017
- [x] ET PHISHING Possible Successful Chase Phish Feb 02 2017
- [x] ET PHISHING Possible Successful USAA Phishing Domain Feb 02 2017
- [x] ET PHISHING Possible Successful Bank of America Phishing Domain Feb 02 2017
- [x] ET PHISHING Possible Successful Cartasi Phishing Domain Feb 02 2017
- [x] ET PHISHING Possible Successful Ebay Phishing Domain Feb 02 2017
- [ ] ET PHISHING DNS Request to NilePhish Domain 01
- [ ] ET PHISHING DNS Request to NilePhish Domain 03
- [ ] ET PHISHING DNS Request to NilePhish Domain 05
- [ ] ET PHISHING DNS Request to NilePhish Domain 07
- [ ] ET PHISHING DNS Request to NilePhish Domain 09
- [ ] ET PHISHING DNS Request to NilePhish Domain 11
- [ ] ET PHISHING DNS Request to NilePhish Domain 13
- [ ] ET PHISHING DNS Request to NilePhish Domain 15
- [ ] ET PHISHING DNS Request to NilePhish Domain 17
- [ ] ET PHISHING DNS Request to NilePhish Domain 19
- [ ] ET PHISHING DNS Request to NilePhish Domain 21
- [ ] ET PHISHING DNS Request to NilePhish Domain 23
- [ ] ET PHISHING DNS Request to NilePhish Domain 25
- [ ] ET PHISHING DNS Request to NilePhish Domain 27
- [ ] ET PHISHING DNS Request to NilePhish Domain 29
- [ ] ET PHISHING DNS Request to NilePhish Domain 31
- [ ] ET PHISHING DNS Request to NilePhish Domain 33

- [ ] ET PHISHING DNS Request to NilePhish Domain 34
- [x] ET PHISHING Possible Successful Craigslist Phishing Domain Feb 07 2017
- [ ] ET PHISHING Successful Banco Itau (BR) Mobile Phish M1 Feb 09 2017
- [x] ET PHISHING Successful WeTransfer Phish Oct 04 2016
- [ ] ET PHISHING Successful iCloud (CN) Phish Feb 17 2017
- [x] ET PHISHING Successful Banco Itau (BR) Mobile Phish Feb 17 2017
- [x] ET PHISHING Suspicious JS Refresh - Possible Phishing Redirect Feb 24 2017
- [x] ET PHISHING Successful Craigslist (RO) Phish M1 Feb 24 2017
- [x] ET PHISHING Successful Orderlink (IN) Phish Feb 24 2017
- [ ] ET PHISHING Paypal Phishing Redirect M2 Feb 24 2017
- [x] ET PHISHING Paypal Phishing Landing Feb 24 2017
- [x] ET PHISHING Successful National Bank Phish Mar 13 2017
- [x] ET PHISHING Successful Paypal Phish Mar 14 2017
- [x] ET PHISHING Successful Apple Phish M1 Mar 15 2017
- [x] ET PHISHING Windows Settings Phishing Landing Jul 22 2016
- [x] ET PHISHING Successful RBC Royal Bank Phish Mar 27 2017
- [x] ET PHISHING Successful HM Revenue & Customs Phish M1 Apr 07 2017
- [ ] ET PHISHING Successful Santander Phish M1 Apr 07 2017
- [ ] ET PHISHING Successful Santander Phish M3 Apr 07 2017
- [x] ET PHISHING Suspicious HTML Decimal Obfuscated Title - Possible Phishing Landing Apr 19 2017
- [ ] ET PHISHING Successful iCloud Phish Apr 20 2017
- [x] ET PHISHING Miniproxy Cloned Page - Possible Phishing Landing
- [ ] ET PHISHING Successful Scotiabank Phish M2 May 24 2017
- [x] ET PHISHING Successful Banco do Brasil Phish May 25 2017
- [x] ET PHISHING Successful Banco Itau (BR) Phish Jun 09 2017
- [x] ET PHISHING Possible Successful Hostinger Generic Phish Jun 09 2017
- [x] ET PHISHING Possible iCloud Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible Docusign Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible Alibaba Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible Paypal Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible Free Mobile Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible OWA Mail Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible Facebook Help Center Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible Adobe PDF Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible Adobe ID Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible Dropbox Phishing Landing - Title over non SSL
- [x] ET PHISHING Suspicious HTML Hex Obfuscated Title - Possible Phishing Landing Jun 28 2017
- [x] ET PHISHING Possible Facebook Phishing Landing - Title over non SSL
- [x] ET PHISHING Successful Netflix Payment Phish M1 Jan 04 2017
- [x] ET PHISHING HTTP POST to Free Webhost - Possible Successful Phish (site40 . net) Jul 18 2017
- [ ] ET PHISHING Successful Mail.ru Phish Aug 10 2017
- [x] ET PHISHING Successful Paypal Phish M2 Aug 14 2017
- [x] ET PHISHING Successful Square Phish Nov 16 2015
- [x] ET PHISHING Possible Successful Generic Phish (set) Feb 26 2016
- [x] ET PHISHING Possible Successful Generic Phish (set) Jun 8 2016
- [x] ET PHISHING Possible Successful Generic Phish (set) Aug 19 2016
- [x] ET PHISHING Possible Successful Generic Phish (set) Oct 13 2016
- [x] ET PHISHING Possible Successful Generic Phish (set) Oct 26 2016
- [x] ET PHISHING Possible Successful Generic Phish (set) Nov 16 2016
- [x] ET PHISHING Possible Successful Generic Phish (set) Dec 07 2016
- [x] ET PHISHING Possible Successful Generic Phish (set) Dec 20 2016
- [ ] ET PHISHING DNS Request to NilePhish Domain 35
- [ ] ET PHISHING Successful Apple Phish Feb 09 2017
- [ ] ET PHISHING Successful Banco Itau (BR) Mobile Phish M2 Feb 09 2017
- [x] ET PHISHING Successful Apple Account Phish Feb 17 2017
- [ ] ET PHISHING Successful California Bank & Trust Phish Feb 17 2017
- [x] ET PHISHING Possible Phishing Verified by Visa title over non SSL Feb 17 2017
- [x] ET PHISHING Possible Phishing Redirect Feb 24 2017
- [x] ET PHISHING Successful Craigslist (RO) Phish M2 Feb 24 2017
- [x] ET PHISHING Paypal Phishing Redirect M1 Feb 24 2017
- [x] ET PHISHING Common Paypal Phishing URI Feb 24 2017
- [ ] ET PHISHING Successful Paypal Phish Mar 13 2017
- [x] ET PHISHING Successful Instagram Phish Mar 14 2017
- [ ] ET PHISHING Successful iCloud Phish Mar 15 2017
- [x] ET PHISHING Successful Apple Phish M2 Mar 15 2017
- [x] ET PHISHING Successful Paypal Phish Mar 22 2017
- [ ] ET PHISHING Successful Mail.ru Phish Apr 04 2017
- [x] ET PHISHING Successful HM Revenue & Customs Phish M2 Apr 07 2017
- [ ] ET PHISHING Successful Santander Phish M2 Apr 07 2017
- [x] ET PHISHING Lets Encrypt Free SSL Cert Observed with IDN/ Punycode Domain - Possible Phishing
- [x] ET PHISHING iCloud Phishing Landing 2016-09-02
- [ ] ET PHISHING Successful Alitalia Airline Phish Apr 20 2017
- [x] ET PHISHING Successful Scotiabank Phish M1 May 24 2017
- [x] ET PHISHING Successful Banco do Brasil Phish Mar 30 2017
- [x] ET PHISHING Successful Poste Italiane Phish Jun 08 2017
- [ ] ET PHISHING Successful Apple Phish Jun 09 2017
- [x] ET PHISHING Generic Credit Card Information in HTTP POST - Possible Successful Phish Jun 12 2017
- [x] ET PHISHING Possible Google Docs Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible Dropbox Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible Yahoo Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible Excel Online Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible AOL Mail Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible OWA Mail Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible Yahoo Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible DHL Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible Facebook Phishing Landing - Title over non SSL
- [x] ET PHISHING Amazon Phish Landing Jun 22 2017
- [x] ET PHISHING Possible Phishing Blockchain title over non SSL Jul 10 2017
- [x] ET PHISHING Possible Capitech Internet Banking Phishing Landing - Title over non SSL
- [x] ET PHISHING DNS Query to Generic 107 Phishing Domain
- [x] ET PHISHING Phishery Phishing Tool - Default SSL Certificate Observed
- [x] ET PHISHING Possible Successful Phish - Verify Email Error Message M1 Aug 14 2017
- [ ] ET PHISHING Successful Paypal Phish M3 Aug 14 2017
- [x] ET PHISHING Possible Successful Generic Phish (set) Feb 26 2016
- [x] ET PHISHING Possible Successful Generic Phish (set) Feb 26 2016
- [x] ET PHISHING Possible Successful Generic Phish (set) Jul 13 2016
- [x] ET PHISHING Possible Successful Generic Phish (set) Sept 02 2016
- [x] ET PHISHING Possible Successful Generic Phish (set) Oct 25 2016
- [x] ET PHISHING Possible Successful Generic Phish (set) Nov 15 2016
- [x] ET PHISHING Possible Successful Generic Phish (set) Nov 22 2016
- [x] ET PHISHING Possible Successful Generic Phish (set) Dec 13 2016
- [x] ET PHISHING Possible Successful Generic Phish (set) Dec 27 2016

- [x] ET PHISHING Possible Successful Generic Phish (set) Jan 03 2017
- [x] ET PHISHING Possible Successful Generic Phish (set) Jan 17 2017
- [x] ET PHISHING Possible Successful Generic Phish (set) May 24 2017
- [x] ET PHISHING Possible Successful Generic Phish (set) May 31 2017
- [x] ET PHISHING Possible Successful Generic Phish (set) Jul 06 2017
- [x] ET PHISHING Possible Successful Generic Phish (set) Jul 11 2017
- [x] ET PHISHING Successful RBC Royal Bank Phish M1 Aug 17 2017
- [x] ET PHISHING Possible Interac Phish Aug 18 2017
- [x] ET PHISHING Successful Blockchain Account Phish Aug 19 2016
- [x] ET PHISHING Successful Exmo Cryptocurrency Exchange Phish Aug 28 2017
- [x] ET PHISHING Possible NatWest Bank Phishing Landing - Title over non SSL
- [ ] ET PHISHING Possible NatWest Bank Phishing Landing - Title over non SSL
- [x] ET PHISHING Successful LocalBitcoins Cryptocurrency Exchange Phish Aug 30 2017
- [x] ET PHISHING Apple Phishing Landing M1 Sep 14 2017
- [x] ET PHISHING Apple Phishing Landing M3 Sep 14 2017
- [x] ET PHISHING Possible Raiffeisen Bank Phishing Landing - Title over non SSL
- [x] ET PHISHING Successful Banco do Brasil Phish M2 Sep 29 2017
- [x] ET PHISHING Possible Scotiabank Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible CIBC Phishing Landing - Title over non SSL
- [ ] ET PHISHING Phishing Landing Oct 04 2017
- [ ] ET PHISHING Successful Santander Phish M3 Oct 04 2017
- [x] ET PHISHING Possible Facebook Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible Successful Paypal Phishing Domain (IT) Oct 10 2017
- [x] ET PHISHING Successful Ziraat Bankasi (TK) Phish M2 Oct 12 2017
- [x] ET PHISHING Successful Paypal Phish Oct 16 2017
- [x] ET PHISHING Successful HMRC Phish Oct 18 2017
- [x] ET PHISHING Raiffeisen Phishing Domain Nov 03 2017
- [x] ET PHISHING BankAustria Phishing Domain Nov 03 2017
- [x] ET PHISHING Successful Sparkasse Phish Nov 03 2017
- [x] ET PHISHING Possible Paypal Phishing Landing - Title over non SSL
- [x] ET PHISHING Successful Generic AES Phish M1 Oct 24 2017
- [x] ET PHISHING Successful OWA Phish Apr 25 2017
- [x] ET PHISHING Possible Successful Websocket Credential Phish Sep 15 2017
- [x] ET PHISHING Successful TeamIPwned Phish 2016-08-30
- [x] ET PHISHING Possible Successful Generic Phish Jan 14 2016
- [x] ET PHISHING Possible Successful Generic Phish (set) Nov 20 2017
- [x] ET PHISHING Successful Tesco Phish (set) M1 Jul 18 2017
- [x] ET PHISHING Successful Tesco Phish (set) M3 Jul 18 2017
- [x] ET PHISHING Successful Generic Phish (set) Aug 21 2017
- [x] ET PHISHING Possible Successful Generic Phish (set) Sep 19 2017
- [x] ET PHISHING Successful Generic Credit Card Information Phish Oct 10 2017
- [x] ET PHISHING Possible Successful Generic Phish (set) Oct 26 2017
- [x] ET PHISHING Possible Successful Generic Phish Nov 09 2017 (set)
- [x] ET PHISHING Possible Credentials Sent to Suspicious TLD via HTTP GET
- [x] ET PHISHING Possible Successful Generic Phish (set) 2017-12-04
- [x] ET PHISHING Possible MyEtherWallet Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible Halkbank (TK) Phishing Landing - Title over non SSL
- [x] ET PHISHING Paypal Phishing Landing 2017-12-26
- [x] ET PHISHING Possible Successful Generic Phish (set) Jan 12 2017
- [x] ET PHISHING Possible Successful Generic Phish (set) Jan 17 2017
- [x] ET PHISHING Possible Successful Generic Phish (set) May 25 2017
- [x] ET PHISHING Possible Successful Generic Phish (set) Jun 08 2017
- [x] ET PHISHING Possible Successful Generic Phish (set) Jul 10 2017
- [x] ET PHISHING Possible YapiKredi Bank (TR) Phishing Landing - Title over non SSL
- [x] ET PHISHING Successful RBC Royal Bank Phish M2 Aug 17 2017
- [x] ET PHISHING Possible Successful Generic Phish (set) Aug 25 2017
- [x] ET PHISHING Successful Poloniex Cryptocurrency Exchange Phish Aug 28 2017
- [x] ET PHISHING Successful Paxful Cryptocurrency Wallet Phish Aug 30 2017
- [ ] ET PHISHING Possible NatWest Bank Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible Successful Generic Phish (set) Aug 31 2017
- [x] ET PHISHING Dropbox Phishing Landing - Title over non SSL
- [x] ET PHISHING Apple Phishing Landing M2 Sep 14 2017
- [x] ET PHISHING Possible Apple Phishing Landing - Title over non SSL
- [x] ET PHISHING Successful Banco do Brasil Phish M1 Sep 29 2017
- [x] ET PHISHING Successful Banco do Brasil Phish M3 Sep 29 2017
- [x] ET PHISHING Possible Desjardins Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible BMO Bank of Montreal Phishing Landing - Title over non SSL
- [x] ET PHISHING Successful Santander Phish M1 Oct 04 2017
- [x] ET PHISHING Successful Santander Phish M2 Oct 04 2017
- [x] ET PHISHING Possible Paypal Phishing Domain (IT) Oct 10 2017
- [x] ET PHISHING Successful Ziraat Bankasi (TK) Phish M1 Oct 12 2017
- [x] ET PHISHING Possible Google Docs Phishing Landing - Title over non SSL
- [x] ET PHISHING Successful Paypal (FR) Phish Oct 16 2017
- [x] ET PHISHING 401TRG Successful Multi-Email Phish - Observed in Docusign/Dropbox/Onedrive/Gdrive Nov 02 2017
- [x] ET PHISHING Sparkasse Phishing Domain Nov 03 2017
- [x] ET PHISHING Successful Raiffeisen Phish Nov 03 2017
- [x] ET PHISHING Successful BankAustria Phish Nov 03 2017
- [x] ET PHISHING Browser Plugin Detect - Observed in Apple Phishing
- [x] ET PHISHING Successful Generic AES Phish M2 Oct 24 2017
- [x] ET PHISHING Possible Successful Phish to Hostinger Domains Apr 4 M4
- [x] ET PHISHING Successful Personalized OWA Webmail Phish Oct 04 2016
- [x] ET PHISHING Google Drive Phishing Landing Sept 3
- [x] ET PHISHING Possible Phishing Redirect Feb 09 2016
- [x] ET PHISHING Successful Tesco Bank Phish (set) Jul 17 2017
- [x] ET PHISHING Successful Tesco Phish (set) M2 Jul 18 2017
- [x] ET PHISHING Successful Tesco Phish (set) M4 Jul 18 2017
- [x] ET PHISHING Possible Successful Generic Phish (set) Aug 22 2017
- [x] ET PHISHING Successful Generic Phish (set) Sep 28 2017
- [x] ET PHISHING Successful Office 365 Phish Oct 10 2017 (set)
- [x] ET PHISHING Successful Generic Phish (set) Oct 30 2017
- [x] ET PHISHING Possible Successful Generic Phish (set) 2017-12-03
- [x] ET PHISHING Successful EDU Phish 2017-12-04
- [x] ET PHISHING Possible Facebook Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible Fedex Phishing Landing - Title over non SSL
- [x] ET PHISHING Possible Ziraat Bank (TK) Phishing Landing - Title over non SSL
- [x] ET PHISHING Successful Yobit Cryptocurrency Exchange Phish 2017-12-28

- [x] ET PHISHING Successful HitBTC Cryptocurrency Exchange Phish 2017-12-28
- [x] ET PHISHING Possible Successful Generic Phish (set) 2018-01-02
- [x] ET PHISHING Dropbox Phishing Landing 2018-01-18
- [x] ET PHISHING Office 365 Phishing Landing 2018-01-18
- [x] ET PHISHING Bank of America Phishing Landing 2018-01-18 M1
- [x] ET PHISHING Possible Chase Phishing Landing - Title over non SSL
- [x] ET PHISHING Paypal Phishing Landing 2018-01-18 M2
- [x] ET PHISHING Possible Phishing Landing - Common Multiple JS Unescape May 25 2017
- [x] ET PHISHING Multiple Javascript Unescapes - Common Obfuscation Observed in Phish Landing
- [x] ET PHISHING Dropbox Phishing Landing - Title over non SSL
- [x] ET PHISHING Blocked Incoming Emails Phishing Landing 2018-01-23
- [x] ET PHISHING AT&T Phishing Landing 2018-01-23
- [x] ET PHISHING LCL Banque et Assurance (FR) Phishing Landing 2018-01-23
- [x] ET PHISHING Generic Multi-Email Popupwnd Phishing Landing 2018-01-25
- [x] ET PHISHING Office 365 Phishing Landing 2018-01-25
- [x] ET PHISHING Possible Halkbank (TK) Phishing Landing - Title over non SSL
- [x] ET PHISHING Apple Phishing Landing 2018-01-29 M1
- [x] ET PHISHING Paypal Phishing Landing 2018-01-29
- [x] ET PHISHING Microsoft Onedrive Phishing Landing 2018-01-29
- [x] ET PHISHING Possible Phishing Redirect 2018-01-30
- [x] ET PHISHING Turbotax Phishing Landing 2018-01-30
- [x] ET PHISHING Possible Capital One Phishing Landing - Title over non SSL
- [x] ET PHISHING Paypal Phishing Landing 2018-01-31
- [x] ET PHISHING Mailbox Verification Phishing Landing 2018-01-31
- [x] ET PHISHING Generic Roundcube Multi-Brand Phishing Landing 2018-01-31
- [x] ET PHISHING Cloned Website Phishing Landing - Mirrored Website Comment Observed
- [x] ET PHISHING TSB Bank / Lloyds Bank Phishing Landing 2018-02-01
- [x] ET PHISHING Likely Cloned .EDU Website Phishing Landing 2018-02-02
- [x] ET PHISHING Wells Fargo Phishing Landing 2018-02-02 M2
- [x] ET PHISHING Wells Fargo Phishing Landing 2018-02-02 M4
- [x] ET PHISHING Wells Fargo Phishing Landing 2018-02-02 M6
- [x] ET PHISHING Wells Fargo Phishing Landing 2018-02-02 M8
- [ ] ET PHISHING Wells Fargo Phishing Landing 2018-02-02 M10
- [x] ET PHISHING Paypal Phishing Landing 2018-02-05
- [x] ET PHISHING Facebook Upgrade Payment Phishing Landing 2018-02-05
- [x] ET PHISHING Yahoo Account Verification Phishing Landing 2018-02-05
- [x] ET PHISHING Orange Phishing Landing 2018-02-05 (FR)
- [x] ET PHISHING Possible MyEtherWallet Phishing Landing - SSL/TLS Certificate Observed
- [x] ET PHISHING Ebay Phishing Landing 2018-02-07
- [x] ET PHISHING Dropbox Business Phishing Landing 2018-02-07
- [x] ET PHISHING Dropbox Business Phishing Landing 2018-02-07
- [x] ET PHISHING Dropbox/OneDrive Phishing Landing 2018-02-07
- [x] ET PHISHING Mailbox Verification Phishing Landing 2018-02-07
- [x] ET PHISHING ASB Bank Phishing Landing 2018-02-09 M1
- [x] ET PHISHING ASB Bank Phishing Landing 2018-02-09 M2
- [x] ET PHISHING LinkedIn Phishing Landing 2018-02-09 M2
- [x] ET PHISHING Mailbox Revalidation Phishing Landing 2018-02-09
- [x] ET PHISHING OneDrive Phishing Landing 2018-02-12
- [x] ET PHISHING Facebook Phishing Landing 2018-02-13 M1
- [x] ET PHISHING LinkedIn Phishing Landing 2018-02-13
- [x] ET PHISHING Wells Fargo Phishing Landing 2018-02-13
- [x] ET PHISHING Generic Email Validation Phishing Landing 2018-02-13
- [x] ET PHISHING Dropbox Phishing Landing 2018-02-14
- [x] ET PHISHING Successful Liqui Cryptocurrency Exchange Phish 2017-12-28
- [x] ET PHISHING Paypal Phishing Landing 2018-01-03
- [x] ET PHISHING Chase Phishing Landing 2018-01-18
- [x] ET PHISHING Chase Phishing Landing 2018-01-18
- [x] ET PHISHING Bank of America Phishing Landing 2018-01-18 M2
- [x] ET PHISHING Paypal Phishing Landing 2018-01-18 M1
- [x] ET PHISHING Microsoft Questionnaire Phishing Landing 2018-01-19
- [x] ET PHISHING Email Verification/Upgrade Phishing Landing 2018-01-22
- [x] ET PHISHING Email Server Mobile Security Settings Phishing Landing 2018-01-22
- [x] ET PHISHING Possible Compromised Wordpress - Generic Phishing Landing 2018-01-22
- [x] ET PHISHING ABSA Online Phishing Landing 2018-01-23
- [x] ET PHISHING Facebook Phishing Landing 2018-01-23
- [x] ET PHISHING Paypal Phishing Landing 2018-01-25
- [x] ET PHISHING Generic Multi-Email Phishing Landing 2018-01-25
- [x] ET PHISHING Mailbox Phishing Landing 2018-01-29
- [x] ET PHISHING Generic Smail Phishing Landing 2018-01-29
- [x] ET PHISHING Generic Phishing Landing M2 2018-01-29
- [x] ET PHISHING Office 365 Phishing Landing 2018-01-29
- [x] ET PHISHING Smartsheet Phishing Landing 2018-01-29
- [x] ET PHISHING Impots.gouv.fr Phishing Landing 2018-01-30
- [x] ET PHISHING Bank of America Phishing Landing 2018-01-30
- [x] ET PHISHING Verizon Wireless Phishing Landing 2018-01-30
- [x] ET PHISHING Apple iTunes Phishing Landing (DE) 2018-01-31
- [x] ET PHISHING Hellion Postmaster Phishing Landing 2018-01-31
- [x] ET PHISHING Cloned Website Phishing Landing - Saved Website Comment Observed
- [x] ET PHISHING Microsoft Live Login Phishing Landing 2018-02-01
- [x] ET PHISHING Wells Fargo Phishing Landing 2018-02-01
- [x] ET PHISHING Wells Fargo Phishing Landing 2018-02-02 M1
- [x] ET PHISHING Wells Fargo Phishing Landing 2018-02-02 M3
- [x] ET PHISHING Wells Fargo Phishing Landing 2018-02-02 M5
- [x] ET PHISHING Wells Fargo Phishing Landing 2018-02-02 M7
- [x] ET PHISHING Wells Fargo Phishing Landing 2018-02-02 M9
- [x] ET PHISHING Banque Populaire Phishing Landing 2018-02-05
- [x] ET PHISHING Possible Generic Antibots Phishing Landing 2018-02-05
- [x] ET PHISHING Mailbox Upgrade Phishing Landing 2018-02-05
- [x] ET PHISHING Google/Adobe Shared Document Phishing Landing 2018-02-05
- [x] ET PHISHING Office 365 Phishing Landing 2018-02-06
- [x] ET PHISHING Possible MyMonero Phishing Landing - SSL/TLS Certificate Observed
- [x] ET PHISHING Google Drive Phishing Landing 2018-02-07
- [ ] ET PHISHING Apple Phishing Landing 2018-02-07
- [x] ET PHISHING Outlook Web App Phishing Landing 2018-02-07
- [x] ET PHISHING Chase Phishing Landing 2018-02-07
- [x] ET PHISHING Successful Generic .EDU Phish (Legit Set)
- [x] ET PHISHING LinkedIn Phishing Landing 2018-02-09 M1
- [x] ET PHISHING Wells Fargo Phishing Landing 2018-02-09
- [x] ET PHISHING Facebook Phishing Landing 2018-02-09
- [x] ET PHISHING Facebook Phishing Landing 2018-02-12
- [x] ET PHISHING Wells Fargo Phishing Landing 2018-02-12
- [x] ET PHISHING Facebook Phishing Landing 2018-02-13 M2
- [x] ET PHISHING Capital One Phishing Landing 2018-02-13 M1
- [x] ET PHISHING Capital One Phishing Landing 2018-02-13 M2
- [x] ET PHISHING Possible Successful Generic Phish (set) 2018-02-13
- [x] ET PHISHING Linkedin Phishing Landing 2018-02-14

- [x] ET PHISHING Facebook Phishing Landing 2018-02-14
- [x] ET PHISHING Sparkasse Phishing Landing 2018-02-15
- [x] ET PHISHING Facebook Phishing Landing 2018-02-15
- [x] ET PHISHING Dropbox Phishing Landing 2018-02-15
- [x] ET PHISHING Square Phishing Landing 2018-02-15
- [x] ET PHISHING Spotify Phishing Landing 2018-02-19
- [x] ET PHISHING USAA Phishing Landing 2018-02-20
- [x] ET PHISHING Wells Fargo Phishing Landing 2018-02-22
- [x] ET PHISHING Upgrade Advantage Phishing Landing 2018-02-22
- [x] ET PHISHING Craigslist Phishing Landing 2018-02-26
- [x] ET PHISHING Facebook Mobile Phishing Landing 2018-02-26
- [x] ET PHISHING Amazon Phishing Landing (DE) 2018-02-26
- [x] ET PHISHING OneDrive Phishing Landing 2018-03-08
- [x] ET PHISHING Chalbhai Phishing Landing 2018-03-12
- [x] ET PHISHING Successful Wells Fargo Phish 2018-03-12
- [x] ET PHISHING Retrieve Pending Emails Phishing Landing 2018-03-12
- [x] ET PHISHING Successful Generic Phish (set) 2018-03-13
- [x] ET PHISHING IRS Phishing Landing 2018-03-28
- [x] ET PHISHING Impots Phishing Landing 2018-03-28
- [x] ET PHISHING Wells Fargo Phishing Landing 2018-04-09
- [x] ET PHISHING Chase Phishing Landing 2018-04-09
- [x] ET PHISHING s0m3 Phishing Landing 2018-04-09
- [x] ET PHISHING Facebook Phishing Landing 2018-04-09
- [x] ET PHISHING Apple Phishing Landing 2018-04-09
- [x] ET PHISHING Google Drive Phishing Landing 2018-04-14
- [x] ET PHISHING Successful Halkbank Phish M2 2018-04-16
- [x] ET PHISHING Successful DenizBank Phish 2018-04-16
- [x] ET PHISHING Mail Verification Phishing Landing 2018-04-18
- [x] ET PHISHING Bank of America Phishing Landing 2018-04-19
- [x] ET PHISHING Centurylink Phishing Landing 2018-04-19
- [x] ET PHISHING Microsoft Account Phishing Landing M1 2018-04-19
- [x] ET PHISHING Generic Popupwnd Phishing Landing 2018-04-19
- [x] ET PHISHING LCL Banque Phishing Landing 2018-04-19
- [x] ET PHISHING Bank of America Phishing Landing 2018-05-01
- [ ] ET PHISHING Docusign Phishing Landing 2018-05-01
- [x] ET PHISHING Netflix Phishing Landing 2018-05-02
- [x] ET PHISHING IRS Phishing Landing 2018-05-07
- [x] ET PHISHING Possible TSB Bank Phishing Landing 2018-05-07
- [x] ET PHISHING Successful Generic Phish 2018-05-08 (set)
- [x] ET PHISHING Netflix Phishing Landing 2018-05-09
- [x] ET PHISHING Paypal Phishing Landing 2018-05-09
- [x] ET PHISHING Paypal Phishing Landing 2018-05-09
- [x] ET PHISHING Successful Generic Phish 2018-05-16 (set)
- [x] ET PHISHING Possible Successful Generic Phish (set) 2018-06-11
- [x] ET PHISHING Generic Paypal Phish Kit Landing
- [x] ET PHISHING Santander Phishing Landing
- [x] ET PHISHING Adobe PDF Online Phishing Landing
- [x] ET PHISHING iTunes Connect Phishing Landing
- [x] ET PHISHING Microsoft Account Phishing Landing
- [x] ET PHISHING Assurance Maladie Phishing Landing
- [x] ET PHISHING Capital One Phishing Landing
- [x] ET PHISHING American Express Phishing Landing
- [x] ET PHISHING Generic Phishing Kit Landing
- [x] ET PHISHING [eSentire] Wells Fargo Phishing Landing 2018-06-20
- [x] ET PHISHING [eSentire] Successful Generic Phish 2018-06-15
- [x] ET PHISHING Successful Generic Phish 2018-06-27 (set)
- [x] ET PHISHING [eSentire] Adobe Phishing Landing 2018-07-04
- [x] ET PHISHING Chalbhai Phishing Landing Feb 18 2016
- [x] ET PHISHING AES Crypto Observed in Javascript - Possible Phishing Landing
- [x] ET PHISHING Generic Phishing Landing M1 2017-02-13
- [x] ET PHISHING Paypal Phishing Landing Jun 28 2017
- [x] ET PHISHING Possible Wells Fargo Phishing Landing - Title over non SSL
- [x] ET PHISHING Dropbox Phishing Landing 2018-02-15
- [ ] ET PHISHING Google Docs Phishing Landing 2018-02-15
- [x] ET PHISHING Chase Phishing Landing 2018-02-15
- [x] ET PHISHING Successful Generic Multi-Account Phish 2018-02-16
- [x] ET PHISHING Smartermail Phishing Landing 2018-02-20
- [x] ET PHISHING Yahoo Phishing Landing 2018-02-20
- [x] ET PHISHING Office 365 Phishing Landing 2018-02-22
- [x] ET PHISHING Wells Fargo Phishing Landing 2018-02-22
- [x] ET PHISHING Credit Mutuel de Bretagne (FR) Phishing Landing 2018-02-26
- [x] ET PHISHING Mailbox Update Phishing Landing 2018-02-26
- [x] ET PHISHING Suspicious Browser Plugin Detect - Observed in Phish Landings
- [x] ET PHISHING Successful Generic Phish (set) 2018-03-12
- [x] ET PHISHING Successful O2 Phish 2018-03-12
- [x] ET PHISHING Upgrade Email Account Phishing Landing 2018-03-12
- [x] ET PHISHING Ourtime Phishing Landing 2018-03-12
- [x] ET PHISHING Adobe PDF Reader Phishing Landing 2018-03-27
- [x] ET PHISHING Chase Phishing Landing 2018-03-28
- [x] ET PHISHING Comcast/Xfinity Phishing Landing 2018-03-30
- [x] ET PHISHING DHL Phishing Landing 2018-04-09
- [x] ET PHISHING [eSentire] Docusign Phishing Landing 2018-04-09
- [x] ET PHISHING Paypal Phishing Landing 2018-04-09
- [x] ET PHISHING OneDrive Phishing Landing 2018-04-09
- [x] ET PHISHING Post.ch Cloned Phishing Landing 2018-04-09
- [x] ET PHISHING Successful Halkbank Phish M1 2018-04-16
- [x] ET PHISHING Successful Facebook Phish 2018-04-16
- [x] ET PHISHING Successful Generic Phish (set) 2018-04-17
- [x] ET PHISHING PDF Cloud Phishing Landing 2018-04-19
- [x] ET PHISHING Dropbox 000webhost Phishing Landing 2018-04-19
- [x] ET PHISHING MyADP Phishing Landing 2018-04-19
- [x] ET PHISHING Microsoft Account Phishing Landing M2 2018-04-19
- [x] ET PHISHING Comcast/Xfinity Phishing Landing 2018-04-19
- [x] ET PHISHING Outlook Web App Phishing Landing 2018-04-26
- [x] ET PHISHING OneDrive Phishing Landing 2018-05-01
- [x] ET PHISHING Possible Successful Generic Phish (set) 2018-05-02
- [x] ET PHISHING Paypal Phishing Landing 2018-05-02
- [x] ET PHISHING Successful IRS Phish 2018-05-07
- [x] ET PHISHING Possible Successful TSB Bank Phish 2018-05-07
- [x] ET PHISHING Successful Generic Phish 2018-05-08 (set)
- [x] ET PHISHING Netflix Phishing Landing 2018-05-09
- [x] ET PHISHING Paypal Phishing Landing 2018-05-09
- [x] ET PHISHING Paypal Phishing Landing 2018-05-09
- [x] ET PHISHING Possible Successful Generic Phish (set) 2018-05-31
- [x] ET PHISHING Possible Successful Generic Phish (set) 2018-06-14
- [x] ET PHISHING Santander Phishing Landing
- [x] ET PHISHING Microsoft Live Phishing Landing
- [x] ET PHISHING Banque et Assurances Phishing Landing
- [x] ET PHISHING Facebook Phishing Landing
- [x] ET PHISHING Paypal Phishing Landing
- [x] ET PHISHING Adobe Phishing Landing
- [x] ET PHISHING US Bank Phishing Landing
- [x] ET PHISHING HM Revenue Phishing Landing
- [x] ET PHISHING Office 365 Phishing Landing
- [x] ET PHISHING [eSentire] OneDrive Phishing Landing 2018-06-15
- [x] ET PHISHING [eSentire] Successful Personalized Phish 2018-06-15
- [x] ET PHISHING Successful Generic Phish (set) 2018-06-29
- [x] ET PHISHING Possible Chalbhai (Multibrand) Phishing Landing 2018-05-10
- [x] ET PHISHING Chalbhai Phishing Landing Oct 23 2017
- [x] ET PHISHING AES Crypto Observed in Javascript - Possible Phishing Landing M1 Dec 28 2015
- [x] ET PHISHING Suspicious Dropbox Page - Possible Phishing Landing
- [x] ET PHISHING Dropbox Phishing Landing May 31 2017

- [x] ET PHISHING Docusign Phishing Landing Mar 08 2017
- [x] ET PHISHING Microsoft Live Email Account Phishing Landing Mar 16 2017
- [x] ET PHISHING Bank of America Phishing Landing Aug 19 2015
- [x] ET PHISHING Stripe Phishing Landing Dec 09 2016
- [x] ET PHISHING Wells Fargo Mobile Phishing Landing 2016-08-01
- [x] ET PHISHING Shared Document Phishing Landing Nov 16 2016
- [x] ET PHISHING Possible Chase Phishing Landing - Title over non SSL
- [x] ET PHISHING Mailbox Update Phishing Landing M2 2016-05-16
- [x] ET PHISHING Mailbox Shutdown Phishing Landing 2017-12-11
- [x] ET PHISHING Google Drive Phishing Landing Nov 6 2015 M2
- [x] ET PHISHING Google Drive Phishing Landing Jul 24 2015
- [x] ET PHISHING Google Drive Phish Landing 2016-09-01
- [x] ET PHISHING Excel/Adobe Online Phishing Landing Nov 25 2015
- [x] ET PHISHING Dropbox Shared Document Phishing Landing Feb 21 2017
- [x] ET PHISHING DHL Phish Landing Sept 14 2015
- [x] ET PHISHING Chase Account Phish Landing Oct 22
- [x] ET PHISHING Adobe Online Document Phishing Landing M1 Mar 25 2017
- [x] ET PHISHING Bank of America Phishing Landing
- [x] ET PHISHING Successful Generic Phish (set) 2018-07-19
- [x] ET PHISHING GitLab Phishing Landing 2018-07-19
- [x] ET PHISHING Twitter Phishing Landing 2018-07-19
- [x] ET PHISHING LinkedIn Phishing Landing 2017-07-20
- [x] ET PHISHING [eSentire] Successful 163 Webmail Phish 2018-07-25
- [x] ET PHISHING Successful Generic Phish (set) 2018-08-01
- [x] ET PHISHING Microsoft Account Phishing Landing 2018-08-07
- [x] ET PHISHING Free Mobile Phishing Landing 2018-08-07
- [x] ET PHISHING Microsoft Ajax Phishing Landing 2018-08-07
- [x] ET PHISHING Microsoft Phishing Landing 2018-08-07
- [ ] ET PHISHING Successful Generic Phish (set) 2018-08-27
- [x] ET PHISHING Generic Chalbhai Phishing Landing 2018-08-30
- [x] ET PHISHING Hellion Postmaster Phishing Landing 2018-08-30
- [x] ET PHISHING Generic Multi-Email Phishing Landing 2018-08-30
- [x] ET PHISHING Generic Multi-Email Phishing Landing 2018-08-30
- [x] ET PHISHING Stripe Phishing Landing 2018-08-30
- [x] ET PHISHING Google Docs Phishing Landing 2018-08-30
- [x] ET PHISHING Bank of America Phishing Landing 2018-08-30
- [x] ET PHISHING Generic Mailbox Phishing Landing 2018-08-30
- [x] ET PHISHING Dropbox Phishing Landing 2018-08-30
- [x] ET PHISHING AT&T Phishing Landing 2018-08-30
- [x] ET PHISHING Generic PhishKit Author Comment M2 2018-08-30
- [x] ET PHISHING Generic PhishKit Author Comment M4 2018-08-30
- [x] ET PHISHING Generic PhishKit Author Comment M6 2018-08-30
- [x] ET PHISHING Generic PhishKit Author Comment M8 2018-08-30
- [x] ET PHISHING Generic PhishKit Author Comment M10 2018-08-30
- [x] ET PHISHING Successful Generic Phish (set) 2018-09-24
- [x] ET PHISHING Generic MRxJoker Phishing Landing 2018-09-27
- [ ] ET PHISHING Successful Generic Phish (set) 2018-10-10
- [x] ET PHISHING DNS Lookup for Possible Common Brand Phishing Hosted on Legitimate Windows Service
- [x] ET PHISHING Successful Generic Phish (set) 2018-10-16
- [x] ET PHISHING Possible Successful Phish - Generic Credential POST to Ngrok.io
- [x] ET PHISHING Successful Fedex/DHL Phish (set) 2018-10-22
- [x] ET PHISHING Possible Successful Generic Phish to .ml Domain 2018-10-23
- [x] ET PHISHING Possible Successful Generic Phish to .ga Domain 2018-10-23
- [x] ET PHISHING Possible Successful Generic Phish to .gqn Domain 2018-10-23
- [x] ET PHISHING Generic Financial Phish Landing 2017-12-21
- [x] ET PHISHING Generic Credential Phishing Landing Aug 11 2015
- [x] ET PHISHING Apple Phishing Landing M2 Feb 13 2017
- [x] ET PHISHING Suspicious Google Docs Page - Possible Phishing Landing
- [x] ET PHISHING Suspicious Wordpress Redirect - Possible Phishing Landing Jan 7 2016
- [x] ET PHISHING Possible Office 365 Phishing Landing 2016-08-24
- [x] ET PHISHING Microsoft Live External Link Phishing Landing M2 Feb 14 2017
- [x] ET PHISHING Mailbox Update Phishing Landing M1 2016-05-16
- [x] ET PHISHING INTERAC Payment Multibank Phishing Landing Mar 14 2017
- [x] ET PHISHING Google Drive Phishing Landing Nov 6 2015 M1
- [x] ET PHISHING Google Drive Phishing Landing Jul 10 2015
- [x] ET PHISHING Generic Phishing Landing 2018-01-12
- [x] ET PHISHING Email Settings Error Phishing Landing Nov 16 2016
- [x] ET PHISHING Dropbox Phishing Landing Feb 27 2017
- [x] ET PHISHING Chase Mobile Phishing Landing M2
- [x] ET PHISHING Apple Phishing Landing Nov 10 2017
- [x] ET PHISHING Suspicious Wordpress Redirect - Possible Phishing Landing (set) Jan 7
- [x] ET PHISHING Possible Successful Generic Phish (set) 2018-07-19
- [x] ET PHISHING Badoo Phishing Landing 2018-07-19
- [x] ET PHISHING Github Phishing Landing 2018-07-19
- [x] ET PHISHING Netflix Phishing Landing 2017-07-20
- [x] ET PHISHING [eSentire] DHL Phish Landing July 24 2018
- [x] ET PHISHING Paypal Phishing Landing 2018-07-30
- [x] ET PHISHING Christian Mingle Phishing Landing 2018-08-07
- [x] ET PHISHING Paypal Phishing Landing 2018-08-07
- [x] ET PHISHING Adobe Phishing Landing 2018-08-07
- [x] ET PHISHING Alibaba Phishing Landing 2018-08-07
- [x] ET PHISHING Successful Generic Phish Phish 2018-08-21
- [x] ET PHISHING Generic Chalbhai Phishing Landing 2018-08-30
- [x] ET PHISHING Generic AES Phishing Landing 2018-08-30
- [x] ET PHISHING Microsoft Document Phishing Landing 2018-08-30
- [x] ET PHISHING Generic Multi-Email Phishing Landing 2018-08-30
- [x] ET PHISHING Apple AES Phishing Landing 2018-08-30
- [x] ET PHISHING Adobe PDF Phishing Landing 2018-08-30
- [x] ET PHISHING WeTransfer Phishing Landing 2018-08-30
- [x] ET PHISHING Bank of America Phishing Landing 2018-08-30
- [x] ET PHISHING Generic Mailbox Phishing Landing 2018-08-30
- [x] ET PHISHING Linkedin Phishing Landing 2018-08-30
- [x] ET PHISHING Generic PhishKit Author Comment M1 2018-08-30
- [x] ET PHISHING Generic PhishKit Author Comment M3 2018-08-30
- [x] ET PHISHING Generic PhishKit Author Comment M5 2018-08-30
- [x] ET PHISHING Generic PhishKit Author Comment M7 2018-08-30
- [x] ET PHISHING Generic PhishKit Author Comment M9 2018-08-30
- [x] ET PHISHING Successful Generic Phish (set) 2018-09-21
- [x] ET PHISHING Successful Generic Phish (set) 2018-09-26
- [x] ET PHISHING Successful Generic .EDU.TW Phish (Legit Set)
- [ ] ET PHISHING Successful Generic Phish (set) 2018-10-10
- [x] ET PHISHING Request for Possible Common Brand Phishing Hosted on Legitimate Windows Service
- [x] ET PHISHING Successful Generic Phish (set) 2018-10-16
- [x] ET PHISHING Successful Generic Phish (set) 2018-10-18
- [x] ET PHISHING Successful Generic Phish (set) 2018-10-22
- [x] ET PHISHING Possible Successful Generic Phish to .cf Domain 2018-10-23
- [x] ET PHISHING Possible Successful Generic Phish to .gq Domain 2018-10-23
- [x] ET PHISHING Successful Generic Phish to zap-webspace.com Webhost 2018-10-25

- [x] ET PHISHING Successful Cryptocurrency Exchange Phish (set) 2018-10-25
- [x] ET PHISHING Suspicious Fake Login - Possible Phishing - 2018-12-31
- [x] ET PHISHING Suspicious Generic Login - Possible Successful Phish 2019-01-02
- [x] ET PHISHING Successful Generic .EDU.CO Phish (Legit Set)
- [x] ET PHISHING Possible Successful Generic Phish (set) 2019-02-13
- [x] ET PHISHING Possible Successful Generic Phish (set) 2019-02-13
- [x] ET PHISHING Suspicious SSN Parameter in HTTP POST - Possible Phishing
- [x] ET PHISHING Possible Successful Generic Phish (set) 2019-03-06
- [x] ET PHISHING Possible Successful Phish - Password Submitted to *.000webhostapp.com
- [x] ET PHISHING Request for Possible Binance Phishing Hosted on Github.io
- [x] ET PHISHING Request for Possible Ebay Phishing Hosted on Github.io
- [x] ET PHISHING Request for Possible Account Phishing Hosted on Github.io
- [x] ET PHISHING Request for Possible Outlook Phishing Hosted on Github.io
- [x] ET PHISHING Request for Possible Docusign Phishing Hosted on Github.io
- [x] ET PHISHING Request for Possible Microsoft Phishing Hosted on Github.io
- [x] ET PHISHING Successful Generic Phish 2019-04-30 (set)
- [x] ET PHISHING Cloned EWE Telecom Page - Possible Phishing Landing
- [x] ET PHISHING Cloned ATB Bank Online Page - Possible Phishing Landing
- [x] ET PHISHING Cloned CIBC Bank Page - Possible Phishing Landing M1
- [x] ET PHISHING Cloned Instagram Page - Possible Phishing Landing M1
- [x] ET PHISHING Cloned Spotify Page - Possible Phishing Landing
- [x] ET PHISHING Cloned Westpac Bank Page - Possible Phishing Landing
- [x] ET PHISHING Cloned CIBC Bank Page - Possible Phishing Landing M2
- [x] ET PHISHING Cloned Scotiabank Page - Possible Phishing Landing
- [ ] ET PHISHING Cloned Cox Page - Possible Phishing Landing M2
- [x] ET PHISHING Cloned Telstra Page - Possible Phishing Landing
- [x] ET PHISHING Cloned Itscom Page - Possible Phishing Landing
- [x] ET PHISHING Cloned Bank of America Page - Possible Phishing Landing M2
- [x] ET PHISHING Cloned Microsoft Office Apps Page - Possible Phishing Landing
- [x] ET PHISHING Cloned Fidelity Page - Possible Phishing Landing
- [x] ET PHISHING Cloned Impots Gouv FR Page - Possible Phishing Landing
- [x] ET PHISHING Cloned Dropbox Page - Possible Phishing Landing
- [x] ET PHISHING Cloned ABSA Bank Page - Possible Phishing Landing
- [x] ET PHISHING Cloned Telekom / Tmobile Page - Possible Phishing Landing
- [x] ET PHISHING Cloned Google Tools Page - Possible Phishing Landing
- [x] ET PHISHING Cloned Discover Page - Possible Phishing Landing
- [x] ET PHISHING Cloned NAB Page - Possible Phishing Landing
- [ ] ET PHISHING Generic Miarroba Phishing Landing
- [x] ET PHISHING Generic Goth Phishing Landing
- [x] ET PHISHING Successful France Ministry of Action and Public Accounts Phish 2019-07-04
- [x] ET PHISHING Successful Generic Miarroba Phish 2019-07-11
- [x] ET PHISHING Possible Protonmail Phishing Domain in DNS Query
- [x] ET PHISHING Possible Protonmail Phishing Domain in DNS Query
- [x] ET PHISHING Possible Protonmail Phishing Domain in DNS Query
- [x] ET PHISHING Generic Xbalti Phishing Landing 2018-11-26
- [x] ET PHISHING Apple Phishing Redirect 2019-01-02
- [x] ET PHISHING Possible Successful Generic Phish to .icu Domain 2019-02-06
- [x] ET PHISHING Successful Generic .EDU.BR Phish (Legit Set)
- [x] ET PHISHING Possible Successful Generic Phish (set) 2019-02-13
- [x] ET PHISHING Possible Successful Generic Phish (set) 2019-02-13
- [x] ET PHISHING Suspicious CVV Parameter in HTTP POST - Possible Phishing
- [x] ET PHISHING PirateBay Phish - Possibly PirateMatryoshka Related
- [x] ET PHISHING Successful Generic Phish (set) 2019-04-12
- [x] ET PHISHING Request for Possible Paypal Phishing Hosted on Github.io
- [x] ET PHISHING Request for Possible Webmail Phishing Hosted on Github.io
- [x] ET PHISHING Request for Possible Office Phishing Hosted on Github.io
- [x] ET PHISHING Request for Possible DHL Phishing Hosted on Github.io
- [x] ET PHISHING Request for Possible Adobe Phishing Hosted on Github.io
- [x] ET PHISHING Request for Possible Facebook Phishing Hosted on Github.io
- [x] ET PHISHING Successful Generic Phish (set) 2019-05-21
- [x] ET PHISHING Cloned La Banque Postale FR Page - Possible Phishing Landing
- [x] ET PHISHING Cloned RBC Royal Bank Page - Possible Phishing Landing
- [x] ET PHISHING Cloned ABSA Bank Page - Possible Phishing Landing
- [x] ET PHISHING Cloned Instagram Page - Possible Phishing Landing M2
- [x] ET PHISHING Cloned ADP Page - Possible Phishing Landing
- [x] ET PHISHING Cloned Simplii Page - Possible Phishing Landing
- [x] ET PHISHING Cloned Chase Page - Possible Phishing Landing
- [x] ET PHISHING Cloned Cox Page - Possible Phishing Landing M1
- [x] ET PHISHING Cloned Comcast / Xfinity Page - Possible Phishing Landing
- [x] ET PHISHING Cloned Comcast / Xfinity Page - Possible Phishing Landing
- [x] ET PHISHING Cloned Bank of America Page - Possible Phishing Landing M1
- [x] ET PHISHING Cloned Bank of America Page - Possible Phishing Landing M3
- [x] ET PHISHING Cloned Telekom / Tmobile Page - Possible Phishing Landing
- [x] ET PHISHING Cloned Societe Generale FR Page - Possible Phishing Landing
- [x] ET PHISHING Cloned Godaddy Page - Possible Phishing Landing
- [x] ET PHISHING Cloned American Express Page - Possible Phishing Landing
- [x] ET PHISHING Cloned Match Dating Page - Possible Phishing Landing
- [x] ET PHISHING Cloned South State Bank Page - Possible Phishing Landing
- [x] ET PHISHING Cloned Yahoo Page - Possible Phishing Landing
- [x] ET PHISHING Cloned Linkedin Page - Possible Phishing Landing
- [x] ET PHISHING Cloned Ziggo NL Page - Possible Phishing Landing
- [x] ET PHISHING Possible Phishing Landing - Zeus365 Encoding
- [x] ET PHISHING SSL/TLS Certificate Observed (Lucy Phishing Awareness Default Certificate)
- [x] ET PHISHING France Ministry of Action and Public Accounts Phish Landing
- [x] ET PHISHING Successful Generic Adobe Phish 2019-07-29
- [x] ET PHISHING Possible Protonmail Phishing Domain in DNS Query
- [x] ET PHISHING Possible Protonmail Phishing Domain in DNS Query
- [x] ET PHISHING Possible Protonmail Phishing Domain in DNS Query

- [x] ET PHISHING Possible Protonmail Phishing Domain in DNS Query
- [x] ET PHISHING Possible Protonmail Phishing Domain in DNS Query
- [x] ET PHISHING Possible Protonmail Phishing Domain in DNS Query
- [x] ET PHISHING Possible Protonmail Phishing Domain in DNS Query
- [x] ET PHISHING Possible Phishing Landing Obfuscation 2016-03-17
- [x] ET PHISHING Successful Apple Phish (set) 2016-03-01
- [x] ET PHISHING Successful My ADP Phish (set) 2017-02-16
- [x] ET PHISHING Generic XBALTI Phishing Landing
- [x] ET PHISHING Possible Successful Generic Phish (set) 2019-11-06
- [x] ET PHISHING Successful Generic Email Account Phish 2019-12-10
- [x] ET PHISHING Observed Malicious SSL Cert (Office365 Phish Landing Page 2020-01-09)
- [x] ET PHISHING Possible Glitch.me Phishing Domain
- [x] ET PHISHING Successful DHL Account Phish 2015-11-03
- [x] ET PHISHING Successful Mailbox Update Phish 2016-02-17
- [x] ET PHISHING Successful Generic Phish (302) 2016-12-16
- [x] ET PHISHING Successful DHL Phish (Meta HTTP-Equiv Refresh) 2017-02-08
- [x] ET PHISHING Successful Facebook Mobile Phish 2017-08-15
- [x] ET PHISHING Successful OX App Suite Phish 2017-10-12
- [x] ET PHISHING Successful Facebook Phish 2018-01-26
- [x] ET PHISHING Successful Fedex/DHL Phish 2018-10-22
- [x] ET PHISHING Successful Generic Personalized Phish 2019-02-13
- [x] ET PHISHING Successful Generic Personalized Phish 2019-03-11
- [x] ET PHISHING Successful Facebook Phish 2019-04-26
- [x] ET PHISHING Successful Generic Credit Card Information Phish 2019-06-04
- [x] ET PHISHING Successful Facebook Phish 2019-08-29
- [x] ET PHISHING Successful DHL Phish 2019-10-18
- [x] ET PHISHING Successful Microsoft Account Phish 2019-11-06
- [x] ET PHISHING Successful Facebook Phish 2020-01-10
- [x] ET PHISHING Successful Generic Credit Card Information Phish 2020-02-21
- [x] ET PHISHING Successful Generic Credit Card Information Phish 2020-02-21
- [x] ET PHISHING Successful Generic Credit Card Information Phish 2020-02-21
- [x] ET PHISHING Successful Generic Credit Card Information Phish 2020-02-25
- [x] ET PHISHING Successful Microsoft Account Phish 2020-03-04
- [x] ET PHISHING Successful World Health Organization COVID-19 Phish 2020-03-23
- [x] ET PHISHING UK GOV Identity Verification Phishing Landing
- [x] ET PHISHING Successful Colleagues Quarantined with COVID-19 Phish 2020-03-25
- [x] ET PHISHING Successful Airbnb COVID-19 Phish 2020-03-26
- [x] ET PHISHING Possible Successful COVID-19 Related Phish M2
- [x] ET PHISHING Successful Canada Revenue Agency COVID-19 Assistance Eligability (FR) Phish 2020-04-01
- [x] ET PHISHING Canada Revenue Agency COVID-19 Assistance Eligibility Phishing Landing 2020-04-01
- [x] ET PHISHING CDC Coronavirus Related Phishing Landing 2020-04-07
- [x] ET PHISHING GOV UK Possible COVID-19 Phish 2020-04-06
- [x] ET PHISHING OneDrive Phishing Landing 2020-04-10
- [x] ET PHISHING Spotify Phishing Landing 2020-04-14
- [x] ET PHISHING French Government COVID-19 Landing Page
- [x] ET PHISHING IRS COVID-19 Landing Page
- [ ] ET PHISHING Possible Successful Phish to ChangeIP Dynamic DNS Domain
- [x] ET PHISHING Possible Protonmail Phishing Domain in DNS Query
- [x] ET PHISHING Possible Protonmail Phishing Domain in DNS Query
- [x] ET PHISHING Possible Protonmail Phishing Domain in DNS Query
- [x] ET PHISHING Possible Protonmail Phishing Domain in DNS Query
- [x] ET PHISHING Successful Generic Phish (set) 2019-08-23
- [ ] ET PHISHING Successful Gmail Phish (set) 2016-09-12
- [x] ET PHISHING Successful Bank of America Phish (set) 2016-02-27
- [x] ET PHISHING Facebook Phishing Domain in DNS Lookup
- [x] ET PHISHING Possible Successful Generic Phish (set) 2019-11-06
- [x] ET PHISHING Successful Generic Phish (set) 2019-12-12
- [x] ET PHISHING Successful Generic Phish 2020-01-29 (set)
- [x] ET PHISHING Possible Successful Generic Phish Aug 31 2015
- [x] ET PHISHING Successful DHL Phish 2015-09-14
- [x] ET PHISHING Terse POST to Wordpress Folder - Probable Successful Phishing M2
- [x] ET PHISHING Microsoft Office Phishing Landing 2016-12-18
- [x] ET PHISHING Successful Generic Phish - Fake Loading Page 2017-08-03
- [x] ET PHISHING Successful Generic .EDU Phish Aug 17 2017
- [x] ET PHISHING Successful Generic 000webhostapp.com Phish 2017-10-27
- [x] ET PHISHING Successful Generic Personalized Phish 2018-09-27 M2
- [x] ET PHISHING Successful Microsoft Account Phish 2019-01-29
- [x] ET PHISHING Successful Generic Mailbox Phish 2019-03-07
- [x] ET PHISHING Successful Facebook Phish 2019-04-12
- [ ] ET PHISHING Successful Interac Phish 2019-05-15
- [x] ET PHISHING Successful Generic Credit Card Information Phish 2019-08-02
- [x] ET PHISHING Successful Facebook Phish 2019-08-29
- [x] ET PHISHING Successful Generic Credit Card Information Phish 2019-11-04
- [x] ET PHISHING Successful Apple Phish 2019-12-18
- [x] ET PHISHING Successful Generic Credit Card Information Phish 2020-01-27
- [x] ET PHISHING Successful Generic Credit Card Information Phish 2020-02-21
- [x] ET PHISHING Successful Generic Credit Card Information Phish 2020-02-21
- [x] ET PHISHING Successful Generic Credit Card Information Phish 2020-02-21
- [x] ET PHISHING Successful Microsoft Office Phish 2020-02-26
- [x] ET PHISHING Fake World Health Organization COVID-19 Portal 2020-03-20
- [x] ET PHISHING Successful NHS Webmail Phish 2020-03-23
- [x] ET PHISHING Common Unhidebody Function Observed in Phishing Landing
- [x] ET PHISHING Successful Airbnb COVID-19 Phish 2020-03-25
- [x] ET PHISHING Possible Successful COVID-19 Related Phish M1
- [x] ET PHISHING Successful Canada Revenue Agency COVID-19 Assistance Eligability Phish 2020-04-01
- [x] ET PHISHING Canada Revenue Agency COVID-19 Assistance Eligibility Phishing Landing 2020-04-01
- [x] ET PHISHING Possible Successful CDC Coronavirus Related Phish 2020-04-07
- [x] ET PHISHING GOV UK Possible COVID-19 Phish 2020-04-06
- [x] ET PHISHING OneDrive Phishing Landing 2020-04-10
- [x] ET PHISHING Instagram Phishing Landing 2020-04-10
- [x] ET PHISHING 16Shop Phishing Kit Accessed on External Compromised Server
- [x] ET PHISHING NHS Gov UK COVID-19 Landing Page
- [ ] ET PHISHING Possible Successful Phish to NOIP DynDNS Domain
- [ ] ET PHISHING Possible Successful Phish to Afraid.org Top 100 Dynamic DNS Domain

- ET PHISHING Lucy Security - Phishing Landing Page M1
- ET PHISHING Common Form POST - CenturyLink Phishing Landing 2020-06-11
- ET PHISHING Generic T.Goe Phishing Landing
- ET PHISHING Common Form POST - Instagram Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - Facebook Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - Chase Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - Cox Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - SunTrust Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - M&T Bank Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - Paypal Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - Instagram Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - VK Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - Chase Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - Netease Webmail Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - Microsoft Account Phishing Landing 2020-06-11
- ET PHISHING Chalbhai Phishing Landing 2020-06-22
- ET PHISHING Successful Wombat Phishing Test
- ET PHISHING Possible Successful Generic Phish to .ma Domain 2020-07-15
- ET PHISHING Successful Generic Redeye Phish 2020-07-24
- ET PHISHING Generic Phishing Panel Accessed on Internal Server
- ET PHISHING Possible Phishing Landing Hosted on CodeSandbox.io M2
- ET PHISHING Possible Phishing Landing Hosted on CodeSandbox.io M4
- ET PHISHING Generic Phishing Panel Accessed on External Server
- ET PHISHING Instagram Fake Copyright Infringement Hosted on 000webhostapp
- ET PHISHING Observed Let's Encrypt Certificate containing Instagram
- ET PHISHING Generic Financial Phone Support Scam/Phishing Landing M1
- ET PHISHING Possible Sucessful Generic Phish (set) 2020-08-04
- ET PHISHING Successful Paxful Cryptocurrency Wallet Phish 2020-08-17
- ET PHISHING GET Request to Appspot Hosting (set)
- ET PHISHING Outlook Web App Phishing Landing on Appspot Hosting
- ET PHISHING Outlook Webapp Phishing Landing on Appspot Hosting
- ET PHISHING OneDrive Phishing Landing on Appspot Hosting
- ET PHISHING Microsoft Account Phishing Landing on Appspot Hosting
- ET PHISHING Possible Webmail Phishing Landing Utilizing Clearbit
- ET PHISHING GET Request to Googleapis Hosting (set)
- ET PHISHING Generic Phishing Panel Accessed on Internal Server
- ET PHISHING Zimbra Phishing Landing on Appspot Hosting
- ET PHISHING Possible Phishing Landing Hosted on CodeSandbox.io M6
- ET PHISHING Docusign Phishing Landing Hosted via Weebly
- ET PHISHING Generic Phishing Landing Hosted via Weebly
- ET PHISHING Instagram Phishing Landing 2020-10-13
- ET PHISHING Successful Generic Phish (set) 2020-06-10
- ET PHISHING Common Form POST - Chase Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - SunTrust Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - Facebook Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - Webmail Mini Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - Yahoo Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - Linkedin Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - Whatsapp/Facebook Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - Yahoo Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - Multibrand Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - SunTrust Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - Possible Generic Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - Instagram Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - Paypal Phishing Landing 2020-06-11
- ET PHISHING Common Form POST - Yahoo Phishing Landing 2020-06-11
- ET PHISHING Lucy Security - Successful Phish
- ET PHISHING T-Mobile Phishing Landing
- ET PHISHING Possible Successful Phish - Saved Website Comment Observed
- ET PHISHING Generic Phishing Panel Accessed on External Server
- ET PHISHING Possible Phishing Landing Hosted on CodeSandbox.io M1
- ET PHISHING Possible Phishing Landing Hosted on CodeSandbox.io M3
- ET PHISHING Possible Phishing Landing Captcha Check
- ET PHISHING Generic Phishing Panel Accessed on Internal Server
- ET PHISHING Possible Phishing Script Hosted on 000webhostapp
- ET PHISHING Generic Webmail Phishing Landing
- ET PHISHING Generic Financial Phone Support Scam/Phishing Landing M2
- ET PHISHING Possible Generic Microsoft Hosted Phishing Landing M2
- ET PHISHING Possible Successful Credential Phish - Form submitted to submit-form Form Hosting
- ET PHISHING Microsoft Account Phishing Landing on Appspot Hosting
- ET PHISHING Microsoft Account Phishing Landing on Appspot Hosting
- ET PHISHING Linkedin Phishing Landing on Appspot Hosting
- ET PHISHING Outlook Web App Phishing Landing on Appspot Hosting
- ET PHISHING Adobe Shared Document Phishing Landing on Appspot Hosting
- ET PHISHING Fedex Phishing Landing on Appspot Hosting
- ET PHISHING Generic Phishing Panel Accessed on External Server
- ET PHISHING Caixa Phishing Landing
- ET PHISHING Possible Phishing Landing Hosted on CodeSandbox.io M5
- ET PHISHING Mailgun Phishing Landing
- ET PHISHING Generic Phishing Landing Hosted via Weebly
- ET PHISHING Generic Phishing Landing Hosted via Weebly
- ET PHISHING Amazon Phishing Landing 2020-10-13

- [x] ET PHISHING Possible Instagram Phishing Domain
- [x] ET PHISHING Chase Phish Landing 2020-10-13
- [x] ET PHISHING Possible Successful Generic Windows.net Hosted Phish 2020-10-14
- [x] ET PHISHING Apple Phishing Panel Accessed on Internal Server
- [x] ET PHISHING Outlook Phishing Landing 2020-10-23
- [x] ET PHISHING Generic Custom Logo Phishing Landing
- [x] ET PHISHING Multibank Captcha Phishing Landing
- [x] ET PHISHING Cloned IRS Page - Possible Phishing Landing
- [x] ET PHISHING Generic Personalized Google Firebase Hosted Phishing Landing
- [x] ET PHISHING Generic Personalized Google Firebase Hosted Phishing Landing
- [x] ET PHISHING Cloned Instagram Page - Possible Phishing Landing M3
- [x] ET PHISHING Generic Tombol Microsoft Account Phishing Landing 2020-12-16
- [x] ET PHISHING Apple Phishing Panel Accessed on Internal Compromised Server
- [x] ET PHISHING Suspicious TikTok Domain Request - Possible Phishing or Scam
- [ ] ET PHISHING Terse POST to Wordpress Folder - Probable Successful Phishing M5
- [x] ET PHISHING Successful Paypal Phish M1 Dec 8 2015
- [x] ET PHISHING Suspicious Redirect - Possible Phishing May 25 2016
- [x] ET PHISHING Successful Dynamic Folder Phishing Oct 06 2016
- [x] ET PHISHING Terse POST to Wordpress Folder - Probable Successful Phishing M4
- [x] ET PHISHING Successful Chase Phish Dec 29 2016
- [x] ET PHISHING Successful Chase Phish M1 Aug 15 2017
- [x] ET PHISHING Successful Paypal Phish M2 Sep 15 2017
- [x] ET PHISHING Terse POST to Wordpress Folder - Probable Successful Phishing M7
- [x] ET PHISHING Successful Bank of America Phish 2015-10-02
- [x] ET PHISHING Yahoo Account Phish Landing 2015-10-23
- [x] ET PHISHING Outlook WebApp Phish Landing 2015-11-05
- [x] ET PHISHING Excel Online Phish Landing 2015-12-08
- [x] ET PHISHING PHOEN!X Phish Loading Page 2015-12-29
- [x] ET PHISHING Fake Webmail Account Phishing Landing 2015-09-10
- [x] ET PHISHING Obfuscated Phishing Landing 2015-11-05
- [x] ET PHISHING Wire Transfer Phishing Landing 2015-11-19
- [x] ET PHISHING Outlook Webmail Phishing Landing 2015-11-21
- [x] ET PHISHING cPanel Phishing Landing 2015-12-01
- [x] ET PHISHING Anonisma Paypal Phishing Loading Page 2015-12-29
- [x] ET PHISHING Apple Phishing Landing 2015-07-27
- [x] ET PHISHING Possible Successful Apple Phish 2015-07-27
- [x] ET PHISHING Google Drive Phishing Landing 2015-07-28
- [x] ET PHISHING Possible Fedex Phishing Landing 2015-07-28
- [x] ET PHISHING Possible Apple Store Phish Landing 2015-07-30
- [x] ET PHISHING Possible Apple Store Phish Landing 2015-07-30
- [x] ET PHISHING Successful Survey Credential Phish 2015-08-12
- [x] ET PHISHING Mailbox Renewal Phish Landing 2015-08-14
- [x] ET PHISHING Successful Commonwealth Bank Phish Fake Error Page 2015-08-20
- [x] ET PHISHING Successful Horde Webmail Phish 2015-08-21
- [x] ET PHISHING DHL Phish Landing Page 2015-10-17
- [x] ET PHISHING Successful Vmware/Zimbra Phish 2015-09-28
- [x] ET PHISHING Successful Paypal Phish 2015-10-28
- [x] ET PHISHING Successful Paypal Phish 2015-11-03 M3
- [x] ET PHISHING Google Drive Phishing Landing 2015-11-06
- [x] ET PHISHING Successful Adobe Shared Document Phish 2015-11-14
- [x] ET PHISHING Microsoft Account Login Hosted on Firebasestorage
- [x] ET PHISHING Possible Successful Generic Web.App Hosted Phish 2020-10-14
- [x] ET PHISHING Suntrust Captcha Phishing Landing
- [x] ET PHISHING Apple Phishing Panel Accessed on External Server
- [x] ET PHISHING Generic Custom Logo Phishing Landing
- [x] ET PHISHING Generic Custom Logo Phishing Landing
- [x] ET PHISHING Suspected Appspot Hosted Phishing Domain
- [x] ET PHISHING Generic Google Firebase Hosted Phishing Landing
- [x] ET PHISHING Generic Personalized Google Firebase Hosted Phishing Landing
- [x] ET PHISHING Possible Successful Generic Phish (set) 2020-11-19
- [x] ET PHISHING Chase Phish Landing 2020-11-26
- [x] ET PHISHING Successful Clydesdale Bank Phish 2020-12-30
- [x] ET PHISHING Apple Phishing Panel Accessed on External Compromised Server
- [x] ET PHISHING Possible Instagram Phishing or Scam Landing Page
- [x] ET PHISHING Possible Successful Credential Phish Oct 1 2015
- [x] ET PHISHING Terse POST to Wordpress Folder - Probable Successful Phishing
- [x] ET PHISHING Terse POST to Wordpress Folder - Probable Successful Phishing M3
- [x] ET PHISHING Successful Dynamic Folder Phish Oct 07 2016
- [x] ET PHISHING Terse POST to Wordpress Folder - Probable Successful Phishing M6
- [x] ET PHISHING Successful Generic Phish (Meta HTTP-Equiv Refresh) Dec 29 2016
- [x] ET PHISHING Successful Paypal Phish M1 Sep 15 2017
- [x] ET PHISHING Generic 302 Redirect to Phishing Landing
- [x] ET PHISHING Successful Outlook Webmail Account Phish 2015-09-02
- [x] ET PHISHING Successful Paypal Account Phish 2015-10-16
- [x] ET PHISHING Successful Zimbra Phish 2015-11-03
- [x] ET PHISHING Outlook WebApp Phish Landing 2015-11-05
- [x] ET PHISHING PHOEN!X Apple Phish Landing Page 2015-12-29
- [x] ET PHISHING Base64 HTTP URL Refresh - Common Phish Landing Obfuscation 2016-01-01
- [x] ET PHISHING Phishing Fake Document Loading Error 2015-10-01
- [x] ET PHISHING Metro Document Phishing Landing 2015-11-17
- [x] ET PHISHING Google Drive Phishing Landing 2015-11-20
- [x] ET PHISHING Successful Outlook Webmail Phishing 2015-11-21
- [x] ET PHISHING Anonisma Phishing Landing 2015-12-01
- [x] ET PHISHING Possible Google Drive Phishing Landing 2015-07-13
- [x] ET PHISHING Possible Successful Apple Phish 2015-07-27
- [x] ET PHISHING Possible Successful Apple Phish 2015-07-27
- [x] ET PHISHING Google Drive Phishing Landing 2015-07-28
- [x] ET PHISHING Possible Apple Store Phish Landing 2015-07-30
- [x] ET PHISHING Possible Apple Store Phish Landing 2015-07-30
- [x] ET PHISHING Successful Generic Credential Phish - Loading Messages 2015-08-12
- [x] ET PHISHING Cloud Drive Phish Landing 2015-08-12
- [x] ET PHISHING Apple ID Phishing Landing 2015-08-19
- [x] ET PHISHING Horde Webmail Phishing Landing 2015-08-21
- [x] ET PHISHING Successful Fake Webmail Quota Phish 2015-09-10
- [x] ET PHISHING Successful Battle.net Phish 2015-09-22
- [x] ET PHISHING Successful Outlook Web App Phish 2015-10-15
- [x] ET PHISHING Successful Paypal Phish 2015-10-28 3
- [x] ET PHISHING Successful Paypal Phish 2015-11-03 M4
- [x] ET PHISHING Adobe Shared Document Phish Landing 2015-11-14
- [x] ET PHISHING DHL Phish Landing 2015-11-14

- [x] ET PHISHING Apple Account Phishing Landing 2015-11-18
- [x] ET PHISHING Anonisma AES Crypto Observed in Javascript - Possible Phishing Landing 2015-12-29
- [x] ET PHISHING Possible Successful Docusign Phish 2015-07-27
- [x] ET PHISHING Successful Phish Fake Document Loading Error 2015-07-27
- [x] ET PHISHING Possible Successful Google Drive Phish M1 2015-07-28
- [x] ET PHISHING Possible Successful Google Drive Phish 2015-07-28
- [x] ET PHISHING Possible Successful Fedex Phish 2015-07-28
- [x] ET PHISHING Possible Successful Apple Phish 2015-07-30
- [x] ET PHISHING Possible Successful Apple Phish 2015-07-31
- [x] ET PHISHING Possible Successful Generic Phish 2015-07-31
- [x] ET PHISHING Possible Successful AirCanada Phish 2015-08-06
- [x] ET PHISHING Successful Email Credential Phish 2015-08-12
- [x] ET PHISHING Successful Canada Revenue Agency Phish 2015-08-18
- [x] ET PHISHING Successful Canada Revenue Agency Phish 2015-08-18
- [x] ET PHISHING Successful Amazon Account Phish 2015-08-21
- [x] ET PHISHING Successful Amazon Account Phish 2015-08-21
- [x] ET PHISHING Successful Adobe Online Account Phish 2015-08-21
- [x] ET PHISHING Successful BBVA Compass Account Phish 2015-08-21
- [x] ET PHISHING Successful Carribean International Bank Account Phish 2015-08-25
- [x] ET PHISHING Successful Adobe Phish 2015-08-31
- [x] ET PHISHING Successful Account Update Phish 2015-09-01
- [x] ET PHISHING Successful EDF Account Phish 2015-09-01
- [x] ET PHISHING Successful Amazon Phish 2015-09-22
- [x] ET PHISHING Successful Chase Phish 2015-09-24
- [x] ET PHISHING Successful Chase Phish 2015-09-24
- [x] ET PHISHING Successful Chase Phish 2015-09-24
- [x] ET PHISHING Successful Adobe Online Phish 2015-09-30
- [x] ET PHISHING Successful Bank of America Phish M2 2015-10-02
- [x] ET PHISHING Successful Yahoo Credential Phish 2015-10-03
- [x] ET PHISHING Successful Alibaba Credential Phish 2015-10-05
- [x] ET PHISHING Successful Blackboard Account Phish 2015-10-08
- [x] ET PHISHING Successful AOL Phish 2015-10-09
- [x] ET PHISHING Successful Apple Phish 2015-10-23
- [x] ET PHISHING Successful Bank of America Phish 2015-10-29
- [x] ET PHISHING Successful Paypal Phish 2015-10-29
- [x] ET PHISHING Successful Bank of Scotland Phish M1 2015-11-05
- [x] ET PHISHING Successful Amazon Phish 2015-11-07
- [x] ET PHISHING Data Submitted to Weebly.com - Possible Phishing
- [x] ET PHISHING Weebly Phishing Landing Observed 2015-11-10
- [x] ET PHISHING Google Drive Phishing Landing 2015-11-17
- [x] ET PHISHING Successful Adobe Shared Document Phishing 2015-11-20
- [x] ET PHISHING Successful Bank of America Phish 2015-11-21
- [x] ET PHISHING Successful SFR Phishing 2015-11-24
- [x] ET PHISHING Anonisma Phishing CSS 2015-12-01
- [x] ET PHISHING Successful Apple Phish M1 2015-12-02
- [x] ET PHISHING Successful iCloud Phish 2015-12-02
- [x] ET PHISHING Successful Wildblue/CenturyLink Phish 2015-12-08
- [x] ET PHISHING Successful Paypal Phish 2015-12-05
- [x] ET PHISHING Successful Google Docs Phish 2015-12-09
- [x] ET PHISHING Successful Dropbox Phish 2015-12-10
- [x] ET PHISHING Successful Chase Phish 2015-12-22
- [x] ET PHISHING Successful Paypal Phish 2015-12-24 M1
- [x] ET PHISHING Anonisma Phishing CSS 2015-12-29
- [x] ET PHISHING Successful Anonisma Paypal Phish 2015-12-29
- [x] ET PHISHING Successful PHOEN!X Apple Phish M2 2015-12-29
- [x] ET PHISHING Successful Mailbox Renew Phish 2015-08-14
- [x] ET PHISHING Successful Apple ID Phish 2015-08-18
- [x] ET PHISHING Successful Wells Fargo Account Phish 2015-08-18
- [x] ET PHISHING Successful Commonwealth Bank Phish 2015-08-20
- [x] ET PHISHING Successful Amazon Account Phish M3 2015-08-21
- [x] ET PHISHING Successful Impots.gouv.fr Phish M1 2015-08-21
- [x] ET PHISHING Successful Impots.gouv.fr Phish M2 2015-08-21
- [x] ET PHISHING Successful OWA Account Phish 2015-08-21
- [x] ET PHISHING Successful Horde Webmail Phish 2015-08-21
- [x] ET PHISHING Successful Facebook Phish 2015-08-27
- [x] ET PHISHING Successful Woodforest Bank Phish M1 2015-08-31
- [x] ET PHISHING Successful SFR Account Phish 2015-09-01
- [x] ET PHISHING Successful Generic Phish - Phone Number 2015-09-02
- [x] ET PHISHING Successful Google Drive Phish Sept 1 M2 2015-09-02
- [x] ET PHISHING Successful Webmail Account Phish 2015-09-02
- [x] ET PHISHING Successful Telstra Phish M1 2015-09-05
- [x] ET PHISHING Successful USAA Phish 2015-09-05
- [x] ET PHISHING Successful ViewDocsOnline Phish 2015-09-15
- [x] ET PHISHING Successful LinkedIn Phish 2015-09-17
- [x] ET PHISHING Successful DHL Phish 2015-09-17
- [x] ET PHISHING Successful Google Drive Phish 2015-09-22
- [x] ET PHISHING Successful DHL Phish 2015-09-30
- [x] ET PHISHING Successful Phish Gmail Recovery Information 2015-10-01
- [x] ET PHISHING Successful Mailbox Update Credential Phish 2015-10-02
- [x] ET PHISHING Successful Generic Credential Phish 2015-10-03
- [x] ET PHISHING Successful Webmail Update Phish 2015-10-08
- [x] ET PHISHING Successful Samsung Portal Phish 2015-10-13
- [x] ET PHISHING Successful Paypal Account Phish 2015-10-16
- [x] ET PHISHING Successful USAA Phish 2015-10-20
- [x] ET PHISHING Successful Zimbra Account Phish 2015-10-23
- [x] ET PHISHING Successful Paypal Phish 2015-10-23
- [x] ET PHISHING Successful Paypal Phish 2015-10-23
- [x] ET PHISHING Successful Paypal Phish 2015-10-23
- [x] ET PHISHING Successful Paypal Phish 2015-10-23
- [x] ET PHISHING Successful Docusign Phish 2015-10-28
- [x] ET PHISHING Successful IBC Bank Phish 2015-10-29
- [x] ET PHISHING Successful Zimbra Phish 2015-10-30
- [x] ET PHISHING Successful NatWest Bank Phish 2015-11-03
- [x] ET PHISHING Successful Chase Phish 2015-11-03
- [x] ET PHISHING Successful Dropbox Phish 2015-11-04
- [x] ET PHISHING Successful UPS Phish 2015-11-05
- [x] ET PHISHING Successful LCL Bank Phish 2015-11-05
- [x] ET PHISHING Successful Bank of America Phish 2015-11-06
- [x] ET PHISHING Successful DHL Phish 2015-11-14
- [x] ET PHISHING Successful Tradekey Phish 2015-11-19
- [x] ET PHISHING Successful Hinet Phish 2015-11-19
- [x] ET PHISHING Successful Excel Online Phish 2015-12-08
- [x] ET PHISHING Successful Paypal Phish 2015-12-08 M3
- [x] ET PHISHING Anonisma Paypal Phishing Uri Structure 2015-12-29
- [x] ET PHISHING Successful Generic L33bo Phish - URI Contents (set)
- [x] ET PHISHING Possible Successful Generic Phish (set) 2017-12-19
- [x] ET PHISHING Possible Successful Generic Phish (set) 2017-12-20
- [x] ET PHISHING Successful Generic Phish 2018-02-26 (set)
- [x] ET PHISHING Successful Generic Phish (set) 2018-03-08
- [x] ET PHISHING Possible Successful Generic Phish (set) 2019-01-30
- [x] ET PHISHING Successful Generic Phish (set) 2019-05-14
- [x] ET PHISHING Successful Generic Phish (set) 2019-07-09
- [x] ET PHISHING Successful Generic Phish (set) 2020-08-07
- [x] ET PHISHING Possible Successful Generic Phish (set) 2020-09-03
- [x] ET PHISHING Possible Successful Generic Phish (set) 2020-09-29
- [x] ET PHISHING Generic Credential Phish 2020-07-27 (set)
- [x] ET PHISHING Possible Successful Generic Phish (set) 2021-03-08
- [x] ET PHISHING Possible Successful Phish (Google/Dropbox/Netflix) 2015-07-11
- [x] ET PHISHING Successful Wells Fargo Account Phish 2015-08-14
- [x] ET PHISHING Successful Outlook Phish 2015-08-18
- [x] ET PHISHING Successful Key Bank Phish M1 2015-08-20
- [x] ET PHISHING Successful Key Bank Phish M2 2015-08-20
- [x] ET PHISHING Successful Wells Fargo/CIBC Bank Phish M1 2015-08-25
- [x] ET PHISHING Successful Webmail Phish 2015-08-27

- [x] ET PHISHING Successful Google Drive Phish 2015-09-04
- [x] ET PHISHING Successful Chase Phish 2015-09-23
- [x] ET PHISHING APT SWC PluginDetect Landing Cookie 2015-10-15
- [x] ET PHISHING Successful Gmail Phish 2015-11-05
- [x] ET PHISHING Successful Natwest Bank Phish 2015-11-21
- [x] ET PHISHING Successful Wells Fargo Phish M2 2015-11-21
- [x] ET PHISHING Successful Wildblue Phishing M1 2015-11-24
- [x] ET PHISHING Successful Xoom Phishing 2015-11-24
- [x] ET PHISHING Successful Excel Online Phish 2015-11-26
- [x] ET PHISHING Successful Chase Phish M2 2015-12-01
- [x] ET PHISHING Successful Apple Phish M2 2015-12-02
- [x] ET PHISHING Successful Dropbox Phish M2 2015-12-10
- [x] ET PHISHING Successful US Bank Phish M2 2015-12-22
- [x] ET PHISHING Successful Gmail Account Update Phish 2016-05-10
- [x] ET PHISHING Generic Redirector Phishing Landing 2021-03-10
- [x] ET PHISHING Generic Custom Logo Phishing Landing 2021-03-10
- [x] ET PHISHING Generic NewInjection Phishing Landing 2021-03-10
- [x] ET PHISHING Successful Adobe Phish M3 2016-07-11
- [x] ET PHISHING Base64 Data URI Javascript Refresh - Possible Phishing Landing
- [x] ET PHISHING Successful Wells Fargo Phish Loading Page 2016-01-07
- [x] ET PHISHING Webmail Update Phishing Landing 2016-01-15
- [x] ET PHISHING Successful Paypal Phish 2016-01-15 M2
- [x] ET PHISHING Phishing Landing via Webeden.co.uk (set) 2016-01-22
- [x] ET PHISHING Canada Revenue Agency Phishing Landing 2016-01-25
- [x] ET PHISHING USPS Phishing Landing 2016-02-10
- [x] ET PHISHING Google Maps Phishing Landing 2016-02-17
- [x] ET PHISHING USAA Phishing Landing 2016-02-26
- [x] ET PHISHING Apple Phishing Landing 2016-03-01 M2
- [x] ET PHISHING Successful Apple Phishing 2016-03-01 M5
- [x] ET PHISHING Phishing Landing via MyFreeSites.com M2 2016-03-31
- [x] ET PHISHING Phishing Landing via Tripod.com M2 2016-03-31
- [x] ET PHISHING OWA Phishing Landing 2016-04-04 M2
- [x] ET PHISHING Adobe Online Document Phishing Landing M1 2016-04-25
- [x] ET PHISHING Successful Adobe Online Document Phish 2016-04-25
- [x] ET PHISHING Successful Citizenbank Phish 2016-05-24 M1
- [x] ET PHISHING Phishing Fake Mailbox Quota Increase Messages 2016-05-25
- [x] ET PHISHING Successful Paypal Phish 2016-05-26
- [x] ET PHISHING Generic Email Login Phishing Landing 2016-06-02
- [x] ET PHISHING DrSpam Phishing Landing CSS 2016-06-08
- [x] ET PHISHING Successful DrSpam Phish 2016-06-08 M2
- [x] ET PHISHING OneDrive Phishing Landing 2021-03-15
- [x] ET PHISHING Phishing Landing via Tripod.com Mar 31 M3
- [x] ET PHISHING Tripod/Lycos Form Submission - Possible Successful Phish
- [x] ET PHISHING Successful US Bank Phish 2016-06-09 M2
- [x] ET PHISHING Webmail Phishing Landing 2016-06-22
- [x] ET PHISHING Possible Phishing Data Submitted to yolasite.com
- [x] ET PHISHING Successful Mailbox Upgrade Phish 2016-06-27 M1
- [x] ET PHISHING Data Submitted to MyFreeSites.com - Possible Phishing
- [x] ET PHISHING Successful Hotmail Phish 2016-07-14
- [x] ET PHISHING Webmail Account Upgrade Phishing Landing 2016-07-15
- [x] ET PHISHING Webmail Account Upgrade Phishing Landing 2016-07-20
- [x] ET PHISHING Successful Wells Fargo Mobile Phish 2016-08-01 M2
- [x] ET PHISHING DHL/EMS Documents Phishing Landing 2016-08-10
- [x] ET PHISHING Possible Phishing Landing - Tectite Web Form Abuse
- [x] ET PHISHING Adobe Shared Document Phishing Landing Common CSS 2016-08-10
- [x] ET PHISHING Successful Phish OWA Credentials 2016-08-16
- [x] ET PHISHING Successful Telstra Phish M2 2015-09-05
- [x] ET PHISHING Successful Shipping Document Phish 2015-09-29
- [x] ET PHISHING Successful Paypal Phish M2 2015-11-03
- [x] ET PHISHING Successful Squirrelmail Phishing 2015-11-20
- [x] ET PHISHING Successful Wells Fargo Phish M1 2015-11-21
- [x] ET PHISHING Successful Outlook Webmail Phishing M2 2015-11-21
- [x] ET PHISHING Successful Wildblue Phishing M2 2015-11-24
- [x] ET PHISHING Successful Trademe Phish M3 2015-11-26
- [x] ET PHISHING Possible Base64 Obfuscated Phishing Landing 2015-11-30
- [x] ET PHISHING Successful Anonisma Phish 2015-12-01
- [x] ET PHISHING Successful Halifax Bank Phish M1 2015-12-10
- [x] ET PHISHING Successful US Bank Phish M1 2015-12-22
- [x] ET PHISHING Successful PHOEN!X Apple Phish M1 2015-12-29
- [x] ET PHISHING Microsoft Account Phishing Landing 2021-03-10
- [x] ET PHISHING Generic Encoded Phishing Landing 2021-03-10
- [x] ET PHISHING Generic NewInjection Phishing Landing 2021-03-10
- [x] ET PHISHING Successful WZ-REKLAMA Phish 2016-01-08
- [x] ET PHISHING Email Account Exceeded Quota Phishing Landing 2016-07-11
- [x] ET PHISHING Wells Fargo Phishing Landing 2016-01-07
- [x] ET PHISHING IRS Phishing Landing 2016-01-15
- [x] ET PHISHING Successful Paypal Phish M1 2016-01-19
- [x] ET PHISHING Successful Paypal Phish 2016-01-15 M3
- [x] ET PHISHING Phishing Landing via Webeden.co.uk M1 2016-01-22
- [x] ET PHISHING Navy Federal Credit Union Phishing Landing 2016-01-30
- [x] ET PHISHING Successful Mailbox Update Phish 2016-02-17 M2
- [x] ET PHISHING Possible Phishing Landing - Data URI Inline Javascript 2016-02-09
- [x] ET PHISHING Successful Apple Phishing 2016-03-01 M3
- [x] ET PHISHING Apple Phishing Landing 2016-03-01 M3
- [x] ET PHISHING Phishing Landing via MyFreeSites.com (set) 2016-03-31
- [x] ET PHISHING Phishing Landing via Tripod.com M1 2016-03-31
- [x] ET PHISHING Possible Successful Tripod.com Phish 2016-03-31
- [x] ET PHISHING Email System Manager Phishing Landing 2016-04-12
- [x] ET PHISHING Adobe Online Document Phishing Landing M2 2016-04-25
- [x] ET PHISHING Successful Craigslist Phish 2016-04-25
- [x] ET PHISHING Successful Citizenbank Phish 2016-05-24 M2
- [x] ET PHISHING Suspicious File Download Post-Phishing 2016-05-25
- [x] ET PHISHING Avast Phishing Landing 2016-06-02
- [x] ET PHISHING DrSpam Phishing Landing 2016-06-08
- [x] ET PHISHING Successful DrSpam Phish 2016-06-08 M1
- [x] ET PHISHING DHL Phishing Landing 2016-07-11
- [x] ET PHISHING Phishing Landing via Tripod.com (set) 2016-03-31
- [x] ET PHISHING Possible Websc Phishing Page 2016-02-05
- [x] ET PHISHING Successful US Bank Phish 2016-06-09 M1
- [x] ET PHISHING Email Termination Phishing Landing 2016-06-22
- [x] ET PHISHING Microsoft Encrypted Email Phishing Landing 2016-06-23
- [x] ET PHISHING Mailbox Upgrade Phishing Landing 2016-06-27
- [x] ET PHISHING Successful Mailbox Upgrade Phish 2016-06-27 M2
- [x] ET PHISHING Possible USAA Phishing Landing 2016-07-05
- [x] ET PHISHING Synchronize Email Account Phishing Landing 2016-07-15
- [x] ET PHISHING Successful Generic Webmail Account Phish 2016-07-15
- [x] ET PHISHING Successful Wells Fargo Mobile Phish 2016-08-01 M1
- [x] ET PHISHING Successful Wells Fargo Mobile Phish 2016-08-01 M3
- [x] ET PHISHING Suspicious Credential POST to FormBuddy.com - Possible Phishing Aug 10 2016
- [x] ET PHISHING Successful Tectite Web Form Submission - Possible Phishing
- [x] ET PHISHING Successful Gmail Phish M1 2016-08-12
- [x] ET PHISHING Adobe Phishing Landing M1 2016-08-16

- [x] ET PHISHING Successful Docusign Phish M1 2016-08-17
- [x] ET PHISHING Universal Webmail Phishing Landing 2016-08-19
- [x] ET PHISHING Blocked Email Account Phishing Landing 2016-08-23
- [x] ET PHISHING Targeted Office 365 Phishing Landing 2016-08-23
- [x] ET PHISHING Successful Yahoo Password Strength Phish M1 2016-08-24
- [x] ET PHISHING Successful Yahoo Password Strength Phish M2 2016-08-24
- [x] ET PHISHING Successful Chase Phish M1 2016-08-26
- [x] ET PHISHING Successful Chase Phish M4 2016-08-26
- [x] ET PHISHING Successful Paypal Phish 2016-08-30
- [x] ET PHISHING Successful CIBC Phish 2016-08-30
- [x] ET PHISHING DHL Phishing Landing 2016-08-31
- [x] ET PHISHING Adobe Shared Document Phishing Landing 2016-08-30
- [x] ET PHISHING Alibaba Phishing Landing 2016-08-31
- [x] ET PHISHING Data Submitted to Webeden.co.uk - Possible Phishing
- [x] ET PHISHING Successful Google Docs Phish 2016-09-01
- [x] ET PHISHING Successful Outlook Password Update Phish M2 2016-09-01
- [x] ET PHISHING Facebook Phishing Landing 2016-09-02
- [x] ET PHISHING Possible Phishing Landing via MoonFruit.com (set)
- [x] ET PHISHING Possible Phishing Landing via MoonFruit.com M2 2016-01-22
- [x] ET PHISHING Possible Phishing Landing via Moonfruit M2 2016-01-26
- [x] ET PHISHING Successful Chase Phish 2016-09-02
- [x] ET PHISHING Webmail Validator Phishing Landing 2016-09-02
- [x] ET PHISHING Successful Paypal Phish 2016-09-06
- [x] ET PHISHING Fedex Javascript Phishing Landing 2016-09-08
- [x] ET PHISHING Successful Paypal Phish 2016-09-09
- [x] ET PHISHING Successful SeniorPeopleMeet Phish M2 2016-09-14
- [x] ET PHISHING Successful Wells Fargo Phish M1 2016-09-16
- [x] ET PHISHING Successful US Bank Phish 2016-09-20
- [x] ET PHISHING Successful Apple Phish 2016-09-27
- [x] ET PHISHING Successful Dropbox Phish 2016-09-29
- [x] ET PHISHING Successful Facebook Phish M1 2016-09-30
- [x] ET PHISHING Successful Postbank Online Banking Phish M2 2016-09-30
- [x] ET PHISHING Possible Phishing Landing via Moonfruit M2 2016-10-03
- [x] ET PHISHING Successful Generic OWA Phish 2016-10-04
- [x] ET PHISHING Successful Amazon Phish M1 2016-10-05
- [x] ET PHISHING Successful Orange (FR) Phish 2016-10-06
- [x] ET PHISHING Successful DHL Phish 2016-10-07
- [x] ET PHISHING Successful Apple Phish (FR) M2 2016-10-07
- [x] ET PHISHING Successful Google Drive Phish 2016-10-11
- [x] ET PHISHING Phishing Landing via Webeden.net 2016-10-13
- [x] ET PHISHING Successful Paypal Phish M1 2016-10-17
- [x] ET PHISHING Successful Generic Webmail Phish 2016-10-21
- [x] ET PHISHING Successful Yahoo Phish 2016-10-25
- [x] ET PHISHING Successful Outlook Phish 2016-10-25
- [x] ET PHISHING Successful Chase Phish 2016-10-25
- [x] ET PHISHING Successful Office 365 Phish 2016-10-31
- [x] ET PHISHING Successful American Express Phish M2 2016-10-31
- [x] ET PHISHING Successful Paypal Phish 2016-10-31
- [x] ET PHISHING Successful Apple Phish M2 2016-11-15
- [x] ET PHISHING Successful Personalized Email Update Phish 2016-11-17
- [x] ET PHISHING Shared Document Base64 Phishing Landing 2016-01-20
- [x] ET PHISHING Successful Apple Phishing 2016-03-03
- [x] ET PHISHING Successful Google Drive Phish 2016-08-18
- [x] ET PHISHING Successful Google Drive Phish M1 2016-09-01
- [x] ET PHISHING Adobe Shared Document Phishing Landing 2016-08-19
- [x] ET PHISHING Possible Phishing Data Submitted to yolasite.com M2
- [x] ET PHISHING Successful Blocked Email Account Phish M2 2016-08-23
- [x] ET PHISHING Yahoo Password Strength Phishing Landing 2016-08-24
- [x] ET PHISHING Successful Team IPwned Phish 2016-08-24
- [x] ET PHISHING Google Drive Phishing Landing 2016-08-25
- [x] ET PHISHING Successful Chase Phish M3 2016-08-26
- [x] ET PHISHING Suspicious Yahoo Page - Possible Phishing Landing
- [x] ET PHISHING TeamIPwned/Hellion Phishing Landing 2016-08-30
- [x] ET PHISHING Successful Paypal Phish 2016-08-31
- [x] ET PHISHING Successful Dropbox Phish 2016-08-31
- [x] ET PHISHING Adobe Shared Document Phishing Landing M2 2016-08-31
- [x] ET PHISHING Outlook 365 Encrypted Email Phishing Landing M1 2016-08-31
- [x] ET PHISHING Data Submitted to Weebly.com - Possible Phishing
- [x] ET PHISHING Successful Outlook Password Update Phish M1 2016-09-01
- [x] ET PHISHING Successful Outlook Password Update Phish M3 2016-09-01
- [x] ET PHISHING Successful Facebook Phish 2016-09-02
- [x] ET PHISHING Possible Phishing Landing via MoonFruit.com M1 2016-01-22
- [x] ET PHISHING Possible Phishing Landing via MoonFruit.com M3 2016-01-22
- [x] ET PHISHING Successful Google Drive Phish 2016-09-02
- [x] ET PHISHING Successful Webmail Validator Phish M2 2016-09-02
- [x] ET PHISHING Account Update Phishing Landing 2016-09-06
- [x] ET PHISHING Suspicious Minimal HTTP Refresh to Googledrive.com - Possible Phishing
- [x] ET PHISHING Successful Microsoft Live Email Account Phish 2016-09-08
- [x] ET PHISHING Successful SeniorPeopleMeet Phish M1 2016-09-14
- [x] ET PHISHING Successful View Samples Phish 2016-09-09
- [x] ET PHISHING Successful Wells Fargo Phish M2 2016-09-16
- [x] ET PHISHING Successful Excel Phish 2016-09-26
- [x] ET PHISHING Successful FreeMobile (FR) Phish 2016-09-28
- [x] ET PHISHING Successful Apple Phish M1 2016-09-29
- [x] ET PHISHING Successful Postbank Online Banking Phish M1 2016-09-30
- [x] ET PHISHING Possible Phishing Landing via Moonfruit M1 2016-10-03
- [x] ET PHISHING Suspicious Byethost Phishing Redirect 2016-10-04
- [x] ET PHISHING Paypal Phishing Landing (DE) 2016-10-04
- [x] ET PHISHING Successful Paypal Phish M2 2016-10-05
- [x] ET PHISHING Successful Supplier Portal Phish 2016-10-07
- [x] ET PHISHING Successful Apple Phish (FR) M1 2016-10-07
- [x] ET PHISHING Successful Bank of America Phish M2 2016-10-10
- [x] ET PHISHING Successful Gmail Phish M2 2016-10-12
- [x] ET PHISHING Successful Yahoo Phish 2016-10-14
- [x] ET PHISHING Successful DHL Phish 2016-10-18
- [x] ET PHISHING Successful Wells Fargo Phish 2016-10-21
- [x] ET PHISHING Successful Banco do Brasil Phish M2 2016-10-25
- [x] ET PHISHING Successful Apple ID Phish 2016-10-25
- [x] ET PHISHING Successful 163.com Email Account Phish 2016-10-26
- [x] ET PHISHING Successful American Express Phish M1 2016-10-31
- [x] ET PHISHING Successful Impots.gouv.fr Phish 2016-10-31
- [x] ET PHISHING Successful Apple Phish M1 2016-11-15
- [x] ET PHISHING Successful Dropbox Business Phish 2016-11-17
- [x] ET PHISHING Possible Successful Generic Phish (set) 2021-03-18
- [x] ET PHISHING Successful Generic Phish (Redirect to Download PDF) 2016-02-08
- [x] ET PHISHING Successful Apple Phish 2016-03-09
- [x] ET PHISHING Successful Bank of America Phish M1 2016-08-31
- [x] ET PHISHING Successful Western Union/Paypal Phish 2016-09-26

- [x] ET PHISHING Successful Apple Phish M2 2016-09-29
- [x] ET PHISHING Successful Google Drive Phish 2016-10-14
- [x] ET PHISHING Successful Windows Live Account Phish 2016-10-26
- [x] ET PHISHING Successful FreeMobile (FR) Phish M1 2016-10-31
- [x] ET PHISHING Successful Linkedin Phish 2016-11-18
- [x] ET PHISHING Successful HM Revenue Phish 2016-11-23
- [x] ET PHISHING Successful Personalized Adobe Online PDF Phish 2016-11-28
- [x] ET PHISHING Successful WhatsApp Phish M2 2016-12-07
- [x] ET PHISHING Successful Paypal Phish 2016-12-09
- [x] ET PHISHING Successful Password Protected AMEX Phish 2016-12-09
- [x] ET PHISHING Successful Paypal Phish M1 2016-12-13
- [x] ET PHISHING Successful Paypal Phish M3 2016-12-13
- [x] ET PHISHING Successful Paypal Phish M5 2016-12-13
- [x] ET PHISHING Successful Chase Phish 2016-12-13
- [x] ET PHISHING Successful Mailbox Deactivation Phish 2016-12-15
- [x] ET PHISHING Successful Windows Live Phish 2016-12-23
- [x] ET PHISHING Successful Adobe Phish 2016-04-29
- [x] ET PHISHING Successful Adobe Phish M1 2016-07-11
- [x] ET PHISHING Successful AOL Phish M1 2016-07-14
- [x] ET PHISHING Successful Adobe Phish 2016-07-21
- [x] ET PHISHING Successful Adobe Shared Document Phish 2016-08-26
- [x] ET PHISHING Successful Generic Epass Phish 2016-09-01
- [x] ET PHISHING Successful Apple Phish M1 2016-09-14
- [x] ET PHISHING Successful Apple Phish M3 2016-09-14
- [x] ET PHISHING Successful Personalized Phish 2016-09-14
- [x] ET PHISHING Successful Alibaba Phish 2016-09-28
- [x] ET PHISHING Successful Alibaba Phish 2016-09-29
- [x] ET PHISHING Successful Apple ID Phish M1 2016-10-04
- [x] ET PHISHING Successful Amazon Phish M2 2016-10-05
- [x] ET PHISHING Successful Apple Phish M2 2016-10-07
- [x] ET PHISHING Successful Alibaba Phish 2016-10-18
- [x] ET PHISHING Successful ABSA Phish 2016-10-26
- [x] ET PHISHING Successful Ameli.fr Phish M2 Oct 26 2016-10-26
- [x] ET PHISHING Successful Apple Phish Oct 31 2016
- [x] ET PHISHING Successful Generic Webmail Phish M1 2016-11-18
- [x] ET PHISHING Successful Apple Store Phish M1 2016-12-29
- [x] ET PHISHING Successful Apple Store Phish M3 2016-12-29
- [x] ET PHISHING Successful UK Tax Phishing M1 2016-02-01
- [x] ET PHISHING Successful Apple Phishing M1 2016-03-01
- [x] ET PHISHING L33bo Phishing Kit - Successful Credential Phish M2 2016-03-29
- [x] ET PHISHING L33bo Phishing Kit - Successful Credential Phish M4 2016-03-29
- [x] ET PHISHING Successful Webmail Phish M2 2016-06-22
- [x] ET PHISHING Successful Outlook Phish 2016-07-14
- [x] ET PHISHING Successful Canada Revenue Agency Phish 2016-08-30
- [x] ET PHISHING Successful Barclays Phish M2 2016-09-09
- [x] ET PHISHING Possible Successful Banking Phish (BR) 2016-09-29
- [x] ET PHISHING Successful Barclays Phish M1 2016-10-06
- [x] ET PHISHING Successful CenturyLink Phish 2016-10-12
- [x] ET PHISHING Successful Chase Phish M2 2016-10-17
- [x] ET PHISHING Successful Bank of America Phish M1 2016-10-27
- [x] ET PHISHING Successful Bank of America Phish M3 2016-10-27
- [x] ET PHISHING Successful Bank of America Phish M1 2016-11-23
- [x] ET PHISHING Successful Chase Phish M2 2016-12-07
- [x] ET PHISHING Successful Banco Itau (BR) Phish M2 2016-12-08
- [x] ET PHISHING Successful Chase Phish 2016-12-16
- [x] ET PHISHING ANTIBOT Phishing Panel Accessed on Internal Compromised Server
- [x] ET PHISHING Generic Phishing Panel Accessed on External Server
- [x] ET PHISHING Successful Gmail Phish 2016-09-30
- [x] ET PHISHING Successful Credit Agricole Bank (FR) Phish M1 2016-10-19
- [x] ET PHISHING Successful Yahoo Phish 2016-10-27
- [x] ET PHISHING Successful Shared Adobe PDF Phish 2016-11-17
- [x] ET PHISHING Successful Credential Phish (Multiple Brands) 2016-11-18
- [x] ET PHISHING Successful Barclays Phish M1 2016-11-23
- [x] ET PHISHING Successful Chase Phish 2016-12-01
- [x] ET PHISHING Successful Free Mobile (FR) Phish 2016-12-08
- [x] ET PHISHING Javascript XOR Encoding - Observed in Apple Phishing 2016-12-09
- [x] ET PHISHING Successful Chase Phishing 2016-12-12
- [x] ET PHISHING Successful Paypal Phish M2 2016-12-13
- [x] ET PHISHING Successful Paypal Phish M4 2016-12-13
- [x] ET PHISHING Successful Adobe Shared PDF Phish 2016-12-13
- [x] ET PHISHING Mailbox Deactivation Phishing Landing 2016-12-15
- [x] ET PHISHING Successful Credential Phish (Multiple Brands) 2016-12-22
- [x] ET PHISHING Successful Banamex Bank Phish 2016-12-29
- [x] ET PHISHING Successful Adobe Shared Document Phish 2016-05-04
- [x] ET PHISHING Successful AOL Phish M1 2016-07-14
- [x] ET PHISHING Successful AOL Phish M3 2016-07-14
- [x] ET PHISHING Successful Adobe Shared Document Phish 2016-08-10
- [x] ET PHISHING Successful Apple Store Transaction Cancellation Phish 2016-08-30
- [x] ET PHISHING Successful Account Update Phish 2016-09-06
- [x] ET PHISHING Successful Apple Phish M2 2016-09-14
- [x] ET PHISHING Successful Adobe Phish 2016-09-14
- [x] ET PHISHING Possible Successful Phish - Generic Form Names 2016-09-16
- [x] ET PHISHING Successful Adobe Shared Document Phish 2016-09-29
- [x] ET PHISHING Successful Apple Phish M3 2016-09-29
- [x] ET PHISHING Successful Apple Phish 2016-10-05
- [x] ET PHISHING Successful Apple Phish M1 2016-10-07
- [x] ET PHISHING Successful Amazon (UK) Phish 2016-10-17
- [x] ET PHISHING Successful Alibaba Phish 2016-10-26
- [x] ET PHISHING Successful Ameli.fr Phish M1 2016-10-26
- [x] ET PHISHING Successful Alibaba Phish 2016-10-28
- [x] ET PHISHING Successful Adobe Shared Document Phish 2016-11-15
- [x] ET PHISHING Successful Alibaba Phish 2016-12-20
- [x] ET PHISHING Successful Apple Store Phish M2 2016-12-29
- [x] ET PHISHING Successful Apple Store Phish M4 2016-12-29
- [x] ET PHISHING Successful UK Tax Phishing M2 2016-02-01
- [x] ET PHISHING L33bo Phishing Kit - Successful Credential Phish M1 2016-03-29
- [x] ET PHISHING L33bo Phishing Kit - Successful Credential Phish M3 2016-03-29
- [x] ET PHISHING Successful Dropbox Phish 2016-05-16
- [x] ET PHISHING Successful Webmail Phish M3 2016-06-22
- [x] ET PHISHING Successful Blocked Email Account Phish M1 2016-08-23
- [x] ET PHISHING Successful Barclays Phish M1 2016-09-09
- [x] ET PHISHING Successful Barclays Phish M3 2016-09-09
- [x] ET PHISHING Successful Bank of America Phish 2016-10-03
- [x] ET PHISHING Successful Barclays Phish M2 2016-10-06
- [x] ET PHISHING Successful Chase Phish M1 2016-10-17
- [x] ET PHISHING Successful Bank of America Phish M2 2016-10-21
- [x] ET PHISHING Successful Bank of America Phish M2 2016-10-27
- [x] ET PHISHING Successful Bank of America Phish M4 2016-10-27
- [x] ET PHISHING Successful Bank of America Phish M2 2016-11-23
- [x] ET PHISHING Successful Banco Itau (BR) Phish M1 2016-12-08
- [x] ET PHISHING Successful Banque Populaire (FR) Phish 2016-12-12
- [ ] ET PHISHING Observed CloudFlare Interstitial Phishing Page
- [x] ET PHISHING ANTIBOT Phishing Panel Accessed on External Compromised Server
- [x] ET PHISHING Generic Phishing Panel Accessed on Internal Server

- [x] ET PHISHING DHL Phishing Landing 2016-01-07
- [x] ET PHISHING Successful Formbuddy Credential Phish Submission 2016-01-15
- [x] ET PHISHING Phishing Landing via Weebly.com (set) 2016-02-02
- [x] ET PHISHING Phishing Landing via Weebly.com M1 2016-02-02
- [x] ET PHISHING Phishing Landing via Weebly.com M2 2016-02-02
- [x] ET PHISHING Phishing Landing via Weebly.com M3 2016-02-02
- [x] ET PHISHING Phishing Landing via Weebly.com M4 2016-02-02
- [x] ET PHISHING Common /mpp/ Phishing URI Structure 2016-02-08
- [x] ET PHISHING Am3Refh Obfuscated Phishing Landing 2016-02-23
- [x] ET PHISHING Possible Phishing Landing Obfuscation 2016-02-26
- [x] ET PHISHING Adobe Phishing Landing 2016-03-10
- [x] ET PHISHING Successful Free.fr Phish 2016-03-10
- [x] ET PHISHING Obfuscated Chase Phishing Landing 2016-03-23
- [x] ET PHISHING L33bo Phishing Landing 2016-03-29
- [x] ET PHISHING Possible Successful Phish to Hostinger Domains M1 2016-04-04
- [x] ET PHISHING Possible Successful Phish to Hostinger Domains M2 2016-04-04
- [x] ET PHISHING Possible Successful Phish to Hostinger Domains M3 2016-04-04
- [x] ET PHISHING Possible Successful Phish to Hostinger Domains M5 2016-04-04
- [x] ET PHISHING Adobe Online Document Phishing Landing 2016-05-02
- [x] ET PHISHING Successful Mailbox Shutdown Phish M1 2016-05-16
- [x] ET PHISHING Successful Mailbox Shutdown Phish M2 2016-05-16
- [x] ET PHISHING Successful Mailbox Shutdown Phish M3 2016-05-16
- [x] ET PHISHING Successful Wells Fargo Phish 2016-05-26
- [x] ET PHISHING Adobe Cloud Phishing Landing 2016-06-02
- [x] ET PHISHING Possible HMRC Phishing Domain 2016-06-08
- [x] ET PHISHING Suspicious Compound Refresh - Possible Phishing Redirect 2016-06-09
- [x] ET PHISHING Possible Apple Phishing Domain 2016-06-14
- [ ] ET PHISHING Successful Chase Phish 2016-06-15
- [ ] ET PHISHING Successful Apple Phish 2016-06-15
- [ ] ET PHISHING Successful USAA Phish 2016-06-15
- [ ] ET PHISHING Successful Paypal Phish 2016-06-15
- [x] ET PHISHING Phishing Landing via Weebly.com 2016-06-22
- [x] ET PHISHING Shipping Document Phishing Landing 2016-06-23
- [x] ET PHISHING Successful Amazon.com Phish M1 2016-06-27
- [x] ET PHISHING Data Submitted to ukit domain - Possible Phishing M1 2016-06-29
- [x] ET PHISHING Data Submitted to ukit domain - Possible Phishing M2 2016-06-29
- [x] ET PHISHING Successful DHL Phish 2016-07-11
- [x] ET PHISHING Successful Yahoo Phish 2016-07-11
- [x] ET PHISHING Successful Intuit Phish 2016-07-21
- [x] ET PHISHING Successful Generic Phish - JS Redirect to PDF 2016-08-24
- [x] ET PHISHING Successful FR Carte Bleue / BCP Phish 2016-09-06
- [x] ET PHISHING Successful Gmail Phish M1 2016-10-12
- [x] ET PHISHING Successful Banco de la Nacion Phish 2016-10-18
- [x] ET PHISHING Successful Generic Phish - Observed in Apple/Bank of America/Amazon 2016-10-26
- [x] ET PHISHING Successful Generic Phish 2016-10-27
- [x] ET PHISHING Successful Generic Phish M2 2016-10-27
- [x] ET PHISHING Successful Email Settings Phish 2016-10-28
- [x] ET PHISHING Successful Dropbox/Docusign Phish 2016-10-28
- [x] ET PHISHING Successful Linkedin Phish 2016-11-17
- [x] ET PHISHING Successful Generic Wembail Phish M2 2016-11-18
- [x] ET PHISHING Successful Bank of America Phish 2016-12-05
- [x] ET PHISHING Successful Microsoft Phish 2016-12-08
- [x] ET PHISHING Obfuscated Phishing Landing 2016-12-19
- [x] ET PHISHING Successful Poste Italiane Phish 2016-12-23
- [ ] ET PHISHING Successful Excel Online Phish 2016-01-06
- [x] ET PHISHING Successful Google Drive Phish 2016-01-12
- [x] ET PHISHING Successful IRS Phish (set) 2016-01-23
- [x] ET PHISHING Successful Workspace Phish 2016-01-26
- [x] ET PHISHING Successful Navy Federal Credit Union Phish 2016-02-01
- [ ] ET PHISHING Successful USAA Phish M1 2016-02-06
- [ ] ET PHISHING Successful USAA Phish M2 2016-02-06
- [x] ET PHISHING Successful Google Credential Phish 2016-02-17
- [x] ET PHISHING Successful Maersk Phishing 2016-02-25
- [x] ET PHISHING Successful FR Gmail Phish M1 2016-03-15
- [x] ET PHISHING Successful FR Gmail Phish M2 2016-03-15
- [x] ET PHISHING Successful Email System Manager Phish 2016-04-13
- [ ] ET PHISHING Successful Sign PDF Phish 2016-05-18
- [ ] ET PHISHING Successful Facebook Phish 2016-05-18
- [x] ET PHISHING Successful Excel Shared Document Phish 2016-06-02
- [ ] ET PHISHING Successful Ebay Phish 2016-06-14
- [ ] ET PHISHING Successful Yahoo Phish M2 2016-06-15
- [ ] ET PHISHING Successful Square Phish 2016-06-15
- [ ] ET PHISHING Successful Navy Federal Phish 2016-06-16
- [ ] ET PHISHING Successful Earthlink Phish 2016-06-16
- [ ] ET PHISHING Successful Christian Mingle Phish 2016-06-17
- [ ] ET PHISHING Successful Maybank2u Phish 2016-06-17
- [ ] ET PHISHING Successful Xfinity/Comcast Phish 2016-06-17
- [x] ET PHISHING Possible Amazon Phishing Domain 2016-06-21
- [x] ET PHISHING Possible barclays .co. uk Phishing Domain 2016-06-22
- [ ] ET PHISHING Successful Singtel Phish 2016-06-22
- [ ] ET PHISHING Successful Email Termination Phish 2016-06-22
- [ ] ET PHISHING Successful H&M Revenue Phish M2 2016-06-22
- [ ] ET PHISHING Successful Microsoft Encrypted Email Phish M2 2016-06-23
- [ ] ET PHISHING Successful Standard Bank Phish 2016-06-23
- [ ] ET PHISHING Successful Google Drive Phish M1 2016-06-11
- [ ] ET PHISHING Successful Google Drive Phish M2 2016-06-11
- [x] ET PHISHING Successful Synchronize Email Account Phish 2016-06-15
- [x] ET PHISHING Successful Webmail Account Upgrade Phish 2016-07-15
- [x] ET PHISHING Successful Earthlink Phish 2016-07-19
- [x] ET PHISHING Successful Webmail Account Upgrade Phish 2016-07-21
- [x] ET PHISHING Successful Intuit Phish 2016-08-01
- [x] ET PHISHING Tectite Web Form Submission - Possible Successful Phish
- [x] ET PHISHING Successful DHL Phish 2016-08-11
- [x] ET PHISHING Successful Adobe Shared Document Phish 2016-08-11
- [x] ET PHISHING Successful Dropbox Phish 2016-09-14
- [x] ET PHISHING Successful Personalized Adobe PDF Online Phish 2016-10-26
- [x] ET PHISHING Successful Santander Bank Phish 2016-10-28
- [x] ET PHISHING Successful Wells Fargo Phish 2016-11-28
- [x] ET PHISHING Successful Generic Webmail Phish 2016-12-02
- [x] ET PHISHING Successful WhatsApp Phish M1 2016-12-07
- [x] ET PHISHING Successful BB&T Bank Phish 2016-12-15
- [x] ET PHISHING Possible Sparkasse Phishing Domain 2021-04-05
- [x] ET PHISHING HTTP POST Contains Only Password (tk) 2021-04-05
- [x] ET PHISHING HTTP POST Contains Only Password (ml) 2021-04-05
- [x] ET PHISHING HTTP POST Contains Only Password (gq) 2021-04-05
- [x] ET PHISHING HTTP POST Contains Only Password (ga) 2021-04-05
- [x] ET PHISHING HTTP POST Contains Only Password (cf) 2021-04-05
- [x] ET PHISHING HTTP POST Contains Only Password (xyz) 2021-04-05
- [x] ET PHISHING Generic Phishing Panel Accessed on External Server
- [x] ET PHISHING Generic Phishing Panel Accessed on Internal Server
- [x] ET PHISHING Generic Phishing Panel Accessed on External Server
- [x] ET PHISHING Generic Phishing Panel Accessed on Internal Server
- [x] ET PHISHING Successful Docusign/Outlook Phish 2016-08-17
- [ ] ET PHISHING Successful Docusign Phish M2 2016-08-17

- ET PHISHING Successful Comcast Phish 2016-08-18
- ET PHISHING Successful Mailbox Renewal Phish 2016-08-19
- ET PHISHING Successful Mailbox Deactivation Phish 2016-08-19
- ET PHISHING Successful Tata Communications Phish 2016-08-19
- ET PHISHING Successful USAA Phish 2016-08-30
- ET PHISHING Successful Wells Fargo Phish 2016-08-31
- ET PHISHING Successful WhatsApp Payment Phish 2016-09-01
- ET PHISHING Successful Webmail Validator Phish M1 2016-09-02
- ET PHISHING Successful Webmail Mailbox Quota Phish 2016-09-02
- ET PHISHING Successful Yahoo Phish M1 2016-09-08
- ET PHISHING Successful Yahoo Phish 2016-09-27
- ET PHISHING Successful Western Union Phish 2016-09-27
- ET PHISHING Generic Hidden Text - Possible Phishing Landing
- ET PHISHING Office Related Appspot Hosted Shared Document Phishing Landing
- ET PHISHING Generic Multibrand NewInjection Phishing Landing Template
- ET PHISHING Generic Multibrand NewInjection Phishing Landing Template
- ET PHISHING Generic Bank Captcha Phishing Landing
- ET PHISHING Successful Linkedin Phish 2016-09-27
- ET PHISHING Successful Made In China Phish 2016-09-28
- ET PHISHING Successful Paypal Phish M1 2016-09-29
- ET PHISHING Successful Paypal Phish M3 2016-09-29
- ET PHISHING Successful Gmail Phish M2 2016-09-29
- ET PHISHING Successful Emirate Phish 2016-09-29
- ET PHISHING Successful Wells Fargo Phish M1 2016-09-30
- ET PHISHING Successful Outlook Phish 2016-10-03
- ET PHISHING Successful Apple ID Phish M2 2016-10-04
- ET PHISHING Successful Adobe Personalized Phish 2016-10-04
- ET PHISHING Successful Wells Fargo Phish 2016-10-05
- ET PHISHING Successful Paypal Phish M1 2016-10-05
- ET PHISHING Successful Excel Online Phish 2016-10-05
- ET PHISHING Successful View Invoice Phish M2 2016-10-05
- ET PHISHING Successful Paypal Phish M4 2016-10-06
- ET PHISHING Successful FreeMobile (FR) Phish M2 2016-10-06
- ET PHISHING Successful Wells Fargo Phish 2016-10-06
- ET PHISHING Successful Paypal Phish M3 2016-10-06
- ET PHISHING Successful Personalized DHL Phish 2016-10-12
- ET PHISHING Successful Netflix Phish 2016-10-12
- ET PHISHING Successful HBL Bank Phish M2 2016-10-12
- ET PHISHING Successful Dropbox Phish 2016-10-14
- ET PHISHING Successful PNC Bank Phish M1 2016-10-14
- ET PHISHING Successful Bank of America Phish (set) M1 2016-10-14
- ET PHISHING Successful Bank of America Phish (set) M3 2016-10-14
- ET PHISHING Successful Outlook Phish 2016-10-18
- ET PHISHING Successful Microsoft Live Email Account Phish 2016-10-18
- ET PHISHING Successful Google Docs Phish M1 2016-10-19
- ET PHISHING Successful NAB Bank Phish M2 2016-10-19
- ET PHISHING Successful Credit Agricole Bank (FR) Phish M3 2016-10-19
- ET PHISHING Successful EC21 B2B Phish 2016-10-21
- ET PHISHING Successful UBS Phish 2016-10-21
- ET PHISHING Successful Paypal Phish 2016-10-21
- ET PHISHING Successful Impots.gouv.fr Phish 2016-10-24
- ET PHISHING Successful Dropbox Phish 2016-10-25
- ET PHISHING Successful Personalized Outlook Phish 2016-10-26
- ET PHISHING Successful Danske Bank Phish (DA) 2016-10-27
- ET PHISHING Successful DHL Phish 2016-11-15
- ET PHISHING Successful WhatsApp Payment Phish M1 2016-11-15
- ET PHISHING Successful Paypal Phish M1 2016-11-17
- ET PHISHING Successful Docusign Phish 2016-11-17
- ET PHISHING Successful Email Settings Error Phish 2016-11-17
- ET PHISHING Successful Wells Fargo Phish M2 2016-11-18
- ET PHISHING Successful Gmail Phish 2016-08-18
- ET PHISHING Successful Excel Phish 2016-08-19
- ET PHISHING Successful Universal Webmail Phish 2016-08-19
- ET PHISHING Successful Office 365 Phish 2016-08-24
- ET PHISHING Successful Westpac Bank Phish 2016-08-31
- ET PHISHING Successful HealthEquity Phish 2016-09-01
- ET PHISHING Successful Outlook WebApp Phish 2016-09-02
- ET PHISHING Successful iCloud Phish 2016-09-02
- ET PHISHING Successful Generic Phish 2016-09-08
- ET PHISHING Successful DHL Phish 2016-09-16
- ET PHISHING Successful Google Drive Phish 2016-09-27
- ET PHISHING Generic Bank Captcha Phishing Landing
- ET PHISHING Generic Bank Captcha Phishing Landing
- ET PHISHING Microsoft Account Redirect to Phishing Landing
- ET PHISHING Generic Multibrand Ajax XHR CredPost Phishing Landing
- ET PHISHING Generic Multibrand NewInjection Phishing Landing Template
- ET PHISHING Possible Successful Generic Phish (set) 2021-04-08
- ET PHISHING Successful National Australia Bank 2016-09-28
- ET PHISHING Successful Google Docs Phish 2016-09-28
- ET PHISHING Successful Paypal Phish M2 2016-09-29
- ET PHISHING Successful Keybank Phish 2016-09-29
- ET PHISHING Successful Facebook Payment Phish M1 2016-09-29
- ET PHISHING Successful Hotmail Phish 2016-09-29
- ET PHISHING Successful Facebook Phish M2 2016-09-30
- ET PHISHING Successful Sparkasse Phish 2016-10-03
- ET PHISHING Successful Paypal (DE) Phish 2016-10-04
- ET PHISHING Successful Personalized Webmail Phish 2016-10-05
- ET PHISHING Successful Wells Fargo Phish 2016-10-05
- ET PHISHING Successful Paypal Phish M3 2016-10-05
- ET PHISHING Successful View Invoice Phish M1 2016-10-05
- ET PHISHING Successful Facebook Phish 2016-10-06
- ET PHISHING Successful FreeMobile (FR) Phish M1 2016-10-06
- ET PHISHING Successful FreeMobile (FR) Phish M3 2016-10-06
- ET PHISHING Successful Paypal Phish M2 2016-10-06
- ET PHISHING Successful HM Revenue Phish 2016-10-06
- ET PHISHING Successful Linkedin Phish 2016-10-12
- ET PHISHING Successful HBL Bank Phish M1 2016-10-12
- ET PHISHING Successful Facebook Phish 2016-10-12
- ET PHISHING Successful Yahoo Mail Phish 2016-10-14
- ET PHISHING Successful PNC Bank Phish M2 2016-10-14
- ET PHISHING Successful Bank of America Phish (set) M2 2016-10-14
- ET PHISHING Successful Paypal Phish M2 2016-10-17
- ET PHISHING Successful Chase Phish 2016-10-18
- ET PHISHING Successful NatWest Bank Phish M3 2016-10-19
- ET PHISHING Successful NAB Bank Phish M1 2016-10-19
- ET PHISHING Successful Credit Agricole Bank (FR) Phish M2 2016-10-19
- ET PHISHING Successful Personalized DHL Phish 2016-10-20
- ET PHISHING Successful Earthlink Phish 2016-10-21
- ET PHISHING Successful iTunes Connect Phish M1 2016-10-21
- ET PHISHING Successful LCL Banque et Assurance (FR) Phish 2016-10-22
- ET PHISHING Successful AOL Phish 2016-10-24
- ET PHISHING Successful Outlook Phish 2016-10-26
- ET PHISHING Successful Paypal Phish M3 2016-10-26
- ET PHISHING Successful Chase Phish 2016-10-31
- ET PHISHING Successful Netflix Phish 2016-11-15
- ET PHISHING Successful WhatsApp Payment Phish M2 2016-11-15
- ET PHISHING Successful Paypal Phish M2 2016-11-17
- ET PHISHING Successful Excel Phish 2016-11-17
- ET PHISHING Successful Wells Fargo Phish M1 2016-11-18
- ET PHISHING Successful Google Drive Phish 2016-11-18

- [x] ET PHISHING Successful Office 365 Phish 2016-11-18
- [ ] ET PHISHING Successful Western Union Phish 2016-09-27
- [x] ET PHISHING Successful Ourtime.com Phish 2016-11-28
- [x] ET PHISHING Successful Paypal Phish M2 2016-11-29
- [x] ET PHISHING Successful Google Drive Phish M1 2016-12-02
- [x] ET PHISHING Successful Three Step Gmail Phish (1 of 3) 2016-12-02
- [x] ET PHISHING Successful Three Step Gmail Phish (3 of 3) 2016-12-02
- [x] ET PHISHING Successful Gmail Phish 2016-12-06
- [x] ET PHISHING Successful Yahoo Phish 2016-12-08
- [x] ET PHISHING Successful Facebook (TR) Phish 2016-12-08
- [x] ET PHISHING Successful Linkedin Phish 2016-12-09
- [x] ET PHISHING Successful Spyus Phish (Multiple Brands) M2 2016-12-12
- [x] ET PHISHING Successful Telstra Refund Phish 2016-12-13
- [x] ET PHISHING Successful iTunes Connect Phish M2 2016-12-13
- [x] ET PHISHING Successful Discover Phish M2 2016-12-14
- [x] ET PHISHING Successful Tesco Bank Phish M1 Phish 2016-12-15
- [x] ET PHISHING Successful Dynamic Folder Phishing 2016-01-08
- [x] ET PHISHING Successful IRS Phish 2016-01-23
- [x] ET PHISHING Successful Dynamic Folder Phishing 2016-02-23
- [x] ET PHISHING Successful Adobe Phish 2016-03-10
- [x] ET PHISHING Redirect to Adobe Shared Document Phishing M3 2016-04-18
- [x] ET PHISHING Successful Onedrive Phish 2016-05-16
- [x] ET PHISHING Successful Email Login Phish 2016-06-02
- [x] ET PHISHING Possible Successful Generic Phish 2016-06-22
- [x] ET PHISHING Successful Craigslist Phish 2016-07-11
- [x] ET PHISHING Successful Personalized Email Phish 2016-07-22
- [x] ET PHISHING Successful Adobe Shared Document Phish 2016-08-19
- [x] ET PHISHING Possible Successful Citibank Phish M2 2016-08-22
- [x] ET PHISHING Successful Google Drive Phish M2 2016-08-25
- [x] ET PHISHING Successful Bank of America Phish M2 2016-08-31
- [x] ET PHISHING Successful Dynamic Folder Phishing 2016-09-12
- [x] ET PHISHING Successful Adobe Shared Document Phish 2016-10-03
- [x] ET PHISHING Successful Paypal Phish M1 2016-10-06
- [x] ET PHISHING Successful Paypal Phish M1 2016-10-06
- [x] ET PHISHING Possible Successful Generic Phish 2016-10-07
- [x] ET PHISHING Successful Dynamic Folder Phish 2016-10-10
- [x] ET PHISHING Successful Bank of America Phish 2016-10-14
- [x] ET PHISHING Successful Dynamic Folder Phish 2016-10-26
- [x] ET PHISHING Successful Generic Banking Phish 2016-10-28
- [x] ET PHISHING Successful USAA Phish 2016-11-22
- [x] ET PHISHING Successful Dynamic Folder Phish M3 2016-11-22
- [x] ET PHISHING Successful Generic Brand Phish 2016-12-01
- [x] ET PHISHING Successful Dynamic Folder Phish M1 2016-12-02
- [x] ET PHISHING Successful Paypal Phish M1 2016-12-05
- [x] ET PHISHING Successful PDF Online Phish 2016-12-19
- [x] ET PHISHING Successful Etisalat Phish 2016-12-20
- [x] ET PHISHING Successful Google Drive Phish 2016-12-22
- [x] ET PHISHING Possible Successful Outlook Web App Phish 2016-12-28
- [x] ET PHISHING Successful Protected PDF (Excel Template) Phish 2016-12-28
- [x] ET PHISHING Successful Ebay Phish M2 2016-12-29
- [ ] ET PHISHING Observed Phish Domain in DNS Query (daviviendapersonalingresos .live) 2021-04-15
- [x] ET PHISHING Observed DNS Query to Phishing Domain (apiujpnkbrhsdn57oi0ns0qmbaj0wcdzjhblj6frlh1tr .eur .lc)
- [x] ET PHISHING Observed DNS Query to Phishing Domain (igconsulting. pe)
- [x] ET PHISHING Successful Generic Phish 2020-09-21
- [x] ET PHISHING PerSwaysion Landing Page M1
- [x] ET PHISHING Possible Phishing Landing Page 2021-05-24
- [x] ET PHISHING PerSwaysion JavaScript Response M2
- [x] ET PHISHING Successful Sparkasse (DE) Phish 2016-11-28
- [x] ET PHISHING Successful Paypal Phish M2 2016-10-06
- [x] ET PHISHING Successful Paypal Phish M1 2016-11-29
- [x] ET PHISHING Successful Microsoft Live Email Account Phish 2016-11-29
- [x] ET PHISHING Successful Google Drive Phish M2 2016-12-02
- [x] ET PHISHING Successful Three Step Gmail Phish (2 of 3) Phish 2016-12-02
- [x] ET PHISHING Successful Paypal Phish M2 2016-12-05
- [x] ET PHISHING Successful Google Drive Phish 2016-12-07
- [x] ET PHISHING Successful DHL Phish 2016-12-08
- [x] ET PHISHING Successful Stripe Phish 2016-12-09
- [x] ET PHISHING Successful Spyus Phish (Multiple Brands) M1 2016-12-12
- [x] ET PHISHING Successful Ebay Phish 2016-12-12
- [x] ET PHISHING Successful iTunes Connect Phish M1 2016-12-13
- [x] ET PHISHING Successful iTunes Connect Phish M3 2016-12-13
- [x] ET PHISHING Successful Discover Phish M3 2016-12-14
- [x] ET PHISHING DHL/Adobe/Excel Phishing Landing 2016-01-07
- [x] ET PHISHING Successful PNC Bank Phish 2016-01-09
- [x] ET PHISHING Successful DHL Phish 2016-02-09
- [x] ET PHISHING Successful Apple Phish M1 2016-02-23
- [x] ET PHISHING Successful Phish to Compromised Wordpress Site 2016-03-23
- [ ] ET PHISHING Possible Successful SWF/XML Phish 2016-05-02
- [ ] ET PHISHING Possible Successful Generic Phish 2016-05-26
- [x] ET PHISHING Successful Yahoo Phish M1 2016-06-15
- [x] ET PHISHING Successful Webmail Phish M1 2016-06-22
- [x] ET PHISHING Successful Docusign/O365 Phish 2016-07-15
- [x] ET PHISHING Possible Successful Generic Phish 2016-08-19
- [x] ET PHISHING Possible Successful Citibank Phish M1 2016-08-22
- [x] ET PHISHING Team IPwned Phishing Landing 2016-08-24
- [x] ET PHISHING Successful Personalized Phish (Multiple Brands) 2016-08-30
- [x] ET PHISHING Successful Outlook Phish 2016-08-31
- [x] ET PHISHING Successful Dynamic Folder Phishing M1 2016-09-26
- [x] ET PHISHING Successful Paypal Phish 2016-10-04
- [x] ET PHISHING Successful Dynamic Folder FreeMobile (FR) Phishing 2016-10-06
- [x] ET PHISHING Successful Google Drive Phish 2016-10-06
- [x] ET PHISHING Successful Chase Phish 2016-10-07
- [x] ET PHISHING Successful Google Drive Phish 2016-10-12
- [x] ET PHISHING Successful Google Docs Phish M2 2016-10-19
- [x] ET PHISHING Successful Amazon Phish 2016-10-27
- [x] ET PHISHING Successful Dynamic Folder Phish 2016-11-15
- [x] ET PHISHING Successful Dynamic Folder Phish M1 2016-11-22
- [x] ET PHISHING Successful Dynamic Folder Phish 2016-11-28
- [x] ET PHISHING Successful National Australia Bank Phish 2016-12-02
- [x] ET PHISHING Successful Dynamic Folder Phish M2 2016-12-02
- [x] ET PHISHING Possible Successful *.myjino. ru Phish 2016-12-16
- [x] ET PHISHING Successful Paypal (DE) Phish 2016-12-19
- [x] ET PHISHING Successful Dubai Islamic Internet Bank Phish 2016-12-20
- [x] ET PHISHING Successful Sparkasse (DE) Phish 2016-12-22
- [x] ET PHISHING Successful Webmail Account Upgrade Phish 2016-12-27
- [x] ET PHISHING Successful Ebay Phish M1 2016-12-29
- [x] ET PHISHING Successful Wells Fargo Phish M1 2016-12-29
- [ ] ET PHISHING Observed Phish Domain in DNS Query (daviviendapersonalingresos .xyz) 2021-04-15
- [x] ET PHISHING Observed DNS Query to Phishing Domain (hombreymaquina .com)
- [x] ET PHISHING Possible Phishing Landing Page 2021-05-18
- [x] ET PHISHING Successful Chase Phish 2020-10-14
- [x] ET PHISHING PerSwaysion JavaScript Response M1
- [x] ET PHISHING PerSwaysion Landing Page M2
- [x] ET PHISHING Observed UK Gov Support Landing 2021-06-01

- [x] ET PHISHING PerSwaysion Landing Page M3
- [x] ET PHISHING Observed Possible Phishing Landing Page 2021-06-22
- [x] ET PHISHING Observed Possible Phishing Landing Page 2021-06-25
- [ ] ET PHISHING Observed Possible Phishing Landing Page 2021-06-29
- [x] ET PHISHING Observed DNS Query to Known Scam/Phishing Domain
- [x] ET PHISHING Observed Zimbra Phishing Landing Page 2021-08-09
- [x] ET PHISHING Client Cloaking Javascript Observed
- [x] ET PHISHING PerSwaysion Phishkit Javascript Config Variables
- [x] ET PHISHING PerSwaysion Phishkit Javascript - Observed Repetitive Custom JS Components
- [x] ET PHISHING PerSwaysion Phishkit Landing Page
- [x] ET PHISHING BulletProofLink Phishkit Activity (GET)
- [x] ET PHISHING BulletProofLink Phishkit Password-Processing URL
- [ ] ET PHISHING Possible Generic Phishkit Landing Page M1
- [x] ET PHISHING Generic Phishkit Landing Page M3
- [x] ET PHISHING Covid19 Stimulus Payment Phish Inbound M2 (2021-10-21)
- [x] ET PHISHING Covid19 Stimulus Payment Phish Inbound M4 (2021-10-21)
- [x] ET PHISHING TodayZoo Phishing Kit GET M1
- [x] ET PHISHING Successful CSIS Credential Phish
- [x] ET PHISHING Generic Credential Phish Activity GET
- [x] ET PHISHING Generic Credential Phish Activity GET
- [x] ET PHISHING IRS Payment Credential Phish Form
- [x] ET PHISHING IRS Credential Phish Credit Card Payment Data Exfil
- [x] ET PHISHING Successful Citibank Phish Landing Page
- [x] ET PHISHING Successful Generic Phish 2021-11-10
- [x] ET PHISHING ghayt_Zone Phishing Kit
- [x] ET PHISHING Nourblog1 Phish Kit
- [x] ET PHISHING Successful Facebook Credential Phish 2021-11-16
- [x] ET PHISHING Possible BulletProofLink Phishkit Activity - Retrieving Resources
- [x] ET PHISHING BulletProofLink Phishkit Template
- [x] ET PHISHING Successful Generic Banking Phish 2022-01-11
- [x] ET PHISHING Successful Adobe Phish 2022-01-12
- [x] ET PHISHING Successful Metawallet Phish 2022-01-13
- [x] ET PHISHING Generic Phish Landing Page 2022-01-14
- [x] ET PHISHING LinkedIn Phish Landing Page 2022-01-31
- [ ] ET PHISHING DAWN Comment in Phish Landing Page 2022-02-01
- [x] ET PHISHING Generic Landing Page 2022-02-04
- [x] ET PHISHING Standard Bank Login Phish 2022-02-04
- [x] ET PHISHING Successful Monzo Credential Phish M2 2022-02-17
- [x] ET PHISHING Monzo Credential Phish Landing Page 2022-02-17
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (id .bigmir .space)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (i .ua-passport .space)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain (akademia-mil .space in TLS SNI)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain (id .bigmir .space in TLS SNI)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (creditals-email .space)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (mil-gov .space)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (weryfikacja-konta .space)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (walidacja-uzytkownika .space)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (weryfikacja-poczty .space)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (bigmir .space)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (mirrohost .space)
- [x] ET PHISHING Secure Email Portal Lure Landing Page
- [x] ET PHISHING Observed Possible Phishing Landing Page 2021-06-24
- [ ] ET PHISHING Observed Possible Phishing Landing Page 2021-06-29
- [x] ET PHISHING Observed Possible Phishing 2021-06-29
- [x] ET PHISHING Observed OneDrive Phishing Landing Page 2021-08-09
- [x] ET PHISHING Observed OWA Phishing Landing Page 2021-08-20
- [x] ET PHISHING PerSwaysion Phishkit Javascript Checks if New Visitor
- [x] ET PHISHING PerSwaysion Phishkit Javascript - Observed Repetitive Custom CSS Components
- [x] ET PHISHING PerSwaysion Phishkit Javascript Variable
- [x] ET PHISHING PerSwaysion Phishkit Message Variables
- [x] ET PHISHING BulletProofLink Phishkit Activity (POST)
- [x] ET PHISHING Generic Phishkit Activity (GET)
- [x] ET PHISHING Generic Phishkit Landing Page M2
- [x] ET PHISHING Covid19 Stimulus Payment Phish Inbound M1 (2021-10-21)
- [ ] ET PHISHING Covid19 Stimulus Payment Phish Inbound M3 (2021-10-21)
- [x] ET PHISHING Successful Zoom.us Phish 2021-10-25
- [x] ET PHISHING TodayZoo Phishing Kit GET M2
- [x] ET PHISHING Successful Generic Credential Phish Activity POST
- [x] ET PHISHING Successful Generic Credential Phish Activity POST
- [x] ET PHISHING Generic Credential Phish Activity POST
- [x] ET PHISHING IRS Credential Phish Direct Deposit Payment Data Exfil
- [x] ET PHISHING IRS Payment Credential Phish Debit Card or Check Data Exfil
- [x] ET PHISHING Successful Citibank Phish 2021-11-10
- [x] ET PHISHING Successful PlayerUnknown's Battlegrounds Phish 2021-11-10
- [x] ET PHISHING Nourblog1 Phish Kit
- [x] ET PHISHING Nourblog1 Phish Kit
- [x] ET PHISHING Possible BulletProofLink Phishkit Activity - Retrieving Images
- [x] ET PHISHING Possible BulletProofLink Phishkit Activity - Redirect
- [x] ET PHISHING Generic Banking Phish Landing Page 2022-01-11
- [x] ET PHISHING Successful Generic Banking Phish 2022-01-11
- [x] ET PHISHING Adobe Phish Landing Page 2022-01-12
- [x] ET PHISHING Metawallet Phish Landing Page 2022-01-13
- [x] ET PHISHING DarkX Phish Landing Page 2022-01-22
- [x] ET PHISHING lordspartner Phish Kit
- [x] ET PHISHING Successful Intuit Phish 2022-02-03
- [x] ET PHISHING Successful Generic Credential Phish 2022-02-04
- [x] ET PHISHING Successful Monzo Credential Phish M1 2022-02-17
- [ ] ET PHISHING Successful Monzo Credential Phish M3 2022-02-17
- [x] ET PHISHING Generic Credential Phish Landing Page 2022-02-25
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (aplikacje .ron-mil .space)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (akademia-mil .space)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain (aplikacje .ron-mil .space in TLS SNI)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain (i .ua-passport .space in TLS SNI)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (ua-passport .space)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (verify-email .space)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (konto-verify .space)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (kontrola-poczty .space)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (walidacja-poczty .space)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (mod-mil .site)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (mirohost .online)

- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (meta-ua .space)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (kontrola-poczty .site)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (verify-mail .space)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain (creditals-email .space in TLS SNI)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain (mil-gov .space in TLS SNI)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain (weryfikacja-konta .space in TLS SNI)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain (walidacja-uzytkownika .space in TLS SNI)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain (weryfikacja-poczty .space in TLS SNI)
- [ ] ET PHISHING Suspected TA445 Spearphishing Related Domain (bigmir .space in TLS SNI)
- [ ] ET PHISHING Suspected TA445 Spearphishing Related Domain (mirrohost .space in TLS SNI)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain (meta-ua .space in TLS SNI)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain (kontrola-poczty .site in TLS SNI)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain (verify-mail .space in TLS SNI)
- [x] ET PHISHING Generic Credential Phish Landing Page 2022-03-01
- [x] ET PHISHING Successful Royal Bank of Canada Credential Phish 2022-03-02
- [ ] ET PHISHING FancyBear/APT28 Related Phish Landing Page 2022-03-08
- [ ] ET PHISHING Successful Generic Phish 2022-03-11
- [x] ET PHISHING Ping Identity Landing Page 2022-03-14
- [x] ET PHISHING Successful TA422 Credential Phish 2022-03-17 M1
- [ ] ET PHISHING Possible Successful TA422 Credential Phish 2022-03-17
- [x] ET PHISHING Generic Credential Phish 2022-03-18
- [x] ET PHISHING Generic Phishing domain observed in TLS SNI (info-getting-eu. com)
- [ ] ET PHISHING Generic Phish Landing Page 2022-03-29
- [x] ET PHISHING Generic Credential Phish Landing Page M1 2022-04-05
- [x] ET PHISHING Generic Credential Phish Landing Page M3 2022-04-05
- [x] ET PHISHING Successful Sparkasse Credential Phish M1 2022-04-13
- [x] ET PHISHING Sparkasse Credential Phish Landing Page M1 2022-04-13
- [ ] ET PHISHING Sparkasse Credential Phish Landing Page M3 2022-04-13
- [x] ET PHISHING Successful Wells Fargo Phish 2021-03-16
- [x] ET PHISHING Banca Monte dei Paschi di Siena Credential Phish Landing Page 2022-04-22
- [ ] ET PHISHING Observed Malicious SSL/TLS Certificate - X509v3 Alts (Tech Support/Refund Scam Landing)
- [ ] ET PHISHING Observed Malicious SSL/TLS Certificate - X509v3 Alts (Tech Support/Refund Scam Landing)
- [ ] ET PHISHING Observed Malicious SSL/TLS Certificate - X509v3 Alts (Tech Support/Refund Scam Landing)
- [ ] ET PHISHING Observed Malicious SSL/TLS Certificate - X509v3 Alts (Tech Support/Refund Scam Landing)
- [ ] ET PHISHING Observed Malicious SSL/TLS Certificate - X509v3 Alts (Tech Support/Refund Scam Landing)
- [x] ET PHISHING IRS Credential Phish Domain in DNS Lookup (jbdelmarket .com)
- [ ] ET PHISHING Successful Microsoft Account Credential Phish 2022-04-26
- [x] ET PHISHING Successful Survey Credential Phish M1 2022-04-04
- [x] ET PHISHING Successful Survey Credential Phish M3 2022-04-04
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (mod-mil .online)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (creditals-mirohost .space)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain in DNS Lookup (mirohost .site)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain (ua-passport .space in TLS SNI)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain (verify-email .space in TLS SNI)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain (konto-verify .space in TLS SNI)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain (kontrola-poczty .space in TLS SNI)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain (walidacja-poczty .space in TLS SNI)
- [ ] ET PHISHING Suspected TA445 Spearphishing Related Domain (mod-mil .site in TLS SNI)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain (mirohost .online in TLS SNI)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain (mod-mil .online in TLS SNI)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain (creditals-mirohost .space in TLS SNI)
- [x] ET PHISHING Suspected TA445 Spearphishing Related Domain (mirohost .site in TLS SNI)
- [x] ET PHISHING Successful Generic Credential Phish 2022-03-02
- [x] ET PHISHING Successful Generic Credential Phish 2022-03-02
- [ ] ET PHISHING FancyBear/APT28 Related Phish Landing Page 2022-03-08
- [x] ET PHISHING Microsoft Credential Phish 2022-03-14
- [x] ET PHISHING Generic Credential Phish Redirection 2022-03-14
- [ ] ET PHISHING Successful TA422 Credential Phish 2022-03-17 M2
- [x] ET PHISHING Successful Generic Credential Phish 2022-03-18
- [x] ET PHISHING Generic Phishing Domain in DNS Lookup (info-getting-eu. com)
- [x] ET PHISHING Successful Generic Phish 2022-03-28
- [x] ET PHISHING Successful Generic Social Media Credential Phish 2022-03-31
- [x] ET PHISHING Generic Credential Phish Landing Page M2 2022-04-05
- [x] ET PHISHING Suspicious Form with Action Value Equal to bit .ly
- [x] ET PHISHING Successful Sparkasse Credential Phish M2 2022-04-13
- [x] ET PHISHING Sparkasse Credential Phish Landing Page M2 2022-04-13
- [x] ET PHISHING Sparkasse Credential Phish Landing Page M4 2022-04-13
- [x] ET PHISHING Successful Banca Monte dei Paschi di Siena Credential Phish 2022-04-22
- [x] ET PHISHING Tech Support/Refund Scam Landing Inbound 2022/04/25
- [ ] ET PHISHING Observed Malicious SSL/TLS Certificate - X509v3 Alts (Tech Support/Refund Scam Landing)
- [ ] ET PHISHING Observed Malicious SSL/TLS Certificate - X509v3 Alts (Tech Support/Refund Scam Landing)
- [ ] ET PHISHING Observed Malicious SSL/TLS Certificate - X509v3 Alts (Tech Support/Refund Scam Landing)
- [ ] ET PHISHING Observed Malicious SSL/TLS Certificate - X509v3 Alts (Tech Support/Refund Scam Landing)
- [ ] ET PHISHING IRS Credential Phish Domain in DNS Lookup (supportmicrohere .com)
- [x] ET PHISHING Successful IRS Credential Phish 2022-04-25
- [x] ET PHISHING Microsoft Account Credential Phish Landing Page 2022-04-26
- [x] ET PHISHING Successful Survey Credential Phish M2 2022-04-04
- [x] ET PHISHING Successful Survey Credential Phish M4 2022-04-04

- [x] ET PHISHING Successful Survey Credential Phish M5 2022-04-04
- [x] ET PHISHING Successful Survey Credential Phish M6 2022-04-04
- [x] ET PHISHING Successful Survey Credential Phish M7 2022-04-04
- [x] ET PHISHING Survey Credential Phish Landing Page 2022-04-04
- [x] ET PHISHING Successful Generic Cryptowallet Credential Phish 2022-05-12
- [x] ET PHISHING Possible Cryptowallet Mining Pool Scam Landing Page
- [x] ET PHISHING Axie Infinity Credential Phish Landing Page M1 2022-05-18
- [x] ET PHISHING Successful Axie Infinity Credential Phish M1 2022-05-18
- [x] ET PHISHING Successful Axie Infinity Credential Phish M2 2022-05-18
- [x] ET PHISHING Axie Infinity Credential Phish Landing Page M2 2022-05-18
- [x] ET PHISHING Axie Infinity Credential Phish Landing Page M3 2022-05-18
- [x] ET PHISHING Spox Phishkit HTTP POST Observed
- [x] ET PHISHING Spox Phishkit Landing Page Inbound
- [x] ET PHISHING Successful Generic Phish Observed
- [x] ET PHISHING Successful Generic Credential Phish 2022-05-24
- [x] ET PHISHING Generic Credential Phish Landing Page 2022-05-24
- [x] ET PHISHING Successful Microsoft Credential Phish 2022-05-26
- [x] ET PHISHING Credito Emiliano Credential Phish Landing Page 2022-05-26
- [x] ET PHISHING Successful Generic Credential Phish 2022-05-27
- [x] ET PHISHING ING Credential Phish Landing Page 2022-05-27
- [x] ET PHISHING Faebook Credential Phish Landing Page M1 2022-05-27
- [x] ET PHISHING Facebook Credential Phish Landing Page M2 2022-05-27
- [x] ET PHISHING Generic Credential Phish Landing Page 2022-05-27
- [x] ET PHISHING Facebook Credential Phish Landing Page M1 2022-06-01
- [x] ET PHISHING Successful Generic Credential Phish 2022-06-01
- [x] ET PHISHING Facebook Credential Phish Landing Page M2 2022-06-01
- [x] ET PHISHING Generic Credential Phish Landing Page 2022-06-02
- [x] ET PHISHING Generic Cryptowallet Credential Phish Landing Page 2022-06-03
- [x] ET PHISHING Facebook Credential Phish Landing Page 2022-06-08
- [x] ET PHISHING Successful Generic Credential Phish M1 2022-06-08
- [x] ET PHISHING Successful Generic Credential Phish M2 2022-06-08
- [x] ET PHISHING DHL Credential Phish Landing Page 2022-06-09
- [x] ET PHISHING Successful DHL Credential Phish M1 2022-06-09
- [x] ET PHISHING Successful DHL Credential Phish M2 2022-06-09
- [x] ET PHISHING Sparkasse Credential Phish Landing Page 2022-06-10
- [x] ET PHISHING Successful Generic Credential Phish 2022-06-13
- [x] ET PHISHING Generic Credential Phish Landing Page 2022-06-13
- [x] ET PHISHING Successful Generic Credential Phish 2022-06-14
- [ ] ET PHISHING Generic Phishing DNS Lookup (aberto .click2eat .co .il)
- [x] ET PHISHING Generic Phishing DNS Lookup (xn--sapeaunoticias-kjb .com .br)
- [x] ET PHISHING GCash Credential Phish 2022-06-17
- [x] ET PHISHING GCash Credential Phish Landing Page 2022-06-17
- [x] ET PHISHING Successful Generic Credential Phish 2022-06-17
- [x] ET PHISHING Generic Credential Phish Landing Page 2022-06-21
- [x] ET PHISHING Apple Credential Phish Landing Page M1 2022-06-21
- [x] ET PHISHING Apple Credential Phish Landing Page M2 2022-06-21
- [x] ET PHISHING Facebook Credential Phish Landing Page 2022-06-21
- [x] ET PHISHING Successful Adobe Credential Phish 2022-06-21
- [x] ET PHISHING Successful Phish OWA Credentials 2022-06-20
- [x] ET PHISHING Emirates NBD Bank Credential Phish Landing Page 2022-06-23
- [x] ET PHISHING Successful Emirates NBD Bank Credential Phish 2022-06-23
- [x] ET PHISHING Observed DNS Query to Nedbank Phishing Domain
- [x] ET PHISHING Nedbank Phishing Landing Page 2022-06-22
- [x] ET PHISHING Observed DNS Query to OWA Phishing Domain
- [x] ET PHISHING Successful OWA Phish 2022-06-23
- [x] ET PHISHING Successful ING Group Phish 2022-06-24
- [x] ET PHISHING Observed DNS Query to ING Group Phishing Domain
- [ ] ET PHISHING Observed DNS Query to American Express Phishing Domain
- [x] ET PHISHING Sendinblue Credential Phish Landing Page 2022-06-28
- [x] ET PHISHING Successful ANZ Internet Banking Phish 2022-06-23
- [x] ET PHISHING Generic Credential Phish Landing Page 2022-06-29
- [x] ET PHISHING Successful Caixa Credential Phish 2022-06-29
- [x] ET PHISHING Successful Onedrive Credential Phish 2022-06-22
- [ ] ET PHISHING Observed DNS Query to Alibaba Phishing Domain (krikam .net)
- [x] ET PHISHING Malicious SSL Certificate detected (Alibaba Phishing)
- [ ] ET PHISHING Observed DNS Query to ING Bank Phishing Domain (servesrs -kontendiba .cyou)
- [x] ET PHISHING Successful Microsoft Credential Phish 2022-06-28
- [x] ET PHISHING Sucessful Global Sources Credential Phish 2022-06-29
- [x] ET PHISHING Sucessful Alibaba Credential Phish 2022-06-29
- [x] ET PHISHING Observed Malicious SSL/TLS Certificate (PayPal Phish Landing)
- [x] ET PHISHING BT Group Credential Phish Landing Page 2022-07-01
- [x] ET PHISHING PlayerUnknown's Battlegrounds Credential Phish Landing Page M1 2022-07-05
- [x] ET PHISHING Successful PlayerUnknown's Battlegrounds Credential Phish 2022-07-05
- [x] ET PHISHING PlayerUnknown's Battlegrounds Credential Phish Landing Page M2 2022-07-05
- [x] ET PHISHING Spox Phish Kit Landing Page 2022-07-05
- [x] ET PHISHING Navy Federal Credit Union Credential Phish Landing Page 2022-07-05
- [x] ET PHISHING Successful Facebook Credential Phish 2022-07-05
- [x] ET PHISHING Caixa Credential Phish Landing Page 2022-07-05
- [x] ET PHISHING Successful Caixa Credential Phish 2022-07-05
- [x] ET PHISHING Radobank Phishing Landing Page 2022-07-05
- [x] ET PHISHING Australian Government Credential Phish Landing Page 2022-07-06
- [x] ET PHISHING Successful Australian Government Credential Phish 2022-07-06
- [x] ET PHISHING Successful Orange Credential Phish 2022-07-07
- [x] ET PHISHING Successful Adobe Credential Phish 2022-07-08
- [x] ET PHISHING Successful Generic Credential Phish 2022-07-08
- [x] ET PHISHING Successful OWA Phish 2022-07-11
- [x] ET PHISHING Midea Credential Phish Landing Page 2022-07-12
- [x] ET PHISHING Successful Midea Credential Phish 2022-07-12
- [x] ET PHISHING Successful Microsoft Phish 2022-07-10
- [x] ET PHISHING Successful Standard Bank Credential Phish 2022-07-12 M1
- [x] ET PHISHING Successful Standard Bank Credential Phish 2022-07-12 M2
- [x] ET PHISHING Successful Standard Bank Credential Phish 2022-07-12 M3

- [x] ET PHISHING Successful Standard Bank Credential Phish 2022-07-12 M4
- [x] ET PHISHING Successful OWA Credential Phish 2022-07-13
- [x] ET PHISHING Successful OWA Phish 2022-07-15
- [x] ET PHISHING Facebook Credential Phish Landing Page 2022-07-18
- [x] ET PHISHING Successful Office 365 Phish 2022-07-19
- [x] ET PHISHING Successful Coinbase Phish 2022-07-18
- [x] ET PHISHING Successful RoundCube Phish 2022-07-18
- [x] ET PHISHING Successful Facebook Phish 2022-07-18
- [x] ET PHISHING Successful FedEx Phish 2022-07-20
- [x] ET PHISHING Successful Idaho Central CU Phish 2022-07-24
- [x] ET PHISHING AlaskaUSA FCU Phish 2022-07-24
- [x] ET PHISHING Generic Credential Phish Landing Page 2022-07-26
- [x] ET PHISHING Successful Generic Credential Phish Landing Page 2022-07-26
- [x] ET PHISHING Phishing Landing Page - Excel Purchase Order Form
- [x] ET PHISHING [TW] EvilProxy AiTM Set-Cookie
- [x] ET PHISHING [TW] EvilProxy AiTM Username Checkin
- [x] ET PHISHING [TW] EvilProxy AiTM Cookie Value M1
- [x] ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST M1
- [x] ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST M2
- [x] ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST M3
- [x] ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST M4
- [x] ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST M5
- [x] ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST M6
- [x] ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST M7
- [x] ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST M8
- [x] ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST M9
- [x] ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST M10
- [x] ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST M11
- [x] ET PHISHING [TW] EvilProxy AiTM Network Reporting
- [x] ET PHISHING [TW] Robin Banks HTTP HOST M1
- [x] ET PHISHING [TW] Robin Banks HTTP HOST M2
- [x] ET PHISHING [TW] Robin Banks HTTP GET Struct
- [x] ET PHISHING [TW] Robin Banks Redirect M1
- [x] ET PHISHING [TW] Robin Banks Redirect M2
- [x] ET PHISHING Facebook Credential Phish Landing Page 2022-07-29
- [x] ET PHISHING Successful Generic Phish 2022-07-29
- [x] ET PHISHING Facebook Credential Phish Landing Page M1 2022-08-01
- [x] ET PHISHING Successful Facebook Credential Phish 2022-08-01
- [x] ET PHISHING Facebook Credential Phish Landing Page M2 2022-08-01
- [x] ET PHISHING America First CU Successful Phish 2022-10-27
- [x] ET PHISHING America First CU Account Recovery 2022-10-27
- [x] ET PHISHING Successful Commerce Bank Phish 2022-07-30
- [x] ET PHISHING Successful Generic Phish 2022-08-01
- [x] ET PHISHING Successful Idaho Central Credit Union Credential Phish
- [ ] ET PHISHING Possible Phish with cazanova= Cookie
- [x] ET PHISHING Successful OWA Phish 2022-08-17
- [x] ET PHISHING Facebook Credential Phish Landing Page 2022-08-22
- [x] ET PHISHING PUBG Credential Phish Landing Page 2022-08-22
- [x] ET PHISHING Successful Generic Credential Phish 2022-08-23
- [x] ET PHISHING Generic Credential Phish Landing Page 2022-08-23
- [x] ET PHISHING PyPI Successful Credential Harvesting Attempt
- [x] ET PHISHING Successful Generic Credential Phish 2022-08-26
- [x] ET PHISHING Successful Telstra Credential Phish 2022-08-26
- [x] ET PHISHING Successful Bank of America Credential Phish 2022-08-25
- [x] ET PHISHING Union Bank Credential Phish Landing Page 2022-08-29
- [x] ET PHISHING Successful Telstra Credential Phish 2022-08-29
- [x] ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST Struct M1
- [x] ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST Struct M2
- [x] ET PHISHING [TW] EvilProxy AiTM Microsoft HTTP HOST Struct M3
- [ ] ET PHISHING Successful Generic Credential Phish (.ngrok .io)
- [x] ET PHISHING Successful BECU Phish 2022-09-08
- [x] ET PHISHING Generic Credential Phish Landing Page 2022-09-14
- [x] ET PHISHING Successful Generic Credential Phish 2022-09-14
- [x] ET PHISHING TA398 Phishing Kit URI Pattern M1
- [x] ET PHISHING TA398 Phishing Kit URI Pattern M2
- [x] ET PHISHING Generic Credential Phish Landing Page 2022-09-23
- [x] ET PHISHING Successful Credential Phish M1 2022-09-23
- [x] ET PHISHING Successful Credential Phish M2 2022-09-23
- [x] ET PHISHING Successful Credential Phish M3 2022-09-23
- [x] ET PHISHING Generic Credential Phish Landing Page 2022-09-26
- [x] ET PHISHING Successful Generic Credential Phish 2022-09-26
- [x] ET PHISHING Successful TA398/Sidewinder APT Related Phish 2022-09-28
- [x] ET PHISHING Generic Credential Phish Landing Page M1 2022-09-28
- [x] ET PHISHING Generic Credential Phish Landing Page M2 2022-09-28
- [x] ET PHISHING Successful Generic Credential Phish
- [x] ET PHISHING Interac (CA) Account Credential Phish Landing Page 2022-09-30
- [x] ET PHISHING Generic Credential Phish Landing Page 2022-10-03
- [x] ET PHISHING Successful Microsoft Outlook Credential Phish 2022-10-03
- [x] ET PHISHING Microsoft Excel Credential Phish Landing Page 2022-10-03
- [x] ET PHISHING DHL Credential Phish Landing Page 2022-10-07
- [x] ET PHISHING Binance Credential Phish Landing Page 2022-10-07
- [x] ET PHISHING Successful Binance Credential Phish 2022-10-07
- [x] ET PHISHING Successful Outlook Phish 2022-10-06
- [x] ET PHISHING Successful Generic Credential Phish 2022-10-10
- [ ] ET PHISHING Account Credential Phish Landing Page 2022-10-10
- [x] ET PHISHING Generic Credential Phish Landing Page 2022-10-10
- [x] ET PHISHING Generic Credential Phish Landing Page M1 2022-10-11
- [x] ET PHISHING Successful Generic Credential Phish 2022-10-11
- [x] ET PHISHING Successful Generic Credential Phish 2022-10-11
- [x] ET PHISHING Generic Credential Phish Landing Page M2 2022-10-11
- [x] ET PHISHING Generic Credential Phish Landing Page M1 2022-10-11
- [x] ET PHISHING Successful Generic Credential Phish 2022-10-11
- [x] ET PHISHING Generic Successful Phish 2022-10-11
- [x] ET PHISHING Successful Navy Federal Phish 2022-10-11
- [x] ET PHISHING Successful Trust Wallet Phish 2022-10-11
- [x] ET PHISHING Generic Credential Phish Landing Page 2022-10-12
- [x] ET PHISHING Successful Generic Credential Phish 2022-10-12
- [x] ET PHISHING Generic Credential Phish 2022-10-12
- [ ] ET PHISHING Observed DNS Query to Phishing Domain (ficosha .com)
- [x] ET PHISHING Successful mail .ru Credential Phish
- [x] ET PHISHING Successful Generic Credential Phish 2022-10-20
- [x] ET PHISHING Generic Credential Phish Landing Page 2022-10-20
- [x] ET PHISHING Successful Luno Credential Phish 2022-10-20
- [x] ET PHISHING Successful BoA Credential Phish 2022-10-24
- [x] ET PHISHING Successful Citizens Bank Credential Phish 2022-10-24
- [x] ET PHISHING Generic Credential Phish Landing Page 2022-10-26
- [x] ET PHISHING Successful Generic Credential Phish 2022-10-26
- [x] ET PHISHING Successful Generic Credential Phish 2022-10-26
- [x] ET PHISHING Generic Credential Phish Landing Page 2022-10-28
- [x] ET PHISHING Successful RBFCU Credential Phish 2022-10-31
- [x] ET PHISHING TMOBILE Credential Phish Landing Page 2022-11-01
- [x] ET PHISHING TMOBILE Successful Credential Phish 2022-11-01
- [x] ET PHISHING Twitter Credential Phish Landing Page 2022-11-04
- [x] ET PHISHING Successful Nordea Netbank Credential Phish 2022-11-04

- [x] ET PHISHING Successful Roundcube Credential Phish 2022-11-08
- [x] ET PHISHING Successful Veridian Credit Union Credential Phish 2022-11-08
- [x] ET PHISHING Successful GNCU Credential Phish 2022-11-14
- [x] ET PHISHING TA398/Sidewinder Credential Phish Landing Page M1 2022-11-18
- [x] ET PHISHING TA398/Sidewinder Credential Phish Landing Page M2 2022-11-18
- [x] ET PHISHING TA398/Sidewinder Credential Phish Landing Page M3 2022-11-18
- [ ] ET PHISHING Generic Credential Phish Landing Page 2022-11-22
- [x] ET PHISHING Ulpian Credential Phish Landing Page 2022-11-22
- [x] ET PHISHING Successful Generic Credential OTP Phish 2022-11-22
- [x] ET PHISHING Successful Generic Credential Phish 2022-11-22
- [x] ET PHISHING Successful Credit Agricole Credential Phish 2022-11-23
- [x] ET PHISHING Successful BT GROUP Credential Phish 2022-11-23
- [x] ET PHISHING WalletConnect Stealer Landing Page 2022-11-23
- [x] ET PHISHING Coinbase Credential Phish Landing Page 2022-11-29
- [x] ET PHISHING Successful Alibaba Credential Phish 2022-11-30
- [x] ET PHISHING Successful Banco de la Repblica Oriental del Uruguay Phish 2022-11-30
- [x] ET PHISHING ING Group Credential Phish Landing Page 2022-12-02
- [x] ET PHISHING Coinbase Credential Phish Landing Page 2022-12-02
- [x] ET PHISHING Generic Credential Phish Landing Page 2022-12-02
- [x] ET PHISHING Generic Credential Phish Landing Page 2022-12-02
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (administrator-enoc .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (registration-adnoc .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (kilimondoilgas-dubai .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (horsespeedtravel .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (snocprojectae .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (snoc-projectae .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (qatarenergys .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (nowmcopetroleum .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (bidders-enoc .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (proposal-enoc .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (llhhospitals .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (alzarafatravellsae .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (specgulfae .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (eaglestravels-ae .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (stalinschoolintlacademy .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (consultant-enoc .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (vendor-enocbid .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (proposal-ae-enoc .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (zbavitae .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (bid-taqa .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (safetravel-services .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (gulfcoastoilngas-ae .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (camschooluae .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (alhmodzinoilfildservices .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (nipmse .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (globalhospae .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (gulfins-ae .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (zirvaenergy .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (tenders-adio .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (uae-snocproject .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (alfayhaatravels .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (contract-snoc .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (biding-enoc .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (dibfinancialservice-uae .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (registrations-adnoc .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (enocbids .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (snocprojectuae .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (adio-gov .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (gulfmarineoilservices .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (fenczyflyemiratetravels .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (abienceinvestments-fze .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (flywaytravelandtourism .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (aiischools .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (emspgenerahospae .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (investinadio .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (mohregov-ae .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (enacopetroleum .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (emsclikoil .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (westernmedicalspecialisthosp .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (contact-adnocae .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (quickcitytravel .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (snoc-projectuae .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (consultant-ae-enoc .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (salacomimmigration .com) 2022-12-05

- [x] ET PHISHING Observed Phish Domain in DNS Lookup (dubaiferryae .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (adbntogo .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (alfujairah-ae .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (stabluk .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (siemenoilandgas .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (hamraoilgroup .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (ae-snoctenders .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (registrations-enoc .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (oceanicflyimmigration .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (consultants-ae-enoc .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (snocproject-ae .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (duramtravelagency .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (hpschooluae .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (arabianmigration .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (atenaeps .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (harvesttravelagency .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (toursolutions4u .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (contractor-enoc .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (tenders-adnoc .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (abdul-sattar-abdul-tr .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (builds-emaar .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (sheikhmouradoil .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (rambolloil .com) 2022-12-05
- [x] ET PHISHING iCloud Credential Phish Landing Page 2022-12-06
- [x] ET PHISHING Generic Credential Phish Landing Page 2022-12-07
- [x] ET PHISHING Successful ING Banking Credential Phish 2022-12-12
- [x] ET PHISHING Successful PostBank Credential Phish 2022-12-12
- [x] ET PHISHING Successful America First CU Credential Phish 2022-12-14
- [x] ET PHISHING Suncoast Credit Union Credential Phish Landing Page 2022-12-19
- [x] ET PHISHING Successful DarkX Credential Phish 2022-12-19
- [ ] ET PHISHING Lucy Security Time Tracking POST
- [x] ET PHISHING Socios Credential Phish Landing Page 2022-12-22
- [x] ET PHISHING Generic Credential Phish Landing Page 2022-12-27
- [x] ET PHISHING US Government Bid Credential Phish Landing Page 2022-12-28
- [x] ET PHISHING Successful MetaMask Pass Phrase Phish 2022-12-27
- [ ] ET PHISHING Office 365 Credential Harvesting Domain (rightofcourse .com) in DNS Lookup
- [x] ET PHISHING Successful American First CU Credential Phish 2023-01-03
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (bid-adnoc .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (iconiqueimmigration .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (contractors-adnoc .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (bid-enoc .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (proposals-ae-enoc .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (flylinkimmigration .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (contracts-adnoc .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (uae-snoctenders .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (rfq-taziz .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (abbrossgeneralhospital .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (dahilalcapitalinvest .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (biddings-enoc .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (rakpetrolae .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (snocuae .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (ae-snocproject .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (registration-ae-enoc .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (easternbaytravels .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (ahaliahospitalae .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (emarataljabrisolicitors .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (tenders-aisschools .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (tender-adnoc .com) 2022-12-05
- [x] ET PHISHING Observed Phish Domain in DNS Lookup (diligencefinconsultants .com) 2022-12-05
- [x] ET PHISHING Successful Generic Credential Phish 2022-12-06
- [x] ET PHISHING Fifth Third Banking Credential Phish Landing Page 2022-12-07
- [x] ET PHISHING ING Banking Credential Phish Landing Page 2022-12-12
- [x] ET PHISHING e-Orico Credential Phish Landing Page 2022-12-12
- [x] ET PHISHING Successful Australian Government myGov Credential Phish 2022-12-14
- [x] ET PHISHING Successful Made in China Credential Phish 2022-12-14
- [x] ET PHISHING DarkX Phish Landing Page 2022-12-19
- [x] ET PHISHING Successful o365 Credential Phish 2022-12-19
- [x] ET PHISHING Lucy Security - Phishing Landing Page M2
- [x] ET PHISHING Facebook Credential Phish Landing Page 2022-12-27
- [x] ET PHISHING Generic Cryptocurrency Credential Phish Related Domain in DNS Lookup (thedoodles .site)
- [x] ET PHISHING Successful US Government Bid Credential Phish 2022-12-28
- [x] ET PHISHING Successful Netflix Credential Phish 2022-12-27
- [x] ET PHISHING Office 365 Credential Harvesting Domain (rightofcourse .com) in TLS SNI
- [x] ET PHISHING Generic Korean Bank Credential Theft 2023-01-09

- [x] ET PHISHING Successful Coinbase Credential Phish 2023-01-09
- [x] ET PHISHING Observed Phishing Domain in DNS Lookup (infollnes-r-us .co .uk)
- [x] ET PHISHING Observed Phishing Domain in DNS Lookup (microsoftonlinesupport .cf)
- [x] ET PHISHING Successful Manhattan College Credential Phish 2022-01-10
- [x] ET PHISHING Successful Banco Galacia Credential Phish 2023-01-23
- [x] ET PHISHING Successful AU myGov Credential Phish 2023-01-30
- [x] ET PHISHING Successful Metamask Pass Phrase Phish 2023-02-01
- [x] ET PHISHING Successful Wallet Connect Pass Phrase Phish 2023-02-03
- [ ] ET PHISHING Possible Phishing Domain in DNS Lookup (c1 .biz)
- [ ] ET PHISHING AWS Phishing Domain (aws1-console-login .us) in DNS Lookup
- [ ] ET PHISHING AWS Phishing Domain (aws1-us-west .info) in DNS Lookup
- [ ] ET PHISHING AWS Phishing Domain (aws2-console-login .xyz) in DNS Lookup
- [x] ET PHISHING Prohqcker Phish Kit
- [x] ET PHISHING Sidewinder Credential Phish Landing Page M2 2023-02-16
- [x] ET PHISHING VigLink Redirect To HiYu Phishing Landing Page
- [x] ET PHISHING Successful Generic Credential Phish M1 2023-02-22
- [x] ET PHISHING Successful Generic Credential Phish M2 2023-02-22
- [x] ET PHISHING Successful Generic Credential Phish M2 2023-02-22
- [x] ET PHISHING Successful Generic Credential Phish M4 2023-02-22
- [x] ET PHISHING HiYu - Request for Victim Enrichment
- [x] ET PHISHING HiYu - Victim Enrichment Response M2
- [x] ET PHISHING HiYu - Request for User Specific Landing Page
- [x] ET PHISHING TA453 Phishing Domain in DNS Lookup
- [x] ET PHISHING TA453 Phishing Domain in DNS Lookup
- [x] ET PHISHING Coinbase Credential Phish 2023-02-24
- [x] ET PHISHING Generic Credential Phish Landing Page 2023-02-27
- [x] ET PHISHING Successful Ionos Credential Phish 2023-02-28
- [x] ET PHISHING PUBG Credential Phish 2023-03-06
- [x] ET PHISHING Possible Credential Phish Landing Page 2023-03-10
- [x] ET PHISHING Observed DNS Query to Possible Phish Hosted on onlinehome.us
- [x] ET PHISHING Generic Credential Phish Landing Page 2023-03-13
- [x] ET PHISHING EDD Credential Phish Landing Page M2 2023-03-16
- [x] ET PHISHING Silicon Valley Bank Credential Phish Landing Page M1
- [x] ET PHISHING Silicon Valley Bank Phish Domain in DNS Lookup (cash4svb .com)
- [x] ET PHISHING Snapchat Credential Phish Landing Page 2023-03-21
- [x] ET PHISHING Silicon Valley Bank Credential Phish Landing Page (2023-03-30)
- [x] ET PHISHING Generic Credential Phish Landing Page 2023-04-03
- [x] ET PHISHING Generic Antibot Phish Landing Page 2023-04-05
- [x] ET PHISHING Tech Support Phone Scam Landing 2023-04-17
- [x] ET PHISHING Successful OneDrive Credential Phish 2023-04-18
- [x] ET PHISHING Fake Google Chrome Error Landing Page, Anti-Analysis Technique
- [x] ET PHISHING Fake Google Chrome Error Landing Page, Load Payload
- [x] ET PHISHING Successful DHL Credential Phish 2023-04-24
- [x] ET PHISHING W3LL STORE Credential Phish Landing Page 2023-04-25
- [x] ET PHISHING USPS Credential Phish Landing Page M1 2023-04-28
- [x] ET PHISHING Generic Credential Phish Landing Page 2023-04-28
- [x] ET PHISHING Generic Credential Phish Landing Page from Text Scam M1 2023-05-01
- [x] ET PHISHING Observed Phishing Domain in DNS Lookup (circle-ci .com)
- [x] ET PHISHING Observed Phishing Domain in DNS Lookup (mcrsfts-passwdupdate .com)
- [x] ET PHISHING Manhattan College Phish Landing Page 2022-01-10
- [x] ET PHISHING EvilProxy AiTM Cookie Value M2
- [x] ET PHISHING Successful Banco G&T Continental Credential Phish 2023-01-25
- [x] ET PHISHING Successful VyStar CU Credential Phish 2023-01-31
- [x] ET PHISHING Successful Wallet Connect Private Key Phish 2023-02-03
- [x] ET PHISHING Successful Wallet Connect Key Store Phish 2023-02-03
- [x] ET PHISHING Successful Generic Credential Phish 2023-02-07
- [ ] ET PHISHING AWS Phishing Domain (us2-eat-a-w-s .blogspot .com) in DNS Lookup
- [ ] ET PHISHING AWS Phishing Domain (aws1-ec2-console .com) in DNS Lookup
- [x] ET PHISHING myGov Credential Phish 2023-02-15
- [x] ET PHISHING Sidewinder Credential Phish Landing Page M1 2023-02-16
- [x] ET PHISHING Generic Credential Phish Landing Page 2023-02-21
- [x] ET PHISHING Generic Credential Phish Landing Page M1 2023-02-22
- [x] ET PHISHING Generic Credential Phish Landing Page M2 2023-02-22
- [x] ET PHISHING Successful Generic Credential Phish M1 2023-02-22
- [x] ET PHISHING Successful Generic Credential Phish M3 2023-02-22
- [x] ET PHISHING Successful Royal Credit Union Credential Phish 2023-02-23
- [x] ET PHISHING HiYu - Victim Enrichment Response M1
- [x] ET PHISHING HiYu - Victim Enrichment Response M3
- [x] ET PHISHING TA453 Phishing Domain in DNS Lookup
- [x] ET PHISHING TA453 Phishing Domain in DNS Lookup
- [x] ET PHISHING TA453 Phishing Domain in DNS Lookup
- [x] ET PHISHING Successful Generic Credential Phish 2023-02-27
- [x] ET PHISHING Successful Orange.fr Credential Phish 2023-02-27
- [x] ET PHISHING Successful CenturyLink Credential Phish 2023-03-01
- [x] ET PHISHING Roblox Credential Phish 2023-03-06
- [x] ET PHISHING United Parcel Service Landing Page 2023-03-10
- [x] ET PHISHING Scam Redirect Domain in DNS Lookup
- [x] ET PHISHING EDD Credential Phish Landing Page 2023-03-16 M1
- [x] ET PHISHING Generic Credential Phish Landing Page 2023-03-16
- [x] ET PHISHING Silicon Valley Bank Credential Phish Landing Page M2
- [x] ET PHISHING Generic Credential Phish Landing Page 2023-03-21
- [x] ET PHISHING Generic Credential Phish Landing Page using submit-form .com
- [x] ET PHISHING Successful Office365 Credential Phish 2023-03-31
- [x] ET PHISHING Generic Credential Phish Landing Page 2023-04-05
- [x] ET PHISHING Crypto Credential Phish Landing Page 2023-04-17
- [x] ET PHISHING Successful Bank of America Credential Phish 2023-04-17
- [x] ET PHISHING Successful International Card Services Credential Phish 2023-04-20
- [x] ET PHISHING Fake Google Chrome Error Landing Page, Control Access with Cookie
- [ ] ET PHISHING W3LL STORE Phish Kit Landing Page 2023-04-24
- [x] ET PHISHING Successful Generic Credential Phish from W3LL STORE Phishkit 2023-04-25
- [ ] ET PHISHING W3LL STORE Phish Kit Landing Page 2023-04-26
- [x] ET PHISHING USPS Credential Phish Landing Page M2 2023-04-28
- [x] ET PHISHING Lucy Security - Phishing Framework Plugin List POST
- [x] ET PHISHING Generic Credential Phish Landing Page from Text Scam M2 2023-05-01

- [x] ET PHISHING Generic Credential Phish Landing Page from Text Scam M3 2023-05-01
- [x] ET PHISHING W3LL STORE Phish Kit Landing Page 2023-05-02
- [x] ET PHISHING W3LL STORE Credential Phish Landing Page (Capt) 2023-05-05
- [x] ET PHISHING W3LL STORE Credential Phish Landing Page (Success) 2023-05-05
- [x] ET PHISHING Greatness Phish Kit Landing Page M1 2023-05-15
- [x] ET PHISHING Successful iCloud Credential Phish 2023-06-12
- [x] ET PHISHING Known Phishing Related Domain in DNS Lookup (schseels .com)
- [x] ET PHISHING ID.me Credential Theft Landing Page 2023-06-21
- [x] ET PHISHING Generic Obfuscated Sign In Landing Page 2023-06-22
- [x] ET PHISHING Successful BDO Bank Credential Phish 2023-06-23
- [x] ET PHISHING Ankarex Smishing as a Service Domain in DNS Lookup (ankarex .net)
- [ ] ET PHISHING RomCom Phishing Domain in DNS Lookup (ukrainianworldcongress .info)
- [x] ET PHISHING Vietnamese Govt Credential Phish M2 2023-07-18
- [x] ET PHISHING Generic Credential Phish Landing Page 2023-08-09
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cashapphelp06 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (hpsupport08 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cashapphelp011 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (apples9 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mshelp51 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mshelp03 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mshelp09 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mshelp52 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cashapphelp010 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cashapp05 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cashapphelp103 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cshelp09 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cashapphelp08 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mshelp08 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mshelp14 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (help81 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (pcjet .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (hpsupport03 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cshelp10 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mshelp02 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (help87 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (helpdesk24 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (pccharlie .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cshelp03 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cshelp01 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (help89 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cshelp08 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (apples5 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cashapphelp01 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mshelp8 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mshelp3 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (refundpvt .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mshelp15 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cashapp02 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mshelp12 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (apples4 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (help86 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (apples3 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (apples1 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (pcecho .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cashapphelp02 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (apples13 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (pcbravo .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (securenetwork .cc)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cshelp04 .us)
- [x] ET PHISHING Generic Credential Phish Landing Page from Text Scam M4 2023-05-01
- [x] ET PHISHING W3LL STORE Phish Kit Landing Page 2023-05-05
- [x] ET PHISHING W3LL STORE Credential Phish Landing Page (Index) 2023-05-05
- [x] ET PHISHING Successful W3LL STORE Credential Phish 2023-05-10
- [x] ET PHISHING DarkWatchman Phish Domain in DNS Lookup (cryptopro-download .one)
- [x] ET PHISHING GreetingGhoul Stealer Crypto Landing Page
- [x] ET PHISHING Generic Survey Credential Phish Landing Page 2022-06-20
- [x] ET PHISHING Obfuscated MrxC0DER Credential Phish Landing Page
- [x] ET PHISHING Suspicious IPFS Domain Rewritten with Google Translate
- [x] ET PHISHING Successful Yahoo Credential Phish 2023-06-30
- [x] ET PHISHING Successful SFR Mail Credential Phish 2023-07-07
- [x] ET PHISHING Vietnamese Govt Credential Phish M1 2023-07-18
- [x] ET PHISHING Vietnamese Govt Credential Phish M3 2023-07-18
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mshelp53 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (pcxhelp .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (ppalsecure .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mshelp2 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cashapphelp101 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cashapp04 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (help88 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mshelp013 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mshelp6 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mshelp01 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cshelp12 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (hpsupport02 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (quickcare .cc)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (apples12 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (pcdelta .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cashapphelp05 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mscare .cc)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mshelp05 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (apples10 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (jcb24 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (support24 .cc)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (apples8 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mshelp012 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cashapphelp102 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (apples6 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cshelp06 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cashapphelp104 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (hpsupport09 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cashapphelp105 .cc)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cashapphelp105 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (hpsupport07 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (apples14 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mshelp010 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (b124 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (securehelp .cc)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (help84 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cashapphelp03 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (help90 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (apples11 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cshelp13 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (nrtnhelp .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cshelp14 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mshelp5 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mshelp .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mshelp015 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (jivajii .us)

- ET PHISHING TOAD Domain in DNS Lookup (mshelp13 .us)
- ET PHISHING TOAD Domain in DNS Lookup (help82 .us)
- ET PHISHING TOAD Domain in DNS Lookup (apples15 .us)
- ET PHISHING TOAD Domain in DNS Lookup (mshelp10 .us)
- ET PHISHING TOAD Domain in DNS Lookup (ncare360 .us)
- ET PHISHING TOAD Domain in DNS Lookup (mshelp11 .us)
- ET PHISHING TOAD Domain in DNS Lookup (hpsupport04 .us)
- ET PHISHING TOAD Domain in DNS Lookup (cashapphelp04 .us)
- ET PHISHING TOAD Domain in DNS Lookup (live855 .us)
- ET PHISHING TOAD Domain in DNS Lookup (mshelp4 .us)
- ET PHISHING TOAD Domain in DNS Lookup (help83 .us)
- ET PHISHING TOAD Domain in DNS Lookup (pcindigo .us)
- ET PHISHING TOAD Domain in DNS Lookup (pchorse .us)
- ET PHISHING TOAD Domain in DNS Lookup (mshelp06 .us)
- ET PHISHING TOAD Domain in DNS Lookup (a128 .us)
- ET PHISHING TOAD Domain in DNS Lookup (mshelp014 .us)
- ET PHISHING TOAD Domain in DNS Lookup (pcalpha .us)
- ET PHISHING TOAD Domain in DNS Lookup (securedhelp .us)
- ET PHISHING TOAD Domain in DNS Lookup (mshelp7 .us)
- ET PHISHING TOAD Domain in DNS Lookup (cashapp06 .us)
- ET PHISHING TOAD Domain in DNS Lookup (supportlife .us)
- ET PHISHING TOAD Domain in DNS Lookup (mshelp04 .us)
- ET PHISHING Observed TOAD Domain (mshelp53 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (pcxhelp .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (ppalsecure .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (mshelp2 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cashapphelp101 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cashapp04 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (help88 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (mshelp013 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (mshelp6 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (mshelp01 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cshelp12 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (hpsupport02 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (quickcare .cc in TLS SNI)
- ET PHISHING Observed TOAD Domain (apples12 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (pcdelta .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cashapphelp05 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (mscare .cc in TLS SNI)
- ET PHISHING Observed TOAD Domain (mshelp05 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (apples10 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (jcb24 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (support24 .cc in TLS SNI)
- ET PHISHING Observed TOAD Domain (apples8 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (mshelp012 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cashapphelp102 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (apples6 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cshelp06 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cashapphelp104 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (hpsupport09 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cashapphelp105 .cc in TLS SNI)
- ET PHISHING Observed TOAD Domain (cashapphelp105 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (hpsupport07 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (apples14 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (mshelp010 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (b124 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (securehelp .cc in TLS SNI)
- ET PHISHING Observed TOAD Domain (help84 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cashapphelp03 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (help90 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (apples11 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cshelp13 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (nrtnhelp .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cshelp14 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (mshelp5 .us in TLS SNI)
- ET PHISHING TOAD Domain in DNS Lookup (pckilo .us)
- ET PHISHING TOAD Domain in DNS Lookup (hpsupport01 .us)
- ET PHISHING TOAD Domain in DNS Lookup (mshelp1 .us)
- ET PHISHING TOAD Domain in DNS Lookup (cshelp05 .us)
- ET PHISHING TOAD Domain in DNS Lookup (cashapp01 .us)
- ET PHISHING TOAD Domain in DNS Lookup (cashapp03 .us)
- ET PHISHING TOAD Domain in DNS Lookup (cshelp11 .us)
- ET PHISHING TOAD Domain in DNS Lookup (cashapphelp07 .us)
- ET PHISHING TOAD Domain in DNS Lookup (mshelp011 .us)
- ET PHISHING TOAD Domain in DNS Lookup (hpsupport06 .us)
- ET PHISHING TOAD Domain in DNS Lookup (help85 .us)
- ET PHISHING TOAD Domain in DNS Lookup (msofthelp .com)
- ET PHISHING TOAD Domain in DNS Lookup (mshelp9 .us)
- ET PHISHING TOAD Domain in DNS Lookup (mshelp07 .us)
- ET PHISHING TOAD Domain in DNS Lookup (apples7 .us)
- ET PHISHING TOAD Domain in DNS Lookup (hpsupport05 .us)
- ET PHISHING TOAD Domain in DNS Lookup (cshelp02 .us)
- ET PHISHING TOAD Domain in DNS Lookup (pcfox .us)
- ET PHISHING TOAD Domain in DNS Lookup (cshelp07 .us)
- ET PHISHING TOAD Domain in DNS Lookup (cashapphelp012 .us)
- ET PHISHING TOAD Domain in DNS Lookup (apples2 .us)
- ET PHISHING TOAD Domain in DNS Lookup (gshelp .us)
- ET PHISHING Observed TOAD Domain (cashapphelp06 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (hpsupport08 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cashapphelp011 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (apples9 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (mshelp51 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (mshelp03 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (mshelp09 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (mshelp52 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cashapphelp010 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cashapp05 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cashapphelp103 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cshelp09 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cashapphelp08 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (mshelp08 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (mshelp14 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (help81 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (pcjet .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (hpsupport03 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cshelp10 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (mshelp02 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (help87 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (helpdesk24 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (pccharlie .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cshelp03 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cshelp01 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (help89 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cshelp08 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (apples5 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cashapphelp01 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (mshelp8 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (mshelp3 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (refundpvt .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (mshelp15 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cashapp02 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (mshelp12 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (apples4 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (help86 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (apples3 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (apples1 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (pcecho .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (cashapphelp02 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (apples13 .us in TLS SNI)
- ET PHISHING Observed TOAD Domain (pcbravo .us in TLS SNI)

- [ ] ET PHISHING Observed TOAD Domain (mshelp .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (mshelp015 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (jivajii .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (pckilo .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (hpsupport01 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (mshelp1 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (cshelp05 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (cashapp01 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (cashapp03 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (cshelp11 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (cashapphelp07 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (mshelp011 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (hpsupport06 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (help85 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (msofthelp .com in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (mshelp9 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (mshelp07 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (apples7 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (hpsupport05 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (cshelp02 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (pcfox .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (cshelp07 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (cashapphelp012 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (apples2 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (gshelp .us in TLS SNI)
- [x] ET PHISHING Ferest Smuggler Request M2
- [x] ET PHISHING Generic Credential Phish Landing Page 2023-09-05
- [x] ET PHISHING [TW] NOTG Obfuscation Redirect Observed M2
- [x] ET PHISHING [TW] NOTG Check Expirations URL Struct
- [x] ET PHISHING [TW] NOTG Check Add User URL Struct
- [ ] ET PHISHING [TW] Tycoon Phishkit Domain Observed (codecrafters .su)
- [ ] ET PHISHING [TW] Tycoon Phishkit Domain (devcraftingsolutions .com in TLS SNI)
- [x] ET PHISHING [TW] Microsoft Credential Phish V3 CnC Domain in DNS Lookup (snxn298y5brpxd67rbntynb6p4qupuuv .com)
- [x] ET PHISHING [TW] Microsoft Credential Phish V3 CnC Domain in DNS Lookup (bc1q922jh6d3zk0aelqdfc7yygzjr29sle .com)
- [x] ET PHISHING [TW] Microsoft Credential Phish V3 CnC Domain in DNS Lookup (bc1q8hn7d0uhpspz9xcp3hl9e5erddlew .com)
- [x] ET PHISHING [TW] Microsoft Credential Phish V3 CnC Domain in DNS Lookup (bc1qp2we64k79237y0npqehprfgynlz02fwpktlwte .com)
- [x] ET PHISHING [TW] Microsoft Credential Phish V3 CnC Domain in DNS Lookup (bc1qm34lmk6eesc65zpw79lxes69zkq3ew .com)
- [x] ET PHISHING [TW] Microsoft Credential Phish V3 CnC Domain in DNS Lookup (13fzyjcfqhnryc4dkxkykbaawkzwrmhcfc .com)
- [x] ET PHISHING [TW] Microsoft Credential Phish V3 CnC Domain in DNS Lookup (bc1q0hcvl2p88zdv4dj97mfwtwv4usxm .com)
- [x] ET PHISHING [TW] Microsoft Credential Phish V3 CnC Domain in DNS Lookup (bc1qjywr9cpsm5u7e4yrmnx2jsahgzzmm7 .com)
- [x] ET PHISHING [TW] Observed Microsoft Credential Phish V3 Domain (snxn298y5brpxd67rbntynb6p4qupuuv .com in TLS SNI)
- [x] ET PHISHING [TW] Observed Microsoft Credential Phish V3 Domain (bc1q922jh6d3zk0aelqdfc7yygzjr29sle .com in TLS SNI)
- [x] ET PHISHING [TW] Observed Microsoft Credential Phish V3 Domain (bc1q8hn7d0uhpspz9xcp3hl9e5erddlew .com in TLS SNI)
- [x] ET PHISHING [TW] Observed Microsoft Credential Phish V3 Domain (bc1qp2we64k79237y0npqehprfgynlz02fwpktlwte .com in TLS SNI)
- [x] ET PHISHING [TW] Observed Microsoft Credential Phish V3 Domain (bc1qm34lmk6eesc65zpw79lxes69zkq3ew .com in TLS SNI)
- [x] ET PHISHING [TW] Observed Microsoft Credential Phish V3 Domain (13fzyjcfqhnryc4dkxkykbaawkzwrmhcfc .com in TLS SNI)
- [x] ET PHISHING [TW] Observed Microsoft Credential Phish V3 Domain (bc1q0hcvl2p88zdv4dj97mfwtwv4usxm .com in TLS SNI)
- [x] ET PHISHING [TW] Observed Microsoft Credential Phish V3 Domain (bc1qjywr9cpsm5u7e4yrmnx2jsahgzzmm7 .com in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (securenetwork .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (cshelp04 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (mshelp13 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (help82 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (apples15 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (mshelp10 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (ncare360 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (mshelp11 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (hpsupport04 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (cashapphelp04 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (live855 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (mshelp4 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (help83 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (pcindigo .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (pchorse .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (mshelp06 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (a128 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (mshelp014 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (pcalpha .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (securedhelp .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (mshelp7 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (cashapp06 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (supportlife .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (mshelp04 .us in TLS SNI)
- [x] ET PHISHING Ferest Smuggler Request M1
- [x] ET PHISHING Facebook Credential Phish Landing Page 2023-09-01
- [x] ET PHISHING [TW] NOTG Obfuscation Redirect Observed M1
- [x] ET PHISHING [TW] NOTG Redirect URL Struct
- [x] ET PHISHING [TW] NOTG Password URL Struct
- [ ] ET PHISHING [TW] Tycoon Phishkit Domain Observed (codecrafterspro .com)
- [ ] ET PHISHING [TW] Tycoon Phishkit Domain Observed (devcraftingsolutions .com)
- [ ] ET PHISHING [TW] Tycoon Phishkit Domain (codecrafterspro .com in TLS SNI)
- [x] ET PHISHING [TW] Microsoft Credential Phish V3 CnC Domain in DNS Lookup (3aqulcx8xkg6qxrhxgmisecrt98kxlenzj .com)
- [x] ET PHISHING [TW] Microsoft Credential Phish V3 CnC Domain in DNS Lookup (bc1qc230lt32ey73qlaj9rkujm0ujtv090 .com)
- [x] ET PHISHING [TW] Microsoft Credential Phish V3 CnC Domain in DNS Lookup (bc1qr0kxc4gcqt2lcpkdnz8ehs02u9n2xkgz89rwpr .com)
- [x] ET PHISHING [TW] Microsoft Credential Phish V3 CnC Domain in DNS Lookup (bc1q6zd25jmkfh5x24ymp60tq99xdugpq .com)
- [x] ET PHISHING [TW] Microsoft Credential Phish V3 CnC Domain in DNS Lookup (1kmtet1wyig94bxbcke45nivfx1w3m3hth .com)
- [x] ET PHISHING [TW] Microsoft Credential Phish V3 CnC Domain in DNS Lookup (bc1q6crq62w2sclm0cwwk6m2wugr6jkh .com)
- [x] ET PHISHING [TW] Microsoft Credential Phish V3 CnC Domain in DNS Lookup (bc1qm34lsc65zpw79lxes69zkqmk6ee3ew .com)
- [x] ET PHISHING [TW] Microsoft Credential Phish V3 CnC Domain in DNS Lookup (bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h .com)
- [x] ET PHISHING [TW] Observed Microsoft Credential Phish V3 Domain (3aqulcx8xkg6qxrhxgmisecrt98kxlenzj .com in TLS SNI)
- [x] ET PHISHING [TW] Observed Microsoft Credential Phish V3 Domain (bc1qc230lt32ey73qlaj9rkujm0ujtv090 .com in TLS SNI)
- [x] ET PHISHING [TW] Observed Microsoft Credential Phish V3 Domain (bc1qr0kxc4gcqt2lcpkdnz8ehs02u9n2xkgz89rwpr .com in TLS SNI)
- [x] ET PHISHING [TW] Observed Microsoft Credential Phish V3 Domain (bc1q6zd25jmkfh5x24ymp60tq99xdugpq .com in TLS SNI)
- [x] ET PHISHING [TW] Observed Microsoft Credential Phish V3 Domain (1kmtet1wyig94bxbcke45nivfx1w3m3hth .com in TLS SNI)
- [x] ET PHISHING [TW] Observed Microsoft Credential Phish V3 Domain (bc1q6crq62w2sclm0cwwk6m2wugr6jkh .com in TLS SNI)
- [x] ET PHISHING [TW] Observed Microsoft Credential Phish V3 Domain (bc1qm34lsc65zpw79lxes69zkqmk6ee3ew .com in TLS SNI)
- [x] ET PHISHING [TW] Observed Microsoft Credential Phish V3 Domain (bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h .com in TLS SNI)

- [x] ET PHISHING Generic Phishing - Successful Landing Interaction
- [x] ET PHISHING Observed TOAD Domain (eshopper .top in TLS SNI)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (login .pcsystem247 .cc)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mghelp .live)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (support7 .cc)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mta-sts .gub .bio)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (axhelp .live)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mail .retfaqboos .site)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (gbhelp .cc)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (jxhelp .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (retfaqboos .site)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (dfhelp .cc)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (pxhelp .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (emv1 .gub .bio)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (login .helpsystem .cc)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (33 .gub .bio)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (gub .bio)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mshelp58 .us)
- [ ] ET PHISHING Observed TOAD Domain (login .helpsystem .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (lbhelp .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (mchelp .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (mta-sts .gub .bio in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (login .pcsystem247 .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (dbhelp .info in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (axhelp .live in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (cashapphelp19 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (pcsystem247 .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (wdhelp .live in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (mail .retfaqboos .site in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (support7 .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (mail .mrree .gub .bio in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (emv1 .gub .bio in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (retfaqboos .site in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (gchelp .info in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (dfhelp .cc in TLS SNI)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (tenty247 .top)
- [ ] ET PHISHING Observed TOAD Domain (tenty247 .top in TLS SNI)
- [ ] ET PHISHING Phishing Domain in TLS SNI (imedcloud .net)
- [ ] ET PHISHING Observed Crypto Phishing Domain in TLS SNI
- [x] ET PHISHING [TW] Tycoon Phishkit Config Vars
- [x] ET PHISHING Netscaler Gateway Credential Theft (POST)
- [x] ET PHISHING DNS Query to TOAD Domain (300005 .ru)
- [x] ET PHISHING Observed TOAD Domain (300005 .ru in TLS SNI)
- [ ] ET PHISHING DNS Query to TOAD Domain (bshelp .us)
- [ ] ET PHISHING DNS Query to TOAD Domain (cshelp03 .us)
- [ ] ET PHISHING DNS Query to TOAD Domain (bghelp .us)
- [ ] ET PHISHING DNS Query to TOAD Domain (dfhelp .live)
- [ ] ET PHISHING DNS Query to TOAD Domain (j2care .cc)
- [ ] ET PHISHING DNS Query to TOAD Domain (i2care .us)
- [ ] ET PHISHING DNS Query to TOAD Domain (bgcare .info)
- [ ] ET PHISHING DNS Query to TOAD Domain (a2help .us)
- [ ] ET PHISHING DNS Query to TOAD Domain (bscare .help)
- [ ] ET PHISHING DNS Query to TOAD Domain (hscare .info)
- [ ] ET PHISHING DNS Query to TOAD Domain (brhelp .live)
- [ ] ET PHISHING DNS Query to TOAD Domain (cancel247 .info)
- [ ] ET PHISHING DNS Query to TOAD Domain (aphelp .us)
- [ ] ET PHISHING DNS Query to TOAD Domain (g2care .us)
- [ ] ET PHISHING DNS Query to TOAD Domain (j2care .us)
- [ ] ET PHISHING DNS Query to TOAD Domain (n2care .us)
- [ ] ET PHISHING DNS Query to TOAD Domain (bghelp .online)
- [ ] ET PHISHING DNS Query to TOAD Domain (hscare .online)
- [ ] ET PHISHING DNS Query to TOAD Domain (m2care .us)
- [ ] ET PHISHING DNS Query to TOAD Domain (eshopper .top)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (athelp .live)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (jxhelp .cc)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (wdhelp .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (wdhelp .live)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (kbhelp .info)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (helpsystem .cc)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (gbhelp .live)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (gchelp .info)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cxhelp .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mail .mrree .gub .bio)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (pcsystem247 .cc)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (amz34 .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (mchelp .cc)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (jxhelp .info)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (dbhelp .info)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (lbhelp .us)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (cashapphelp19 .us)
- [ ] ET PHISHING Observed TOAD Domain (gbhelp .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (wdhelp .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (kbhelp .info in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (amz34 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (gbhelp .live in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (jxhelp .info in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (jxhelp .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (jxhelp .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (athelp .live in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (gub .bio in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (mghelp .live in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (33 .gub .bio in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (pxhelp .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (helpsystem .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (cxhelp .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (mshelp58 .us in TLS SNI)
- [ ] ET PHISHING TOAD Domain in DNS Lookup (gxcare .cc)
- [ ] ET PHISHING Observed TOAD Domain (gxcare .cc in TLS SNI)
- [ ] ET PHISHING Crypto Phishing DNS Lookup
- [ ] ET PHISHING Crypto Phishing DNS Lookup
- [x] ET PHISHING [TW] Trex Phishkit POST
- [x] ET PHISHING [TW] Tycoon Phishkit CSS
- [x] ET PHISHING MageCart 404 COOKIE_ANNOT
- [x] ET PHISHING DNS Query to TOAD Domain (helpset123 .site)
- [x] ET PHISHING Observed TOAD Domain (helpset123 .site in TLS SNI)
- [ ] ET PHISHING DNS Query to TOAD Domain (b2care .cc)
- [ ] ET PHISHING DNS Query to TOAD Domain (r2care .cc)
- [ ] ET PHISHING DNS Query to TOAD Domain (r2care .us)
- [ ] ET PHISHING DNS Query to TOAD Domain (hshelp .live)
- [ ] ET PHISHING DNS Query to TOAD Domain (hscare .cc)
- [ ] ET PHISHING DNS Query to TOAD Domain (hshelp .info)
- [ ] ET PHISHING DNS Query to TOAD Domain (bgcare .us)
- [ ] ET PHISHING DNS Query to TOAD Domain (bshelp .support)
- [ ] ET PHISHING DNS Query to TOAD Domain (c2care .cc)
- [ ] ET PHISHING DNS Query to TOAD Domain (hscare .live)
- [ ] ET PHISHING DNS Query to TOAD Domain (bscare .cc)
- [ ] ET PHISHING DNS Query to TOAD Domain (m2care .cc)
- [ ] ET PHISHING DNS Query to TOAD Domain (d2care .cc)
- [ ] ET PHISHING DNS Query to TOAD Domain (bgcare .live)
- [ ] ET PHISHING DNS Query to TOAD Domain (bshelp .info)
- [ ] ET PHISHING DNS Query to TOAD Domain (nxhelp .live)
- [x] ET PHISHING DNS Query to TOAD Domain (catreenpr .is)
- [ ] ET PHISHING DNS Query to TOAD Domain (kelbyonel .nl)
- [ ] ET PHISHING DNS Query to TOAD Domain (hshelp .online)

- [ ] ET PHISHING DNS Query to TOAD Domain (bscare .info)
- [ ] ET PHISHING DNS Query to TOAD Domain (hscare .us)
- [ ] ET PHISHING DNS Query to TOAD Domain (b2care .us)
- [ ] ET PHISHING DNS Query to TOAD Domain (bshelp .live)
- [ ] ET PHISHING DNS Query to TOAD Domain (axhelp .us)
- [ ] ET PHISHING DNS Query to TOAD Domain (a2care .cc)
- [ ] ET PHISHING DNS Query to TOAD Domain (mshelp09 .live)
- [ ] ET PHISHING DNS Query to TOAD Domain (cashapphelp2 .us)
- [ ] ET PHISHING DNS Query to TOAD Domain (hshelp .cc)
- [ ] ET PHISHING DNS Query to TOAD Domain (bghelp .live)
- [ ] ET PHISHING DNS Query to TOAD Domain (h2care .us)
- [ ] ET PHISHING DNS Query to TOAD Domain (bghelp .cc)
- [ ] ET PHISHING DNS Query to TOAD Domain (q2care .us)
- [ ] ET PHISHING DNS Query to TOAD Domain (c2care .us)
- [ ] ET PHISHING Observed TOAD Domain (r2care .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (hscare .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (bscare .live in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (cshelp03 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (hscare .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (bghelp .live in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (bshelp .info in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (d2care .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (g2care .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (a2care .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (bscare .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (n2care .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (mshelp09 .live in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (b2care .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (bscare .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (bshelp .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (h2care .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (q2care .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (a2care .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (axhelp .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (i2care .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (bghelp .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (dfhelp .live in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (bgcare .live in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (hshelp .live in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (brhelp .live in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (bghelp .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (b2care .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (bscare .info in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (kelbyonel .nl in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (hshelp .info in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (bshelp .support in TLS SNI)
- [x] ET PHISHING Generic Phish Landing Page (2023-10-26)
- [x] ET PHISHING Generic Phish Landing Page (2023-10-30)
- [x] ET PHISHING SWAT USA Drop Login Panel
- [x] ET PHISHING Successful Greatness Credential Phish M2 (2023-11-07)
- [ ] ET PHISHING Possible Generic Credential Phish with Obfuscated Javascript
- [x] ET PHISHING Suspected Evri Phish Landing Page 2023-12-01
- [x] ET PHISHING TA444 Domain in DNS Lookup (team-meet .xyz)
- [x] ET PHISHING TA444 Domain in DNS Lookup (onelao .line .pm)
- [x] ET PHISHING TA444 Domain in DNS Lookup (meetingverse .app)
- [x] ET PHISHING TA444 Domain in DNS Lookup (online-processing .online)
- [x] ET PHISHING TA444 Domain in DNS Lookup (group-meeting .team)
- [x] ET PHISHING TA444 Domain in DNS Lookup (privymeet .com)
- [x] ET PHISHING TA444 Domain in DNS Lookup (blackleopard .myvnc .com)
- [x] ET PHISHING TA444 Domain in DNS Lookup (skyboxdrive .cloud)
- [x] ET PHISHING TA444 Domain in DNS Lookup (team-meeting .xyz)
- [x] ET PHISHING TA444 Domain in DNS Lookup (online-meeting .team)
- [x] ET PHISHING TA444 Domain in DNS Lookup (team-meet .online)

- [ ] ET PHISHING DNS Query to TOAD Domain (hshelp .us)
- [ ] ET PHISHING DNS Query to TOAD Domain (h2care .cc)
- [ ] ET PHISHING DNS Query to TOAD Domain (bscare .live)
- [ ] ET PHISHING DNS Query to TOAD Domain (suvfix .us)
- [ ] ET PHISHING DNS Query to TOAD Domain (g2care .cc)
- [ ] ET PHISHING DNS Query to TOAD Domain (i2care .cc)
- [ ] ET PHISHING DNS Query to TOAD Domain (n2care .cc)
- [ ] ET PHISHING DNS Query to TOAD Domain (bscare .us)
- [ ] ET PHISHING DNS Query to TOAD Domain (a2care .us)
- [ ] ET PHISHING DNS Query to TOAD Domain (bgcare .cc)
- [ ] ET PHISHING DNS Query to TOAD Domain (bgcare .help)
- [ ] ET PHISHING DNS Query to TOAD Domain (bgcare .online)
- [ ] ET PHISHING DNS Query to TOAD Domain (d2care .us)
- [ ] ET PHISHING Observed TOAD Domain (nxhelp .live in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (bgcare .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (bgcare .online in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (c2care .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (a2help .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (h2care .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (bgcare .info in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (cashapphelp2 .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (c2care .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (hscare .info in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (hscare .online in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (hshelp .online in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (n2care .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (i2care .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (bghelp .online in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (bscare .help in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (g2care .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (j2care .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (r2care .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (d2care .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (bgcare .help in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (suvfix .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (m2care .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (j2care .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (bshelp .live in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (m2care .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (hshelp .cc in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (cancel247 .info in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (hshelp .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (hscare .live in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (catreenpr .is in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (aphelp .us in TLS SNI)
- [ ] ET PHISHING Observed TOAD Domain (bgcare .us in TLS SNI)
- [x] ET PHISHING Generic Phish Landing Page (2023-10-26)
- [x] ET PHISHING SWAT USA Drop Login Panel
- [x] ET PHISHING Successful Greatness Credential Phish M1 (2023-11-07)
- [x] ET PHISHING Successful Greatness Credential Phish M3 (2023-11-07)
- [x] ET PHISHING Tycoon Landing Page
- [x] ET PHISHING USPS Phish Landing Page 2023-12-05
- [x] ET PHISHING TA444 Domain in DNS Lookup (team-meeting .pro)
- [x] ET PHISHING TA444 Domain in DNS Lookup (tiena .einei .line .pm)
- [x] ET PHISHING TA444 Domain in DNS Lookup (ovcloud .online)
- [x] ET PHISHING TA444 Domain in DNS Lookup (meeting-online .site)
- [x] ET PHISHING TA444 Domain in DNS Lookup (group-meeting .online)
- [x] ET PHISHING TA444 Domain in DNS Lookup (naverk .myvnc .com)
- [x] ET PHISHING TA444 Domain in DNS Lookup (bitscrunch .myvnc .com)
- [x] ET PHISHING TA444 Domain in DNS Lookup (meetcentralhub .online)
- [x] ET PHISHING TA444 Domain in DNS Lookup (syncmeet .online)
- [x] ET PHISHING TA444 Domain in DNS Lookup (safemeeting .online)
- [x] ET PHISHING TA444 Domain in DNS Lookup (videomeethub .online)

- ET PHISHING TA444 Domain in DNS Lookup (myself .hopto .org)
- ET PHISHING TA444 Domain in DNS Lookup (dubai .network .cloud .doc-shared .linkpc .net)
- ET PHISHING TA444 Domain in DNS Lookup (internal .bounceme .net)
- ET PHISHING TA444 Domain in DNS Lookup (pdf .cisco-webex .online)
- ET PHISHING TA444 Domain in DNS Lookup (docshared .col-link .linkpc .net)
- ET PHISHING TA444 Domain in DNS Lookup (bitscrunch .pd .linkpc .net)
- ET PHISHING TA444 Domain in DNS Lookup (internal .group .link-net .publicvm .com)
- ET PHISHING TA444 Domain in DNS Lookup (bitscrunch .im .linkpc .net)
- ET PHISHING TA444 Domain in DNS Lookup (bitscrunch .deck .linkpc .net)
- ET PHISHING TA444 Domain in TLS SNI (team-meet .xyz)
- ET PHISHING TA444 Domain in TLS SNI (onelao .line .pm)
- ET PHISHING TA444 Domain in TLS SNI (meetingverse .app)
- ET PHISHING TA444 Domain in TLS SNI (online-processing .online)
- ET PHISHING TA444 Domain in TLS SNI (group-meeting .team)
- ET PHISHING TA444 Domain in TLS SNI (privymeet .com)
- ET PHISHING TA444 Domain in TLS SNI (blackleopard .myvnc .com)
- ET PHISHING TA444 Domain in TLS SNI (skyboxdrive .cloud)
- ET PHISHING TA444 Domain in TLS SNI (team-meeting .xyz)
- ET PHISHING TA444 Domain in TLS SNI (online-meeting .team)
- ET PHISHING TA444 Domain in TLS SNI (team-meet .online)
- ET PHISHING TA444 Domain in TLS SNI (myself .hopto .org)
- ET PHISHING TA444 Domain in TLS SNI (dubai .network .cloud .doc-shared .linkpc .net)
- ET PHISHING TA444 Domain in TLS SNI (internal .bounceme .net)
- ET PHISHING TA444 Domain in TLS SNI (pdf .cisco-webex .online)
- ET PHISHING TA444 Domain in TLS SNI (docshared .col-link .linkpc .net)
- ET PHISHING TA444 Domain in TLS SNI (bitscrunch .pd .linkpc .net)
- ET PHISHING TA444 Domain in TLS SNI (internal .group .link-net .publicvm .com)
- ET PHISHING TA444 Domain in TLS SNI (bitscrunch .im .linkpc .net)
- ET PHISHING TA444 Domain in TLS SNI (bitscrunch .deck .linkpc .net)
- ET PHISHING Tycoon Landing Page
- ET PHISHING Lucy Security Time Tracking - Phishing Simulation
- ET PHISHING Lucy Security - Phishing Landing Page M3
- ET PHISHING Meta Credential Phish Landing Page 2024-01-08
- ET PHISHING Metamask Credential Phish Landing Page 2024-01-24
- ET PHISHING Observed TOAD Domain (desktool .buzz in TLS SNI)
- ET PHISHING Observed TOAD Domain (mvhelp .cc in TLS SNI)
- ET PHISHING [TW] Possible Crypto Wallet Drainer JS M2
- ET PHISHING ResumeLooter Domain in DNS Lookup (qu3 .cc)
- ET PHISHING ResumeLooter Domain in DNS Lookup (8t .ae)
- ET PHISHING ResumeLooter Domain in DNS Lookup (foundit .asia)
- ET PHISHING ResumeLooter Domain in DNS Lookup (9gp .cc)
- ET PHISHING ResumeLooter Domain in DNS Lookup (iimjobs .asia)
- ET PHISHING Observed ResumeLooter Domain (qu3 .cc in TLS SNI)
- ET PHISHING Observed ResumeLooter Domain (8t .ae in TLS SNI)
- ET PHISHING Observed ResumeLooter Domain (foundit .asia in TLS SNI)
- ET PHISHING Observed ResumeLooter Domain (9gp .cc in TLS SNI)
- ET PHISHING Observed ResumeLooter Domain (iimjobs .asia in TLS SNI)
- ET PHISHING Observed DNS Query to Phishing Related Domain [Redacted - Vulgar]
- ET PHISHING Generic Phish Landing Page 2024-02-12
- ET PHISHING Savvy Seahorse CNAME TDS Related Domain in DNS Lookup (b36cname .site)
- ET PHISHING DNS Query to TA455 Domain (teledyneflir.com .de)
- ET PHISHING TA444 Domain in DNS Lookup (manchestercity .work .gd)
- ET PHISHING TA444 Domain in DNS Lookup (group .evalaskatours .com)
- ET PHISHING TA444 Domain in DNS Lookup (mclearoptical .com)
- ET PHISHING TA444 Domain in DNS Lookup (support .cisco-webex .online)
- ET PHISHING TA444 Domain in DNS Lookup (bitscrunch .presentations .life)
- ET PHISHING TA444 Domain in DNS Lookup (on-global .xyz)
- ET PHISHING TA444 Domain in DNS Lookup (j-ic .co .intneral-document-he-gr-me .run .place)
- ET PHISHING TA444 Domain in DNS Lookup (doc .global-link .run .place)
- ET PHISHING TA444 Domain in DNS Lookup (bitscrunch .co)
- ET PHISHING TA444 Domain in TLS SNI (team-meeting .pro)
- ET PHISHING TA444 Domain in TLS SNI (tiena .einei .line .pm)
- ET PHISHING TA444 Domain in TLS SNI (ovcloud .online)
- ET PHISHING TA444 Domain in TLS SNI (meeting-online .site)
- ET PHISHING TA444 Domain in TLS SNI (group-meeting .online)
- ET PHISHING TA444 Domain in TLS SNI (naverk .myvnc .com)
- ET PHISHING TA444 Domain in TLS SNI (bitscrunch .myvnc .com)
- ET PHISHING TA444 Domain in TLS SNI (meetcentralhub .online)
- ET PHISHING TA444 Domain in TLS SNI (syncmeet .online)
- ET PHISHING TA444 Domain in TLS SNI (safemeeting .online)
- ET PHISHING TA444 Domain in TLS SNI (videomeethub .online)
- ET PHISHING TA444 Domain in TLS SNI (manchestercity .work .gd)
- ET PHISHING TA444 Domain in TLS SNI (group .evalaskatours .com)
- ET PHISHING TA444 Domain in TLS SNI (mclearoptical .com)
- ET PHISHING TA444 Domain in TLS SNI (support .cisco-webex .online)
- ET PHISHING TA444 Domain in TLS SNI (bitscrunch .presentations .life)
- ET PHISHING TA444 Domain in TLS SNI (on-global .xyz)
- ET PHISHING TA444 Domain in TLS SNI (j-ic .co .intneral-document-he-gr-me .run .place)
- ET PHISHING TA444 Domain in TLS SNI (doc .global-link .run .place)
- ET PHISHING TA444 Domain in TLS SNI (bitscrunch .co)
- ET PHISHING Obfuscated Javascript from Generic Phishkit
- ET PHISHING Lucy Security - Credential Submission (set)
- ET PHISHING Lucy Security - Phishing to Awareness Landing Page
- ET PHISHING Successful Metamask PassPhrase Phish 2024-01-24
- ET PHISHING DNS Query to TOAD Domain (desktool .buzz)
- ET PHISHING DNS Query to TOAD Domain (mvhelp .cc)
- ET PHISHING [TW] Possible Crypto Wallet Drainer JS M1
- ET PHISHING [TW] Possible Crypto Wallet Drainer Domain Observed
- ET PHISHING ResumeLooter Domain in DNS Lookup (7o .ae)
- ET PHISHING ResumeLooter Domain in DNS Lookup (cloudnetsofe .com)
- ET PHISHING ResumeLooter Domain in DNS Lookup (xn--31-rha .me)
- ET PHISHING ResumeLooter Domain in DNS Lookup (8r .ae)
- ET PHISHING ResumeLooter Domain in DNS Lookup (sb8 .co)
- ET PHISHING Observed ResumeLooter Domain (7o .ae in TLS SNI)
- ET PHISHING Observed ResumeLooter Domain (cloudnetsofe .com in TLS SNI)
- ET PHISHING Observed ResumeLooter Domain (xn--31-rha .me in TLS SNI)
- ET PHISHING Observed ResumeLooter Domain (8r .ae in TLS SNI)
- ET PHISHING Observed ResumeLooter Domain (sb8 .co in TLS SNI)
- ET PHISHING Observed Phishing Related Domain [Redacted - Vulgar]
- ET PHISHING Successful Generic Phish 2024-02-12
- ET PHISHING Savvy Seahorse CNAME TDS Related Domain in DNS Lookup (getyourapi .site)
- ET PHISHING DNS Query to TA455 Domain (1stemployer .com)

- [x] ET PHISHING DNS Query to TA455 Domain (vsliveagent .com)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (vscodeupdater .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (airconnectionsapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (testmanagementapisjson .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (iaidevrssfeed .cloudapp .azure .com)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (apphrquizapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (notebooktextchecking .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (questionsapplicationbackup .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (customercareservice .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (blogvolleyballstatus .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (emirateschecksapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (questionsurveyapp .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (manpowerfeedapijson .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (airconnectionapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (coffeeonlineshop .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (javaruntimestestapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (iaidevrssfeedp .cloudapp .azure .com)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (roadmapselector .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (engineeringssfeed .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (integratedblognewsapi .azurewebsites .com)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (airgadgetsolutions .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (qaquestionapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (iaidevrssfeed .centrualus .cloudapp .azure .com)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (boeisurveyapplications .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (helicopterahtest .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (altnametestapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (ilengineeringrssfeed .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (integratedblognewfeed .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (javaruntimeversionchecking .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (connectairapijson .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (integratedblognewsapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (notebooktextcheckings .com)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (surveyonlinetest .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (questionsapplicationapijson .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (qaquestionsapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (helicoptersahtests .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (regionuaequestions .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (blognewsalphaapijson .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (notebooktextcheckings .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (onequestionsapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (onequestionsapicheck .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (arquestionsapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (uaeaircheckon .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (iaidevrssfeed .centralus .cloudapp .azure .com)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (notebooktexts .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (quiztestapplication .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (engineeringrssfeed .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (javaruntime .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (onequestions .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (logupdatemanagementapijson .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (qaquestions .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (homefurniture .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (blogvolleyballstatusapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (technewsblogapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (emirateschecksapijson .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (airgadgetsolution .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (surveyappquery .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (jupyternotebookcollection .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (hrapplicationtest .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (identifycheckapplication .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (manpowerfeedapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (workersquestionsapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (optionalapplication .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (flighthelicopterahtest .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (customercareserviceapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (exchtestcheckingapihealth .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (questionsdatabases .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (humanresourcesapijson .azurewebsites .net)

- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (openapplicationcheck .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (workersquestionsjson .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (checkapicountryquestionsjson .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (changequestionstypeapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (cashcloudservices .com)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (audiomanagerapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (exchtestcheckingapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (personalizationsurvey .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (turkairline .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (testquestionapplicationapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (registerinsurance .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (countrybasedquestions .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (javaruntimetestapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (logupdatemanagementapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (sportblogs .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (intergratedblognewsapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (queryquestions .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (audioservicetestapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (uaeairchecks .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (refaeldevrssfeed .centralus .cloudapp .azure .com)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (personalitytestquestionapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (humanresourcesapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (testtesttes .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (jupyternotebookcollections .com)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (helicopterahtests .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (testmanagementapi1 .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (answerssurveytest .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (changequestionstypejsonapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (logsapimanagements .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (identifycheckapplications .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (testmanagementapis .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (arquestions .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (birngthemhomenow .co .il)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (logsapimanagement .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (browsercheckap .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (integratedblognews .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (intengineeringrssfeed .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (questionsurveyappserver .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (coffeeonlineshoping .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (surveyonlinetestapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (questionsapplicationapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (identifycheckingapplications .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (tnlsowki .westus3 .cloudapp .azure .com)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (hiringarabicregion .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (apphrquestion .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (browsercheckingapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (qaquestionsapijson .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (changequestiontypesapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (queryfindquestions .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (checkapicountryquestions .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (workersquestions .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (jupyternotebookscollection .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (apphrquestions .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (tnlsowkis .westus3 .cloudapp .azure .com)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (checkservicecustomerapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (humanresourcesapiquiz .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (jupyternotebookcollections .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (changequestiontypes .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (browsercheckjson .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (airconnectionsapijson .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (marineblogapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (javaruntimeversioncheckingapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (connectionhandlerapi .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (tiappschecktest .azurewebsites .net)
- [x] ET PHISHING DNS Query to UNC1549/TA455 Domain (roadmapselectorapi .azurewebsites .net)

- [ ] **emerging-policy.rules** Show
- [x] **emerging-pop3.rules** Hide

- [ ] GPL POP3 x86 BSD overflow
- [x] GPL POP3 x86 Linux overflow
- [x] GPL POP3 POP3 PASS overflow attempt
- [ ] GPL POP3 USER overflow attempt
- [x] GPL POP3 LIST overflow attempt
- [ ] GPL POP3 CAPA overflow attempt
- [x] GPL POP3 STAT overflow attempt
- [ ] GPL POP3 RSET overflow attempt
- [ ] GPL POP3 UIDL negative argument attempt
- [x] GPL POP3 APOP USER overflow attempt
- [ ] GPL POP3 x86 BSD overflow 2
- [x] GPL POP3 x86 SCO overflow
- [x] GPL POP3 APOP overflow attempt
- [x] GPL POP3 AUTH overflow attempt
- [x] GPL POP3 XTND overflow attempt
- [ ] GPL POP3 TOP overflow attempt
- [ ] GPL POP3 DELE overflow attempt
- [ ] GPL POP3 DELE negative argument attempt
- [ ] GPL POP3 USER format string attempt
- [ ] GPL POP3 PASS format string attempt

- [x] **emerging-rpc.rules** Hide

- [x] ET RPC DCERPC SVCCTL - Remote Service Control Manager Access
- [ ] GPL RPC mountd TCP export request
- [x] GPL RPC portmap amountd request UDP
- [x] GPL RPC portmap cmsd request UDP
- [x] GPL RPC portmap nisd request UDP
- [x] GPL RPC portmap rexd request UDP
- [x] GPL RPC portmap rusers request UDP
- [x] GPL RPC portmap selection_svc request UDP
- [x] GPL RPC portmap ttdbserv request UDP
- [x] GPL RPC portmap ypserv request UDP
- [x] GPL RPC portmap snmpXdmi request TCP
- [x] GPL RPC portmap listing TCP 111
- [x] GPL RPC rlogin login failure
- [x] GPL RPC portmap admind request TCP
- [x] GPL RPC portmap bootparam request TCP
- [x] GPL RPC portmap nisd request TCP
- [x] GPL RPC portmap rexd request TCP
- [x] GPL RPC portmap rusers request TCP
- [x] GPL RPC portmap selection_svc request TCP
- [x] GPL RPC portmap yppasswd request TCP
- [x] GPL RPC portmap ypupdated request UDP
- [x] GPL RPC portmap listing UDP 111
- [x] GPL RPC portmap rwalld request UDP
- [x] GPL RPC portmap cachefsd request UDP
- [x] GPL RPC xdmcp info query
- [x] GPL RPC CMSD UDP CMSD_CREATE buffer overflow attempt
- [x] GPL RPC CMSD TCP CMSD_INSERT buffer overflow attempt
- [x] GPL RPC STATD UDP stat mon_name format string exploit attempt
- [x] GPL RPC STATD UDP monitor mon_name format string exploit attempt
- [x] GPL RPC portmap proxy attempt TCP
- [ ] GPL RPC mountd UDP export request
- [ ] GPL RPC mountd UDP exportall request
- [x] GPL RPC portmap SET attempt UDP 111
- [ ] GPL RPC mountd UDP mount request
- [ ] GPL RPC sadmind TCP PING
- [x] GPL RPC portmap NFS request TCP
- [x] GPL RPC portmap RQUOTA request TCP
- [x] GPL RPC tooltalk UDP overflow attempt
- [x] GPL RPC portmap kcms_server request UDP
- [x] GPL RPC kcms_server directory traversal attempt
- [x] GPL RPC portmap UNSET attempt UDP 111
- [x] GPL RPC portmap espd request UDP
- [ ] GPL RPC mountd UDP dump request
- [ ] GPL RPC mountd UDP unmount request
- [x] GPL RPC yppasswd username overflow attempt UDP
- [ ] GPL RPC yppasswd old password overflow attempt UDP
- [ ] GPL RPC yppasswd new password overflow attempt UDP
- [ ] GPL RPC yppasswd user update UDP
- [ ] GPL RPC ypserv maplist request UDP
- [x] GPL RPC portmap network-status-monitor request TCP
- [ ] GPL RPC portmap nlockmgr request TCP
- [x] GPL RPC portmap rpc.xfsmd request TCP
- [x] GPL RPC snmpXdmi overflow attempt TCP
- [x] GPL RPC portmap admind request UDP
- [x] GPL RPC portmap bootparam request UDP
- [x] GPL RPC portmap mountd request UDP
- [x] GPL RPC portmap pcnfsd request UDP
- [x] GPL RPC portmap rstatd request UDP
- [x] GPL RPC portmap sadmind request UDP
- [x] GPL RPC portmap status request UDP
- [x] GPL RPC portmap yppasswd request UDP
- [x] GPL RPC portmap ypupdated request TCP
- [x] GPL RPC portmap espd request TCP
- [x] GPL RPC rlogin LinuxNIS
- [x] GPL RPC rlogin login failure
- [x] GPL RPC portmap amountd request TCP
- [x] GPL RPC portmap cmsd request TCP
- [x] GPL RPC portmap pcnfsd request TCP
- [x] GPL RPC portmap rstatd request TCP
- [x] GPL RPC portmap sadmind request TCP
- [x] GPL RPC portmap ttdbserv request TCP
- [x] GPL RPC portmap ypserv request TCP
- [x] GPL RPC portmap snmpXdmi request UDP
- [ ] GPL RPC portmap listing UDP 32771
- [x] GPL RPC portmap rwalld request TCP
- [x] GPL RPC portmap cachefsd request TCP
- [ ] GPL RPC status GHBN format string attack
- [x] GPL RPC CMSD TCP CMSD_CREATE buffer overflow attempt
- [x] GPL RPC sadmind TCP NETMGT_PROC_SERVICE CLIENT_DOMAIN overflow attempt
- [x] GPL RPC STATD TCP stat mon_name format string exploit attempt
- [x] GPL RPC STATD TCP monitor mon_name format string exploit attempt
- [x] GPL RPC portmap proxy attempt UDP
- [ ] GPL RPC mountd TCP exportall request
- [x] GPL RPC portmap SET attempt TCP 111
- [ ] GPL RPC mountd TCP mount request
- [ ] GPL RPC sadmind UDP PING
- [x] GPL RPC portmap NFS request UDP
- [x] GPL RPC portmap RQUOTA request UDP
- [x] GPL RPC RQUOTA getquota overflow attempt UDP
- [x] GPL RPC tooltalk TCP overflow attempt
- [x] GPL RPC portmap kcms_server request TCP
- [x] GPL RPC portmap UNSET attempt TCP 111
- [x] GPL RPC portmap status request TCP
- [ ] GPL RPC mountd TCP dump request
- [ ] GPL RPC mountd TCP unmount request
- [ ] GPL RPC mountd TCP unmountall request
- [ ] GPL RPC yppasswd username overflow attempt TCP
- [ ] GPL RPC yppasswd old password overflow attempt TCP
- [ ] GPL RPC yppasswd new password overflow attempt TCP
- [ ] GPL RPC yppasswd user update TCP
- [x] GPL RPC portmap network-status-monitor request UDP
- [ ] GPL RPC portmap nlockmgr request UDP
- [ ] GPL RPC portmap rpc.xfsmd request UDP
- [ ] GPL RPC rpc.xfsmd xfs_export attempt UDP

- [ ] GPL RPC rpc.xfsmd xfs_export attempt TCP
- [x] GPL RPC portmap proxy integer overflow attempt TCP
- [ ] GPL RPC CMSD TCP CMSD_CREATE array buffer overflow attempt
- [ ] GPL RPC rexec password overflow attempt
- [x] GPL RPC mountd UDP mount path overflow attempt
- [x] GPL RPC sadmind query with root credentials attempt UDP
- [ ] GPL RPC kerberos principal name overflow TCP
- [ ] GPL RPC ypupdated arbitrary command attempt UDP
- [ ] GPL RPC CMSD UDP CMSD_CREATE array buffer overflow attempt
- [x] GPL RPC rexec username too long response
- [x] GPL RPC mountd TCP mount path overflow attempt
- [x] GPL RPC sadmind query with root credentials attempt TCP
- [ ] GPL RPC kerberos principal name overflow UDP

- [x] **emerging-scada.rules** Hide

- [x] ET SCADA CitectSCADA ODBC Overflow Attempt
- [x] ET SCADA DATAC RealWin SCADA Server Buffer Overflow
- [x] ET SCADA DATAC RealWin SCADA Server 2 On_FC_CONNECT_FCS_a_FILE Buffer Overflow Vulnerability
- [x] ET SCADA Golden FTP Server PASS Command Remote Buffer Overflow Attempt
- [x] ET SCADA PcVue Activex Control Insecure method (DeletePage)
- [x] ET SCADA PcVue Activex Control Insecure method (LoadObject)
- [x] ET SCADA Sunway ForceControl Activex Control Vulnerability
- [x] ET SCADA PROMOTIC ActiveX Control Insecure method (SaveCfg)
- [x] ET SCADA SEIG SYSTEM 9 - Remote Code Execution
- [x] ET SCADA IEC-104 TESTFR (Test Frame) Activation
- [x] ET SCADA IEC-104 STARTDT (Start Data Transfer) Activation
- [x] ET SCADA IEC-104 STOPDT (Stop Data Transfer) Activation
- [x] ET SCADA IEC-104 Station Interrogation - Global ASDU Broadcast
- [x] ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Advanced Diagnostics Information Disclosure Attempt - TCP Statistics
- [x] ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation System Data Details Information Disclosure Attempt
- [x] ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Advanced Diagnostics Information Disclosure Attempt - General Memory Statistics
- [x] ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Advanced Diagnostics Information Disclosure Attempt - ICMP Statistics
- [x] ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Advanced Diagnostics Information Disclosure Attempt - ARP Statistics
- [x] ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Advanced Diagnostics Information Disclosure Attempt - IP Statistics
- [x] ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Information Disclosure Attempt - System List
- [x] ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Information Disclosure Attempt - Chassis Detail Request
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL-series Possible Unauthorized Access - Request for home.sel
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL-series Possible Unauthorized Access - Request for default.sel
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL-2488 Possible Unauthorized Access Attempt - Request for /css/sel.css
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL-3530-RTAC AcSELerator Firmware Activity
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL-3620 Default Cert Subject Common Name
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL-2488 Default Cert Subject Common Name
- [ ] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL Telnet Activity
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL 2032 Processor Telnet Banner
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - Access Change
- [x] ET SCADA RealWin SCADA System Buffer Overflow
- [x] ET SCADA ICONICS WebHMI ActiveX Stack Overflow
- [x] ET SCADA Siemens FactoryLink 8 CSService Logging Buffer Overflow Vulnerability
- [x] ET SCADA PcVue Activex Control Insecure method (AddPage)
- [x] ET SCADA PcVue Activex Control Insecure method (SaveObject)
- [x] ET SCADA PcVue Activex Control Insecure method (GetExtendedColor)
- [x] ET SCADA Sunway ForceControl Activex Control Remote Code Execution Vulnerability 2
- [x] ET SCADA PROMOTIC ActiveX Control Insecure method (AddTrend)
- [x] ET SCADA SEIG Modbus 3.4 - Remote Code Execution
- [x] ET SCADA IEC-104 TESTFR (Test Frame) Confirmation
- [x] ET SCADA IEC-104 STARTDT (Start Data Transfer) Confirmation
- [x] ET SCADA IEC-104 STOPDT (Stop Data Transfer) Confirmation
- [x] ET SCADA IEC-104 Clock Synchronization Command
- [x] ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Advanced Diagnostics Information Disclosure Attempt - UDP Statistics
- [x] ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Advanced Diagnostics Information Disclosure Attempt - IP Routing Data
- [x] ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Advanced Diagnostics Information Disclosure Attempt - General Heap Memory Statistics
- [x] ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Advanced Diagnostics Information Disclosure Attempt - IGMP Statistics
- [x] ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Advanced Diagnostics Information Disclosure Attempt - Interface Statistics
- [x] ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Possible Unauthorized Access Attempt - Request for radevice.css
- [x] ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Information Disclosure Attempt - Browse Chasis
- [x] ET SCADA [nsacyber/ELITEWOLF] Allen-Bradley/Rockwell Automation Information Disclosure Attempt - Crashdump Display
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL-series Possible Unauthorized Access Attempt - Request for err401.sel
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL-2488 Possible Unauthorized Access Attempt - Request for /scripts/dScripts.sel
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL-series Dropbear SSH Banner - Possible SSH Login attempt
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL-3620 Default X509 Certificate String
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL-3620 Default Cert Issuer Common Name
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL-2488 Default Cert Issuer Common Name
- [ ] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL Telnet Elevated Access
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL Calibration Access Level Login Success
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - Change working directory 2701

- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - Current directory /SEL-2701
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - DNPMAP.TXT File Download Attempt
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - STOR SET_DNP1.TXT File Upload Attempt
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - SET_ File Upload Attempt
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - User ACC Login Attempt
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - Default Password otter
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - DNPMAP.TXT File Upload Attempt
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - ERR.TXT File Download Attempt
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - SET_DNP1.TXT File Download Attempt
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - SET_ File Download Attempt
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - Default User Account FTPUSER Login Attempt
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - Default User Account Password TAIL Login Attempt
- [x] ET SCADA [nsacyber/ELITEWOLF] Schweitzer Engineering Laboratories SEL FTP Server Activity - SEL-751A FTP Banner Observed
- [x] ET SCADA [nsacyber/ELITEWOLF] Possible Siemens S7-1200 Unauthorized Access Attempt - Request for /Images/CPU1200/
- [x] ET SCADA [nsacyber/ELITEWOLF] Possible Siemens S7-1200 Unauthorized Access Attempt - Request for /CSS/S7Web.css
- [x] ET SCADA [nsacyber/ELITEWOLF] Siemens S7-1200 Default X509 Certificate String
- [x] ET SCADA [nsacyber/ELITEWOLF] Siemens S7-1200 Default Cert Subject Common Name
- [x] ET SCADA [nsacyber/ELITEWOLF] Siemens S7-1200 Default Cert Issuer Common Name
- [x] ET SCADA [nsacyber/ELITEWOLF] Siemens S7 Redpoint NSE Request CPU Function Read SZL attempt
- [x] ET SCADA [nsacyber/ELITEWOLF] Tridium NiagaraAX Default X509 Certificate String
- [x] ET SCADA [nsacyber/ELITEWOLF] Tridium NiagaraAX Default Cert Subject Common Name
- [x] ET SCADA [nsacyber/ELITEWOLF] Tridium NiagaraAX Default Cert Issuer Common Name
- [x] ET SCADA [nsacyber/ELITEWOLF] Tridium NiagaraN4 Default X509 Certificate String
- [x] ET SCADA [nsacyber/ELITEWOLF] Tridium NiagaraN4 Default Cert Subject Common Name
- [x] ET SCADA [nsacyber/ELITEWOLF] Tridium NiagaraN4 Default Cert Issuer Common Name
- [x] ET SCADA [nsacyber/ELITEWOLF] Tridium Niagara4 Default X509 Certificate String
- [x] ET SCADA [nsacyber/ELITEWOLF] Tridium Niagara4 Default Cert Subject Common Name
- [x] ET SCADA [nsacyber/ELITEWOLF] Tridium Niagara4 Default Cert Issuer Common Name
- [x] ET SCADA [nsacyber/ELITEWOLF] Tridium Niagara Default X509 Certificate
- [x] ET SCADA [nsacyber/ELITEWOLF] Tridium Niagara Default Cert Subject Common Name
- [x] ET SCADA [nsacyber/ELITEWOLF] Tridium Niagara Default Cert Issuer Common Name
- [x] ET SCADA Rockwell RNA Message Large Header Length - 8Kb

- [x] **emerging-scan.rules** Hide

- [ ] ET SCAN NMAP -sO
- [ ] ET SCAN NMAP -sS window 2048
- [ ] ET SCAN NMAP -sA (1)
- [ ] ET SCAN NMAP -sA (2)
- [ ] ET SCAN NMAP -f -sF
- [ ] ET SCAN NMAP -f -sN
- [ ] ET SCAN NMAP -f -sV
- [ ] ET SCAN NMAP -f -sX
- [x] ET SCAN ICMP PING IPTools
- [x] ET SCAN Potential SSH Scan
- [ ] ET SCAN Possible SSL Brute Force attack or Site Crawl
- [x] ET SCAN Behavioral Unusual Port 445 traffic Potential Scan or Infection
- [x] ET SCAN Behavioral Unusual Port 139 traffic Potential Scan or Infection
- [x] ET SCAN Behavioral Unusual Port 137 traffic Potential Scan or Infection
- [x] ET SCAN Behavioral Unusual Port 135 traffic Potential Scan or Infection
- [x] ET SCAN Behavioral Unusual Port 1434 traffic Potential Scan or Infection
- [x] ET SCAN Behavioral Unusual Port 1433 traffic Potential Scan or Infection
- [ ] ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force
- [x] ET SCAN MYSQL 4.0 brute force root login attempt
- [x] ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)
- [x] ET SCAN Potential FTP Brute-Force attempt response
- [x] ET SCAN Nessus User Agent
- [x] ET SCAN Nikto Web App Scan in Progress
- [ ] ET SCAN Yahoo Crawler Crawl
- [x] ET SCAN MYSQL 4.1 brute force root login attempt
- [x] ET SCAN Potential VNC Scan 5800-5820
- [x] ET SCAN Potential VNC Scan 5900-5920
- [ ] ET SCAN Behavioral Unusual Port 3127 traffic, Potential Scan or Backdoor
- [x] ET SCAN Rapid POP3 Connections - Possible Brute Force Attack
- [x] ET SCAN Rapid POP3S Connections - Possible Brute Force Attack
- [x] ET SCAN Rapid IMAP Connections - Possible Brute Force Attack
- [x] ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack
- [x] ET SCAN Potential SSH Scan OUTBOUND
- [x] ET SCAN IBM NSA User Agent
- [x] ET SCAN PHP Attack Tool Morfeus F Scanner
- [ ] ET SCAN Suspicious User-Agent - get-minimal - Possible Vuln Scan
- [x] ET SCAN ProxyReconBot CONNECT method to Mail
- [ ] ET SCAN ProxyReconBot POST method to Mail
- [x] ET SCAN WebHack Control Center User-Agent Inbound (WHCC/)
- [x] ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack
- [x] ET SCAN w3af User Agent
- [x] ET SCAN Grim's Ping ftp scanning tool
- [x] ET SCAN Internal to Internal UPnP Request tcp port 2555
- [x] ET SCAN External to Internal UPnP Request tcp port 2555

- [x] ET SCAN External to Internal UPnP Request udp port 1900
- [x] ET SCAN DirBuster Web App Scan in Progress
- [x] ET SCAN Suspicious User-Agent inbound (bot)
- [x] ET SCAN Watchfire AppScan Web App Vulnerability Scanner
- [x] ET SCAN bsqlbf Brute Force SQL Injection
- [x] ET SCAN Cisco Torch IOS HTTP Scan
- [x] ET SCAN Wapiti Web Server Vulnerability Scan
- [x] ET SCAN Tomcat Auth Brute Force attempt (tomcat)
- [x] ET SCAN Smap VOIP Device Scan
- [x] ET SCAN Hmap Webserver Fingerprint Scan
- [x] ET SCAN NNG MS02-039 Exploit False Positive Generator - May Conceal A Genuine Attack
- [x] ET SCAN Acunetix Version 6 Crawl/Scan Detected
- [x] ET SCAN Sipvicious Scan
- [x] ET SCAN Sipsak SIP scan
- [x] ET SCAN Enumiax Inter-Asterisk Exchange Protocol Username Scan
- [x] ET SCAN Sivus VOIP Vulnerability Scanner SIP Components Scan
- [x] ET SCAN Httprecon Web Server Fingerprint Scan
- [x] ET SCAN Wikto Backend Data Miner Scan
- [x] ET SCAN sipscan probe
- [x] ET SCAN Mini MySqlatOr SQL Injection Scanner
- [x] ET SCAN SQLNinja MSSQL XPCmdShell Scan
- [x] ET SCAN SQLNinja MSSQL Database User Rights Scan
- [x] ET SCAN SQLNinja Attempt To Recreate xp_cmdshell Using sp_configure
- [x] ET SCAN Automated Injection Tool User-Agent (AutoGetColumn)
- [x] ET SCAN Toata Scanner User-Agent Detected
- [x] ET SCAN Tomcat admin-blank login credentials
- [ ] ET SCAN Modbus Scanning detected
- [x] ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
- [ ] ET SCAN Possible jBroFuzz Fuzzer Detected
- [x] ET SCAN Asp-Audit Web Scan Detected
- [x] ET SCAN Grendel-Scan Web Application Security Scan Detected
- [x] ET SCAN Absinthe SQL Injection Tool HTTP Header Detected
- [ ] ET SCAN NMAP -sS window 3072
- [x] ET SCAN Acunetix Version 6 (Free Edition) Scan Detected
- [ ] ET SCAN Multiple NBTStat Query Responses to External Destination, Possible Automated Windows Network Enumeration
- [x] ET SCAN SQL Power Injector SQL Injection User Agent Detected
- [x] ET SCAN DCERPC rpcmgmt ifids Unauthenticated BIND
- [x] ET SCAN Default Mysqloit User Agent Detected - Mysql Injection Takover Tool
- [ ] ET SCAN Unusually Fast 400 Error Messages (Bad Request), Possible Web Application Scan
- [x] ET SCAN Tomcat Web Application Manager scanning
- [x] ET SCAN Suspicious User-Agent Containing Web Scan/er Likely Web Scanner
- [x] ET SCAN SQL Injection Attempt (Agent uil2pn)
- [x] ET SCAN Amap TCP Service Scan Detected
- [x] ET SCAN Non-Allowed Host Tried to Connect to MySQL Server
- [x] ET SCAN Springenwerk XSS Scanner User-Agent Detected
- [x] ET SCAN Multiple FTP Root Login Attempts from Single Source - Possible Brute Force Attempt
- [x] ET SCAN ICMP Delphi Likely Precursor to Scan
- [x] ET SCAN ZmEu exploit scanner
- [x] ET SCAN Suspicious inbound to MSSQL port 1433
- [x] ET SCAN Suspicious inbound to mySQL port 3306
- [x] ET SCAN Suspicious inbound to PostgreSQL port 5432
- [x] ET SCAN crimscanner User-Agent detected
- [x] ET SCAN WhatWeb Web Application Fingerprint Scanner Default User-Agent Detected
- [x] ET SCAN PRO Search Crawler Probe
- [x] ET SCAN Paros Proxy Scanner Detected
- [ ] ET SCAN Behavioral Unusually fast outbound Telnet Connections, Potential Scan or Brute Force
- [x] ET SCAN DEBUG Method Request with Command
- [x] ET SCAN Cisco Torch TFTP Scan
- [x] ET SCAN Httprint Web Server Fingerprint Scan
- [x] ET SCAN Tomcat Auth Brute Force attempt (admin)
- [x] ET SCAN Tomcat Auth Brute Force attempt (manager)
- [x] ET SCAN Core-Project Scanning Bot UA Detected
- [x] ET SCAN Sqlmap SQL Injection Scan
- [x] ET SCAN Voiper Toolkit Torturer Scan
- [x] ET SCAN Voiper Fuzzing Scan
- [x] ET SCAN Sipp SIP Stress Test Detected
- [x] ET SCAN Stompy Web Application Session Scan
- [x] ET SCAN Sivus VOIP Vulnerability Scanner SIP Scan
- [x] ET SCAN Wikto Scan
- [x] ET SCAN WSFuzzer Web Application Fuzzing
- [x] ET SCAN SIP erase_registrations/add registrations attempt
- [x] ET SCAN SQLix SQL Injection Vector Scan
- [x] ET SCAN SQLNinja MSSQL Version Scan
- [x] ET SCAN SQLNinja MSSQL User Scan
- [x] ET SCAN SQLNinja MSSQL Authentication Mode Scan
- [x] ET SCAN SQLNinja Attempt To Create xp_cmdshell Session
- [x] ET SCAN WebShag Web Application Scan Detected
- [x] ET SCAN Tomcat admin-admin login credentials
- [x] ET SCAN Tomcat upload from external source
- [x] ET SCAN Port Unreachable Response to Xprobe2 OS Fingerprint Scan
- [x] ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap NSE)
- [x] ET SCAN SQLBrute SQL Scan Detected
- [x] ET SCAN Grendel Web Scan - Default User Agent Detected
- [x] ET SCAN Grabber.py Web Scan Detected
- [ ] ET SCAN NMAP -sS window 1024
- [ ] ET SCAN NMAP -sS window 4096
- [ ] ET SCAN Unusually Fast 403 Error Messages, Possible Web Application Scan
- [ ] ET SCAN NBTStat Query Response to External Destination, Possible Windows Network Enumeration
- [x] ET SCAN Pavuk User Agent Detected - Website Mirroring Tool for Off-line Analysis
- [x] ET SCAN WITOOL SQL Injection Scan
- [x] ET SCAN Possible Mysqloit Operating System Fingerprint/SQL Injection Test Scan Detected
- [ ] ET SCAN Unusually Fast 404 Error Messages (Page Not Found), Possible Web Application Scan/Directory Guessing Attack
- [x] ET SCAN Suspicious User-Agent Containing SQL Inject/ion Likely SQL Injection Scanner
- [x] ET SCAN Suspicious User-Agent Containing Security Scan/ner Likely Scan
- [ ] ET SCAN pangolin SQL injection tool
- [x] ET SCAN Amap UDP Service Scan Detected
- [x] ET SCAN Multiple MySQL Login Failures Possible Brute Force Attempt
- [x] ET SCAN ICMP @hello request Likely Precursor to Scan
- [x] ET SCAN Multiple FTP Administrator Login Attempts from Single Source - Possible Brute Force Attempt
- [x] ET SCAN ICMP =XXXXXXXX Likely Precursor to Scan
- [x] ET SCAN Open-Proxy ScannerBot (webcollage-UA)
- [x] ET SCAN Suspicious inbound to Oracle SQL port 1521
- [x] ET SCAN Suspicious inbound to mSQL port 4333
- [x] ET SCAN Skipfish Web Application Scan Detected
- [x] ET SCAN Skipfish Web Application Scan Detected (2)
- [x] ET SCAN w3af Scan In Progress ARGENTINA Req Method

- [x] ET SCAN HZZP Scan in Progress calc in Headers
- [x] ET SCAN Netsparker Scan in Progress
- [ ] ET SCAN HTTP POST invalid method case
- [ ] ET SCAN HTTP OPTIONS invalid method case
- [x] ET SCAN DavTest WebDav Vulnerability Scanner Default User Agent Detected
- [ ] ET SCAN Malformed Packet SYN RST
- [x] ET SCAN Nikto Scan Remote File Include Retrieval
- [x] ET SCAN Sipvicious User-Agent Detected (friendly-scanner)
- [x] ET SCAN Possible Fast-Track Tool Spidering User-Agent Detected
- [x] ET SCAN Inspathx Path Disclosure Scanner User-Agent Detected
- [x] ET SCAN Medusa User-Agent
- [x] ET SCAN DotDotPwn User-Agent
- [x] ET SCAN Metasploit WMAP GET len 0 and type
- [x] ET SCAN Goatzapszu Header from unknown Scanning Tool
- [x] ET SCAN Havij SQL Injection Tool User-Agent Inbound
- [x] ET SCAN Possible SQLMAP Scan
- [x] ET SCAN ZmEu Scanner User-Agent Inbound
- [ ] ET SCAN Potential muieblackcat scanner double-URI and HTTP library
- [x] ET SCAN Vega Web Application Scan
- [x] ET SCAN Nessus FTP Scan detected (ftp_writeable_directories.nasl)
- [x] ET SCAN Kingcope KillApache.pl Apache mod_deflate DoS attempt
- [x] ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Outbound)
- [x] ET SCAN NMAP SQL Spider Scan
- [x] ET SCAN Apache mod_proxy Reverse Proxy Exposure 1
- [ ] ET SCAN Gootkit Scanner User-Agent Inbound
- [x] ET SCAN Arachni Scanner Web Scan
- [x] ET SCAN w3af User-Agent 2
- [x] ET SCAN Brutus Scan Outbound
- [x] ET SCAN SFTP/FTP Password Exposure via sftp-config.json
- [x] ET SCAN JCE Joomla Scanner
- [x] ET SCAN GET with HTML tag in start of URI seen with PHPMyAdmin scanning
- [ ] ET SCAN Arachni Web Scan
- [x] ET SCAN SipCLI VOIP Scan
- [x] ET SCAN NETWORK Incoming Masscan detected
- [x] ET SCAN NMAP SIP Version Detect OPTIONS Scan
- [x] ET SCAN Hikvision DVR attempted Synology Recon Scan
- [x] ET SCAN Possible WordPress xmlrpc.php wp.getUsersBlogs Flowbit Set
- [x] ET SCAN Internet Scanning Project HTTP scan
- [x] ET SCAN SSH BruteForce Tool with fake PUTTY version
- [x] ET SCAN H.323 Scanning device
- [x] ET SCAN Nmap NSE Heartbleed Response
- [x] ET SCAN abdullkarem Wordpress PHP Scanner
- [x] ET SCAN COMMIX Command injection scan attempt
- [x] ET SCAN MySQL Malicious Scanning 2
- [x] ET SCAN Redis SSH Key Overwrite Probing
- [x] ET SCAN Acunetix scan in progress acunetix variable in http_uri
- [x] ET SCAN Possible Nmap User-Agent Observed
- [x] ET SCAN NYU Internet Census UA Inbound
- [x] ET SCAN ntop-ng Authentication Bypass via Session ID Guessing
- [x] ET SCAN Geutebrueck re_porter 7.8.974.20 Information Disclosure
- [x] ET SCAN StarDotStar HELO, suspected AUTH LOGIN botnet
- [x] ET SCAN External Host Probing for ChromeCast Devices
- [x] ET SCAN Mirai Variant User-Agent (Inbound)
- [x] ET SCAN Mirai Variant User-Agent (Inbound)
- [x] ET SCAN Mirai Variant User-Agent (Inbound)
- [x] ET SCAN Mirai Variant User-Agent (Inbound)
- [x] ET SCAN Mirai Variant User-Agent (Inbound)
- [x] ET SCAN Mirai Variant User-Agent (Inbound)
- [x] ET SCAN Netsparker Default User-Agent
- [ ] ET SCAN HTTP GET invalid method case
- [ ] ET SCAN HTTP HEAD invalid method case
- [x] ET SCAN Possible DavTest WebDav Vulnerability Scanner Initial Check Detected
- [ ] ET SCAN Malformed Packet SYN FIN
- [x] ET SCAN w3af Scan Remote File Include Retrieval
- [x] ET SCAN Hydra User-Agent
- [x] ET SCAN Possible WafWoof Web Application Firewall Detection Scan
- [x] ET SCAN Modified Sipvicious User-Agent Detected (sundayddr)
- [x] ET SCAN Inspathx Path Disclosure Scan
- [x] ET SCAN DirBuster Scan in Progress
- [x] ET SCAN Havij SQL Injection Tool User-Agent Outbound
- [x] ET SCAN RatProxy in-use
- [x] ET SCAN Modified Sipvicious Sundayddr Scanner (sipsscuser)
- [x] ET SCAN OpenVAS User-Agent Inbound
- [ ] ET SCAN Possible SQLMAP Scan
- [x] ET SCAN Internal Dummy Connection User-Agent Inbound
- [x] ET SCAN DominoHunter Security Scan in Progress
- [x] ET SCAN Nessus FTP Scan detected (ftp_anonymous.nasl)
- [x] ET SCAN libwww-perl GET to // with specific HTTP header ordering without libwww-perl User-Agent
- [x] ET SCAN Apache mod_deflate DoS via many multiple byte Range values
- [x] ET SCAN McAfee/Foundstone Scanner Web Scan
- [x] ET SCAN Positive Technologies XSpider Security Scanner User-Agent (PTX)
- [x] ET SCAN Apache mod_proxy Reverse Proxy Exposure 2
- [x] ET SCAN FHScan core User-Agent Detect
- [ ] ET SCAN critical.io Scan
- [x] ET SCAN HTExploit Method
- [x] ET SCAN Nessus Netbios Scanning
- [x] ET SCAN MYSQL MySQL Remote FAST Account Password Cracking
- [x] ET SCAN Simple Slowloris Flooder
- [ ] ET SCAN Non-Malicious SSH/SSL Scanner on the run
- [x] ET SCAN SipCLI VOIP Scan - TCP
- [x] ET SCAN NETWORK Outgoing Masscan detected
- [x] ET SCAN FOCA uri
- [x] ET SCAN NMAP SIP Version Detection Script Activity
- [x] ET SCAN NMAP OS Detection Probe
- [x] ET SCAN Possible WordPress xmlrpc.php BruteForce in Progress - Response
- [x] ET SCAN Chroot-apache0day Unknown Web Scanner User Agent
- [x] ET SCAN Acunetix Accept HTTP Header detected scan in progress
- [x] ET SCAN Nmap NSE Heartbleed Request
- [x] ET SCAN Xenu Link Sleuth Scanner Outbound
- [x] ET SCAN Possible Scanning for Vulnerable JBoss
- [x] ET SCAN MySQL Malicious Scanning 1
- [x] ET SCAN MySQL Malicious Scanning 3
- [x] ET SCAN Acunetix scan in progress acunetix_wvs_security_test in http_uri
- [x] ET SCAN MS Terminal Server Traffic on Non-standard Port
- [x] ET SCAN struts-pwn User-Agent
- [x] ET SCAN HP Enterprise VAN SDN Controller
- [x] ET SCAN HID VertX and Edge door controllers discover
- [x] ET SCAN Hikvision IP Camera 5.4.0 Information Disclosure
- [x] ET SCAN Hello Peppa! Scan Activity
- [x] ET SCAN Mirai Variant User-Agent (Inbound)
- [x] ET SCAN Mirai Variant User-Agent (Inbound)
- [x] ET SCAN Mirai Variant User-Agent (Inbound)
- [x] ET SCAN Mirai Variant User-Agent (Inbound)
- [x] ET SCAN Mirai Variant User-Agent (Inbound)
- [x] ET SCAN Mirai Variant User-Agent (Inbound)

- [x] ET SCAN Mirai Variant User-Agent (Inbound)
- [x] ET SCAN Dark Nexus IoT Variant User-Agent (Inbound)
- [x] ET SCAN Tomato Router Default Credentials (root:admin)
- [x] ET SCAN Polaris Botnet User-Agent (Inbound)
- [x] ET SCAN ELF/Mirai Variant User-Agent (Inbound)
- [x] ET SCAN Mirai Variant User-Agent (Inbound)
- [x] ET SCAN ELF/Mirai Variant User-Agent (Inbound)
- [x] ET SCAN ELF/Mirai Variant User-Agent (Inbound)
- [x] ET SCAN JAWS Webserver Unauthenticated Shell Command Execution
- [x] ET SCAN Observed Suspicious UA (Callstranger Vulnerability Checker)
- [x] ET SCAN ELF/Mirai Variant User-Agent (Inbound)
- [x] ET SCAN ELF/Mirai Variant User-Agent (Inbound)
- [x] ET SCAN ELF/Mirai Variant User-Agent (Inbound)
- [x] ET SCAN ELF/Mirai Variant User-Agent (Inbound)
- [x] ET SCAN ELF/Mirai Variant User-Agent (Inbound)
- [x] ET SCAN ELF/Mirai Variant User-Agent (Inbound)
- [x] ET SCAN Generic IDBTE4M Exploit Scanner (Outbound)
- [x] ET SCAN DNS Query for allports.exposed
- [x] ET SCAN Yandex Webcrawler User-Agent (YandexBot)
- [x] ET SCAN Bing Webcrawler User-Agent (BingBot)
- [x] ET SCAN OpenVASVT RCE Test String in HTTP Request Inbound
- [x] ET SCAN Exabot Webcrawler User Agent
- [ ] ET SCAN Baidu Spider Webcrawler User Agent - inbound
- [x] ET SCAN Laravel Debug Mode Information Disclosure Probe Inbound
- [x] ET SCAN RDP Connection Attempt from Nmap
- [x] ET SCAN LeakIX Inbound User-Agent
- [ ] GPL SCAN Finger Search Query
- [ ] GPL SCAN Finger Null Request
- [ ] GPL SCAN cybercop redirection
- [ ] GPL SCAN cybercop query
- [ ] GPL SCAN Finger . query
- [x] GPL SCAN PING Delphi-Piette Windows
- [ ] GPL SCAN Nemesis v1.1 Echo
- [ ] GPL SCAN icmpenum v1.1.1
- [x] GPL SCAN webtrends scanner
- [x] GPL SCAN PING CyberKit 2.2 Windows
- [ ] GPL SCAN same SRC/DST
- [ ] GPL SCAN rusers query UDP
- [x] GPL SCAN ssh-research-scanner
- [ ] GPL SCAN NULL
- [ ] GPL SCAN XMAS
- [ ] GPL SCAN cybercop os SFU12 probe
- [ ] GPL SCAN nmap fingerprint attempt
- [ ] GPL SCAN sensepost.exe command shell attempt
- [x] GPL SCAN nessus 1.X 404 probe
- [ ] GPL SCAN whisker HEAD/./
- [ ] GPL SCAN Finger Version Query
- [x] GPL SCAN SolarWinds IP scan attempt
- [x] GPL SCAN nessus 2.x 404 probe
- [x] ET SCAN Zmap User-Agent (Inbound)
- [x] ET SCAN Tomato Router Default Credentials (admin:admin)
- [x] ET SCAN ELF/Mirai User-Agent Observed (Inbound)
- [x] ET SCAN Polaris Botnet User-Agent (Inbound)
- [x] ET SCAN ELF/Mirai Variant User-Agent (Inbound)
- [x] ET SCAN ELF/Mirai Variant User-Agent (Inbound)
- [x] ET SCAN ELF/Mirai Variant User-Agent (Inbound)
- [x] ET SCAN ELF/Mirai Variant User-Agent (Inbound)
- [x] ET SCAN ELF/Mirai Variant User-Agent (Inbound)
- [x] ET SCAN UPnP SUBSCRIBE Inbound - Possible CallStranger Scan (CVE-2020-12695)
- [ ] ET SCAN Zmap User-Agent (Outbound)
- [x] ET SCAN ELF/Mirai Variant User-Agent (Inbound)
- [x] ET SCAN ELF/Mirai Variant User-Agent (Inbound)
- [x] ET SCAN ELF/Mirai Variant User-Agent (Inbound)
- [x] ET SCAN ELF/Mirai Variant User-Agent (Inbound)
- [x] ET SCAN WordPress Scanner Performing Multiple Requests to Windows Live Writer XML
- [x] ET SCAN Generic IDBTE4M Exploit Scanner (Inbound)
- [x] ET SCAN Google Webcrawler User-Agent (Mediapartners-Google)
- [x] ET SCAN DuckDuckGo Webcrawler User-Agent (DuckDuckBot)
- [x] ET SCAN Naver Webcrawler User-Agent (Naver.me)
- [x] ET SCAN OpenVASVT RCE Test String in HTTP Request Outbound
- [x] ET SCAN AOL Webcrawler User-Agent
- [x] ET SCAN FTPSync Settings Disclosure Attempt
- [ ] ET SCAN WordPress HelloThinkCMF Scan
- [x] ET SCAN Web Scanner - Fuzz Faster U Fool (Inbound)
- [ ] GPL SCAN Finger Account Enumeration Attempt
- [ ] GPL SCAN Finger Root Query
- [ ] GPL SCAN Finger Probe 0 Attempt
- [ ] GPL SCAN Finger Redirection Attempt
- [ ] GPL SCAN Finger 0 Query
- [x] GPL SCAN adm scan
- [x] GPL SCAN ISS Pinger
- [ ] GPL SCAN PING NMAP
- [x] GPL SCAN superscan echo
- [ ] GPL SCAN Broadscan Smurf Scanner
- [x] GPL SCAN PING Sniffer Pro/NetXRay network scan
- [ ] GPL SCAN loopback traffic
- [ ] GPL SCAN myscan
- [ ] GPL SCAN cybercop os probe
- [ ] GPL SCAN SYN FIN
- [ ] GPL SCAN cybercop os PA12 attempt
- [ ] GPL SCAN nmap TCP
- [ ] GPL SCAN Webtrends Scanner UDP Probe
- [ ] GPL SCAN cybercop scan
- [ ] GPL SCAN cybercop os probe
- [ ] GPL SCAN nmap XMAS
- [x] GPL SCAN SSH Version map attempt
- [ ] GPL SCAN NetGear router default password login attempt admin/password
- [ ] GPL SCAN Finger / execution attempt

- [x] **emerging-shellcode.rules** Hide

- [ ] ET SHELLCODE x86 PexFnstenvMov/Sub Encoder
- [ ] ET SHELLCODE x86 Countdown Encoder
- [ ] ET SHELLCODE x86 PexCall Encoder
- [ ] ET SHELLCODE Possible UTF-8 encoded Shellcode Detected
- [ ] ET SHELLCODE Bindshell2 Decoder Shellcode
- [ ] ET SHELLCODE Lindau (linkbot) xor Decoder Shellcode
- [ ] ET SHELLCODE Mainz/Bielefeld Shellcode
- [ ] ET SHELLCODE Schauenburg Shellcode
- [ ] ET SHELLCODE Lichtenfels Shellcode
- [ ] ET SHELLCODE Berlin Shellcode
- [ ] ET SHELLCODE Aachen Shellcode
- [ ] ET SHELLCODE Langenfeld Shellcode
- [ ] ET SHELLCODE x86 Alpha2 GetEIPs Encoder
- [ ] ET SHELLCODE x86 PexAlphaNum Encoder
- [ ] ET SHELLCODE x86 JmpCallAdditive Encoder
- [ ] ET SHELLCODE Possible UTF-16 encoded Shellcode Detected
- [x] ET SHELLCODE Rothenburg Shellcode
- [ ] ET SHELLCODE Adenau Shellcode
- [ ] ET SHELLCODE Wuerzburg Shellcode
- [ ] ET SHELLCODE Koeln Shellcode
- [ ] ET SHELLCODE Mannheim Shellcode
- [ ] ET SHELLCODE Leimbach Shellcode
- [ ] ET SHELLCODE Furth Shellcode
- [ ] ET SHELLCODE Bonn Shellcode

- [ ] ET SHELLCODE Siegburg Shellcode
- [ ] ET SHELLCODE Plain2 Shellcode
- [ ] ET SHELLCODE Bindshell1 Decoder Shellcode (UDP)
- [ ] ET SHELLCODE Plain1 Shellcode (UDP)
- [ ] ET SHELLCODE Bonn Shellcode (UDP)
- [ ] ET SHELLCODE Furth Shellcode (UDP)
- [ ] ET SHELLCODE Leimbach Shellcode (UDP)
- [ ] ET SHELLCODE Mannheim Shellcode (UDP)
- [ ] ET SHELLCODE Koeln Shellcode (UDP)
- [ ] ET SHELLCODE Wuerzburg Shellcode (UDP)
- [ ] ET SHELLCODE Adenau Shellcode (UDP)
- [ ] ET SHELLCODE Rothenburg Shellcode (UDP)
- [ ] ET SHELLCODE METASPLOIT BSD Bind shell
- [ ] ET SHELLCODE METASPLOIT BSD Bind shell (Countdown Encoded 3)
- [ ] ET SHELLCODE METASPLOIT BSD Bind shell (Countdown Encoded 5)
- [ ] ET SHELLCODE METASPLOIT BSD Bind shell (Pex Encoded 2)
- [ ] ET SHELLCODE METASPLOIT BSD Bind shell (Not Encoded 2)
- [ ] ET SHELLCODE METASPLOIT BSD Bind shell (Not Encoded 4)
- [ ] ET SHELLCODE METASPLOIT BSD Bind shell (Pex Alphanumeric Encoded 1)
- [ ] ET SHELLCODE METASPLOIT BSD Bind shell (Pex Alphanumeric Encoded 3)
- [ ] ET SHELLCODE METASPLOIT BSD Bind shell (Pex Alphanumeric Encoded 5)
- [ ] ET SHELLCODE METASPLOIT BSD Bind shell (PexFstEnvMov Encoded 2)
- [ ] ET SHELLCODE METASPLOIT BSD Bind shell (Alpha2 Encoded 1)
- [ ] ET SHELLCODE METASPLOIT BSD Bind shell (Alpha2 Encoded 3)
- [ ] ET SHELLCODE METASPLOIT BSD Reverse shell (Countdown Encoded 1)
- [ ] ET SHELLCODE METASPLOIT BSD Reverse shell (Countdown Encoded 3)
- [ ] ET SHELLCODE METASPLOIT BSD Reverse shell (Pex Encoded 1)
- [ ] ET SHELLCODE METASPLOIT BSD Reverse shell (Not Encoded 1)
- [ ] ET SHELLCODE METASPLOIT BSD Reverse shell (Not Encoded 3)
- [ ] ET SHELLCODE METASPLOIT BSD Reverse shell (Pex Alphanumeric Encoded 2)
- [ ] ET SHELLCODE METASPLOIT BSD Reverse shell (PexFnstenvMov Encoded 1)
- [ ] ET SHELLCODE METASPLOIT BSD Reverse shell (Alpha2 Encoded 1)
- [ ] ET SHELLCODE METASPLOIT BSD Reverse shell (Alpha2 Encoded 3)
- [ ] ET SHELLCODE METASPLOIT BSD SPARC Bind shell (SPARC Encoded 2)
- [ ] ET SHELLCODE METASPLOIT BSD SPARC Bind shell (Not Encoded 2)
- [ ] ET SHELLCODE METASPLOIT BSD SPARC Bind shell (Not Encoded 4)
- [ ] ET SHELLCODE METASPLOIT BSD SPARC Reverse shell (Not Encoded 2)
- [ ] ET SHELLCODE METASPLOIT BSD SPARC Reverse shell (SPARC Encoded 2)
- [ ] ET SHELLCODE Possible Unescape %u Shellcode/Heap Spray
- [ ] ET SHELLCODE Possible UDP x86 JMP to CALL Shellcode Detected
- [ ] ET SHELLCODE Possible Call with No Offset TCP Shellcode
- [ ] ET SHELLCODE Possible Call with No Offset TCP Shellcode
- [x] ET SHELLCODE Possible Call with No Offset TCP Shellcode
- [x] ET SHELLCODE Possible UTF-8 %u90 NOP SLED
- [x] ET SHELLCODE Possible Encoded %90 NOP SLED
- [x] ET SHELLCODE Possible Unescape Encoded Content With Split String Obfuscation
- [x] ET SHELLCODE Common 0a0a0a0a Heap Spray String
- [x] ET SHELLCODE Common %u0a0a%u0a0a UTF-16 Heap Spray String
- [ ] ET SHELLCODE Common 0c0c0c0c Heap Spray String
- [x] ET SHELLCODE Common %u0c0c%u0c0c UTF-16 Heap Spray String
- [ ] ET SHELLCODE Plain1 Shellcode
- [ ] ET SHELLCODE Bindshell1 Decoder Shellcode
- [ ] ET SHELLCODE Plain2 Shellcode (UDP)
- [ ] ET SHELLCODE Siegburg Shellcode (UDP)
- [ ] ET SHELLCODE Langenfeld Shellcode (UDP)
- [ ] ET SHELLCODE Aachen Shellcode (UDP)
- [ ] ET SHELLCODE Berlin Shellcode (UDP)
- [ ] ET SHELLCODE Lichtenfels Shellcode (UDP)
- [ ] ET SHELLCODE Schauenburg Shellcode (UDP)
- [ ] ET SHELLCODE Mainz/Bielefeld Shellcode (UDP)
- [ ] ET SHELLCODE Lindau (linkbot) xor Decoder Shellcode (UDP)
- [x] ET SHELLCODE Bindshell2 Decoder Shellcode (UDP)
- [ ] ET SHELLCODE METASPLOIT BSD Bind shell (Countdown Encoded 2)
- [ ] ET SHELLCODE METASPLOIT BSD Bind shell (Countdown Encoded 4)
- [ ] ET SHELLCODE METASPLOIT BSD Bind shell (Pex Encoded 1)
- [ ] ET SHELLCODE METASPLOIT BSD Bind shell (Not Encoded 1)
- [ ] ET SHELLCODE METASPLOIT BSD Bind shell (Not Encoded 3)
- [ ] ET SHELLCODE METASPLOIT BSD Bind shell (Not Encoded 5)
- [ ] ET SHELLCODE METASPLOIT BSD Bind shell (Pex Alphanumeric Encoded 2)
- [ ] ET SHELLCODE METASPLOIT BSD Bind shell (Pex Alphanumeric Encoded 4)
- [ ] ET SHELLCODE METASPLOIT BSD Bind shell (PexFstEnvMov Encoded 1)
- [ ] ET SHELLCODE METASPLOIT BSD Bind shell (JmpCallAdditive Encoded)
- [ ] ET SHELLCODE METASPLOIT BSD Bind shell (Alpha2 Encoded 2)
- [ ] ET SHELLCODE METASPLOIT BSD Reverse shell (PexFnstenvSub Encoded 1)
- [ ] ET SHELLCODE METASPLOIT BSD Reverse shell (Countdown Encoded 2)
- [ ] ET SHELLCODE METASPLOIT BSD Reverse shell (Countdown Encoded 4)
- [ ] ET SHELLCODE METASPLOIT BSD Reverse shell (Pex Encoded 2)
- [ ] ET SHELLCODE METASPLOIT BSD Reverse shell (Not Encoded 2)
- [ ] ET SHELLCODE METASPLOIT BSD Reverse shell (Pex Alphanumeric Encoded 1)
- [ ] ET SHELLCODE METASPLOIT BSD Reverse shell (Pex Alphanumeric Encoded 3)
- [ ] ET SHELLCODE METASPLOIT BSD Reverse shell (JmpCallAdditive Encoded 1)
- [ ] ET SHELLCODE METASPLOIT BSD Reverse shell (Alpha2 Encoded 2)
- [ ] ET SHELLCODE METASPLOIT BSD SPARC Bind shell (SPARC Encoded 1)
- [ ] ET SHELLCODE METASPLOIT BSD SPARC Bind shell (Not Encoded 1)
- [ ] ET SHELLCODE METASPLOIT BSD SPARC Bind shell (Not Encoded 3)
- [ ] ET SHELLCODE METASPLOIT BSD SPARC Reverse shell (Not Encoded 1)
- [ ] ET SHELLCODE METASPLOIT BSD SPARC Reverse shell (SPARC Encoded 1)
- [ ] ET SHELLCODE METASPLOIT BSD SPARC Reverse shell (Not Encoded 3)
- [ ] ET SHELLCODE Possible TCP x86 JMP to CALL Shellcode Detected
- [ ] ET SHELLCODE Possible Call with No Offset UDP Shellcode
- [ ] ET SHELLCODE Possible Call with No Offset UDP Shellcode
- [x] ET SHELLCODE Possible Call with No Offset UDP Shellcode
- [x] ET SHELLCODE Possible Call with No Offset UDP Shellcode
- [x] ET SHELLCODE Possible UTF-16 %u9090 NOP SLED
- [ ] ET SHELLCODE Possible Usage of Actionscript ByteArray writeByte Function to Build Shellcode
- [x] ET SHELLCODE Possible Unescape Encoded Content With Split String Obfuscation 2
- [ ] ET SHELLCODE Common %0a%0a%0a%0a Heap Spray String
- [x] ET SHELLCODE Common %u0a%u0a%u0a%u0a UTF-8 Heap Spray String
- [x] ET SHELLCODE Common %0c%0c%0c%0c Heap Spray String
- [x] ET SHELLCODE Common %u0c%u0c%u0c%u0c UTF-8 Heap Spray String

- [ ] ET SHELLCODE UTF-8/16 Encoded Shellcode
- [x] ET SHELLCODE Unescape Variable Unicode Shellcode
- [x] ET SHELLCODE Possible 0x0a0a0a0a Heap Spray Attempt
- [x] ET SHELLCODE Possible 0x0c0c0c0c Heap Spray Attempt
- [x] ET SHELLCODE Possible %0d%0d%0d%0d Heap Spray Attempt
- [x] ET SHELLCODE Possible %u0d0d%u0d0d UTF-16 Heap Spray Attempt
- [x] ET SHELLCODE Possible Backslash Unicode Heap Spray Attempt
- [x] ET SHELLCODE Possible %u41%u41%u41%u41 UTF-8 Heap Spray Attempt
- [ ] ET SHELLCODE JavaScript Redefinition of a HeapLib Object - Likely Malicious Heap Spray Attempt
- [x] ET SHELLCODE Hex Obfuscated JavaScript Heap Spray 0c0c0c0c
- [x] ET SHELLCODE Hex Obfuscated JavaScript NOP SLED
- [ ] ET SHELLCODE Hex Obfuscated JavaScript Heap Spray 41414141
- [x] ET SHELLCODE Double BackSlash Hex Obfuscated JavaScript Heap Spray 0b0b0b0b
- [x] ET SHELLCODE Double BackSlash Hex Obfuscated JavaScript Heap Spray 0d0d0d0d
- [x] ET SHELLCODE Double BackSlash Hex Obfuscated JavaScript Heap Spray 41414141
- [ ] ET SHELLCODE Unicode UTF-16 Heap Spray Attempt
- [ ] ET SHELLCODE Possible Backslash Escaped UTF-16 0c0c Heap Spray
- [x] ET SHELLCODE Linux/x86-64 - Polymorphic Flush IPTables Shellcode
- [x] ET SHELLCODE Linux/x86-64 - Reverse Shell Shellcode
- [ ] GPL SHELLCODE SGI NOOP
- [x] GPL SHELLCODE AIX NOOP
- [x] GPL SHELLCODE HP-UX NOOP
- [x] GPL SHELLCODE sparc NOOP
- [x] GPL SHELLCODE sparc NOOP
- [ ] GPL SHELLCODE x86 NOOP
- [ ] GPL SHELLCODE x86 setuid 0
- [x] GPL SHELLCODE Linux shellcode
- [x] GPL SHELLCODE MSSQL shellcode attempt
- [ ] GPL SHELLCODE ssh CRC32 overflow NOOP
- [x] GPL SHELLCODE x86 0xEB0C NOOP
- [x] GPL SHELLCODE x86 0x71FB7BAB NOOP unicode
- [ ] ET SHELLCODE Unescape Variable %u Shellcode
- [x] ET SHELLCODE Javascript Split String Unicode Heap Spray Attempt
- [x] ET SHELLCODE Possible 0x0b0b0b0b Heap Spray Attempt
- [x] ET SHELLCODE Possible 0x0d0d0d0d Heap Spray Attempt
- [x] ET SHELLCODE Possible %u0d%u0d%u0d%u0d UTF-8 Heap Spray Attempt
- [x] ET SHELLCODE Possible Vertical Slash Unicode Heap Spray Attempt
- [x] ET SHELLCODE Possible %41%41%41%41 Heap Spray Attempt
- [x] ET SHELLCODE Possible %u4141%u4141 UTF-16 Heap Spray Attempt
- [x] ET SHELLCODE Hex Obfuscated JavaScript Heap Spray 0b0b0b0b
- [x] ET SHELLCODE Hex Obfuscated JavaScript Heap Spray 0d0d0d0d
- [x] ET SHELLCODE Unescape Hex Obfuscated Content
- [x] ET SHELLCODE Double BackSlash Hex Obfuscated JavaScript Heap Spray 0a0a0a0a
- [x] ET SHELLCODE Double BackSlash Hex Obfuscated JavaScript Heap Spray 0c0c0c0c
- [x] ET SHELLCODE Double BackSlash Hex Obfuscated JavaScript NOP SLED
- [ ] ET SHELLCODE Unicode UTF-8 Heap Spray Attempt
- [x] ET SHELLCODE Possible Backslash Escaped UTF-8 0c0c Heap Spray
- [x] ET SHELLCODE Possible UTF-16 u9090 NOP SLED
- [x] ET SHELLCODE Linux/x86-64 - Polymorphic Setuid(0) & Execve(/bin/sh) Shellcode
- [x] ET SHELLCODE Execve(/bin/sh) Shellcode
- [x] GPL SHELLCODE SGI NOOP
- [x] GPL SHELLCODE Digital UNIX NOOP
- [x] GPL SHELLCODE HP-UX NOOP
- [x] GPL SHELLCODE sparc NOOP
- [x] GPL SHELLCODE sparc setuid 0
- [ ] GPL SHELLCODE x86 setgid 0
- [ ] GPL SHELLCODE x86 stealth NOOP
- [ ] GPL SHELLCODE x86 0x90 unicode NOOP
- [ ] GPL SHELLCODE ssh CRC32 overflow /bin/sh
- [ ] GPL SHELLCODE x86 inc ebx NOOP
- [x] GPL SHELLCODE x86 0x71FB7BAB NOOP
- [ ] GPL SHELLCODE x86 0x90 NOOP unicode

- [x] **emerging-smtp.rules** Hide

- [ ] ET SMTP Potential Exim HeaderX with run exploit attempt
- [x] ET SMTP Abuseat.org Block Message
- [ ] ET SMTP Sophos.com Block Message
- [x] ET SMTP Robtex.com Block Message
- [x] ET SMTP Possible ComputerCop Log Transmitted via SMTP
- [x] ET SMTP Message Containing search-ms URI With subquery Parameter In Message Body - Possible NTLM Hash Leak Attempt
- [x] ET SMTP Message Containing Windows Performance Analyzer URI In Message Body - Possible NTLM Hash Leak Attempt
- [ ] GPL SMTP ehlo cybercop attempt
- [x] GPL SMTP RCPT TO overflow
- [x] GPL SMTP expn root
- [ ] GPL SMTP OUTBOUND bad file attachment
- [ ] GPL SMTP expn *@
- [x] GPL SMTP AUTH LOGON brute force attempt
- [ ] ET SMTP IBM Lotus Domino iCalendar Email Address Stack Buffer Overflow Attempt
- [x] ET SMTP Spamcop.net Block Message
- [x] ET SMTP Sorbs.net Block Message
- [x] ET SMTP EXE - ZIP file with .pif filename inside
- [x] ET SMTP Incoming SMTP Message with Possibly Malicious MIME Epilogue 2016-05-13 (BadEpilogue)
- [x] ET SMTP Message Containing search-ms URI With crumb location Parameter In Message Body - Possible NTLM Hash Leak Attempt
- [ ] GPL SMTP SMTP relaying denied
- [ ] GPL SMTP expn cybercop attempt
- [x] GPL SMTP expn decode
- [x] GPL SMTP vrfy decode
- [x] GPL SMTP vrfy root
- [x] GPL SMTP EXPN overflow attempt
- [ ] GPL SMTP MAIL FROM overflow attempt

- [x] **emerging-snmp.rules** Hide

- [ ] ET SNMP Cisco Non-Trap PDU request on SNMPv1 trap port
- [ ] ET SNMP Cisco Non-Trap PDU request on SNMPv3 trap port
- [ ] ET SNMP Cisco Non-Trap PDU request on SNMPv2 random port
- [x] ET SNMP Attempted UDP Access Attempt to Cisco IOS 12.1 Hidden Read/Write Community String ILMI
- [x] ET SNMP Attempted UDP Access Attempt to Cisco IOS 12.1 Hidden Read/Write Community String cable-docsis
- [x] ET SNMP Attempt to retrieve Cisco Config via TFTP (CISCO-CONFIG-COPY)
- [ ] ET SNMP Cisco Non-Trap PDU request on SNMPv2 trap port
- [ ] ET SNMP Cisco Non-Trap PDU request on SNMPv1 random port
- [ ] ET SNMP Cisco Non-Trap PDU request on SNMPv3 random port
- [ ] ET SNMP Attempted TCP Access Attempt to Cisco IOS 12.1 Hidden Read/Write Community String ILMI
- [x] ET SNMP Attempted TCP Access Attempt to Cisco IOS 12.1 Hidden Read/Write Community String cable-docsis
- [x] ET SNMP Samsung Printer SNMP Hardcode RW Community String

- [x] ET SNMP missing community string attempt 1
- [x] ET SNMP missing community string attempt 2
- [ ] ET SNMP missing community string attempt 3
- [x] ET SNMP missing community string attempt 4
- [x] GPL SNMP SNMP trap Format String detected
- [x] GPL SNMP SNMP NT UserList
- [ ] GPL SNMP SNMP community string buffer overflow attempt
- [x] GPL SNMP public access udp
- [x] GPL SNMP public access tcp
- [x] GPL SNMP private access udp
- [x] GPL SNMP private access tcp
- [ ] GPL SNMP Broadcast request
- [ ] GPL SNMP broadcast trap
- [ ] GPL SNMP request udp
- [ ] GPL SNMP request tcp
- [ ] GPL SNMP trap udp
- [ ] GPL SNMP trap tcp
- [ ] GPL SNMP community string buffer overflow attempt with evasion
- [x] GPL SNMP PROTOS test-suite-trap-app attempt
- [x] GPL SNMP null community string attempt
- [ ] GPL SNMP missing community string attempt

- [ ] **emerging-sql.rules** Show
- [x] **emerging-telnet.rules** Hide

- [x] ET TELNET External Telnet Attempt To Cisco Device With No Telnet Password Set (Automatically Dissalowed Until Password Set)
- [ ] ET TELNET External Telnet Login Prompt from Cisco Device
- [x] ET TELNET busybox MIRAI hackers - Possible Brute Force Attack
- [x] ET TELNET busybox ECCHI hackers - Possible Brute Force Attack
- [x] ET TELNET busybox MEMES Hackers - Possible Brute Force Attack
- [x] GPL TELNET TELNET login failed
- [ ] GPL TELNET TELNET access
- [x] GPL TELNET Telnet Root not on console
- [x] GPL TELNET root login
- [x] GPL TELNET Bad Login

- [x] **emerging-tftp.rules** Hide

- [x] ET TFTP Outbound TFTP Write Request
- [x] ET TFTP Outbound TFTP Data Transfer
- [x] ET TFTP Outbound TFTP ACK
- [x] ET TFTP Outbound TFTP Error Message
- [x] ET TFTP Outbound TFTP Read Request
- [ ] ET TFTP TFTPGUI Long Transport Mode Buffer Overflow
- [x] ET TFTP Outbound TFTP Data Transfer with Cisco config
- [x] ET TFTP Outbound TFTP Data Transfer With Cisco Config 2
- [x] GPL TFTP Put
- [ ] GPL TFTP parent directory
- [ ] GPL TFTP root directory
- [x] GPL TFTP MISC TFTP32 Get Format string attempt
- [x] GPL TFTP GET Admin.dll
- [x] GPL TFTP GET nc.exe
- [x] GPL TFTP GET shadow
- [x] GPL TFTP GET passwd
- [ ] GPL TFTP Get
- [ ] GPL TFTP GET filename overflow attempt
- [ ] GPL TFTP NULL command attempt
- [ ] GPL TFTP PUT filename overflow attempt

- [ ] **emerging-tor.rules** Show
- [x] **emerging-user_agents.rules** Hide

- [x] ET USER_AGENTS Suspicious User Agent (agent)
- [x] ET USER_AGENTS SideStep User-Agent
- [x] ET USER_AGENTS Suspicious User Agent (Microsoft Internet Explorer)
- [x] ET USER_AGENTS Metafisher/Goldun User-Agent (z)
- [ ] ET USER_AGENTS 2search.org User Agent (2search)
- [x] ET USER_AGENTS Suspicious User Agent (Autoupdate)
- [x] ET USER_AGENTS Suspicious User-Agent - Possible Trojan Downloader (ver18/ver19 etc)
- [ ] ET USER_AGENTS sgrunt Dialer User Agent (sgrunt)
- [ ] ET USER_AGENTS User Agent Containing http Suspicious - Likely Spyware/Trojan
- [x] ET USER_AGENTS Suspicious User-Agent (Updater)
- [x] ET USER_AGENTS Suspicious User-Agent (update)
- [ ] ET USER_AGENTS Suspicious User-Agent (Updater)
- [ ] ET USER_AGENTS Suspicious User-Agent (WinXP Pro Service Pack 2)
- [x] ET USER_AGENTS Suspicious User-Agent outbound (bot)
- [x] ET USER_AGENTS Suspicious User-Agent (MSIE)
- [ ] ET USER_AGENTS WebHack Control Center User-Agent Outbound (WHCC/)
- [x] ET USER_AGENTS Suspicious User-Agent (HTTPTEST) - Seen used by downloaders
- [ ] ET USER_AGENTS Suspicious User-Agent (Snatch-System)
- [ ] ET USER_AGENTS KKtone Suspicious User-Agent (KKTone)
- [x] ET USER_AGENTS Suspicious User-Agent (MyAgent)
- [x] ET USER_AGENTS Suspicious User-Agent (Huai_Huai)
- [x] ET USER_AGENTS Dialer-967 User-Agent
- [x] ET USER_AGENTS Suspicious User-Agent (MYURL)
- [ ] ET USER_AGENTS Matcash or related downloader User-Agent Detected
- [x] ET USER_AGENTS Downloader User-Agent Detected (Windows Updates Manager|3.12|...)
- [x] ET USER_AGENTS Suspicious User-Agent (006)
- [x] ET USER_AGENTS Downloader User-Agent Detected (ld)
- [ ] ET USER_AGENTS Eldorado.BHO User-Agent Detected (netcfg)
- [x] ET USER_AGENTS Win32/Feebs.kw Worm User-Agent Detected
- [x] ET USER_AGENTS Tear Application User-Agent Detected
- [x] ET USER_AGENTS User-agent DownloadNetFile Win32.small.hsh downloader
- [ ] ET USER_AGENTS Cashpoint.com Related checkin User-Agent (inetinst)
- [ ] ET USER_AGENTS Cashpoint.com Related checkin User-Agent (okcpmgr)
- [x] ET USER_AGENTS Suspicious User-Agent (HTTP_CONNECT_)
- [x] ET USER_AGENTS Suspicious User-Agent (API-Guide test program) Used by Several trojans
- [x] ET USER_AGENTS Eldorado.BHO User-Agent Detected (MSIE 5.5)
- [x] ET USER_AGENTS Suspicious User-Agent - Possible Trojan Downloader (WinInet)
- [x] ET USER_AGENTS Suspicious User-Agent Possible Trojan Downloader Shell
- [x] ET USER_AGENTS User-Agent (single dash)
- [x] ET USER_AGENTS Suspicious User-Agent (downloader)
- [x] ET USER_AGENTS User-Agent (Unknown)
- [x] ET USER_AGENTS Suspicious User-Agent - Possible Trojan Downloader (https)
- [x] ET USER_AGENTS Suspicious User-Agent (Mozilla/4.0 (compatible ICS))
- [ ] ET USER_AGENTS Rf-cheats.ru Trojan Related User-Agent (RFRudokop v.1.1 account verification)

- [x] ET USER_AGENTS Suspicious User-Agent (Version 1.23)
- [x] ET USER_AGENTS Suspicious User-Agent (App4)
- [x] ET USER_AGENTS Suspicious User-Agent (INSTALLER)
- [x] ET USER_AGENTS Suspicious User-Agent (GOOGLE)
- [x] ET USER_AGENTS Suspicious User-Agent (RBR)
- [x] ET USER_AGENTS Suspicious User-Agent (MS Internet Explorer)
- [x] ET USER_AGENTS Suspicious User-Agent (QQ)
- [x] ET USER_AGENTS Suspicious User-Agent (SERVER2_03)
- [x] ET USER_AGENTS Suspicious User-Agent (sickness29a/0.1)
- [x] ET USER_AGENTS Suspicious User-Agent (NSIS_DOWNLOAD)
- [x] ET USER_AGENTS Suspicious User-Agent (chek)
- [x] ET USER_AGENTS Suspicious User-Agent (AutoHotkey)
- [x] ET USER_AGENTS Suspicious User-Agent (opera)
- [x] ET USER_AGENTS Suspicious User-Agent (contains loader)
- [x] ET USER_AGENTS Suspicious User-Agent (angel)
- [x] ET USER_AGENTS Suspicious User-Agent (ISMYIE)
- [x] ET USER_AGENTS Suspicious User-Agent (ErrCode)
- [x] ET USER_AGENTS Suspicious User-Agent (ReadFileURL)
- [x] ET USER_AGENTS Suspicious User-Agent (Inet_read)
- [x] ET USER_AGENTS Suspicious User-Agent (CFS_DOWNLOAD)
- [x] ET USER_AGENTS Suspicious User-Agent (HTTP Downloader)
- [x] ET USER_AGENTS Suspicious User-Agent (Download App)
- [x] ET USER_AGENTS Suspicious User-Agent (hacker)
- [ ] ET USER_AGENTS Suspicious User-Agent (adsntD)
- [ ] ET USER_AGENTS Suspicious User-Agent (ieagent)
- [x] ET USER_AGENTS Suspicious User-Agent (SUiCiDE/1.5)
- [x] ET USER_AGENTS Suspicious User-Agent (AVP2006IE)
- [x] ET USER_AGENTS Suspicious User-Agent (Internet HTTP Request)
- [ ] ET USER_AGENTS WinFixer Trojan Related User-Agent (ElectroSun)
- [x] ET USER_AGENTS Suspicious User-Agent Detected (Compatible)
- [ ] ET USER_AGENTS Suspicious User-Agent Detected (aguarovex-loader v3.221)
- [x] ET USER_AGENTS Suspicious User Agent (FTP)
- [x] ET USER_AGENTS Suspicious User-Agent (Kvadrlson 1.0)
- [x] ET USER_AGENTS Suspicious User-Agent (miip)
- [x] ET USER_AGENTS Suspicious User-Agent (Errordigger.com related)
- [x] ET USER_AGENTS Suspicious User-Agent (xr - Worm.Win32.VB.cj related)
- [ ] ET USER_AGENTS Suspicious User-Agent pricers.info related (section)
- [x] ET USER_AGENTS Suspicious User-Agent (IE/1.0)
- [x] ET USER_AGENTS Suspicious User-Agent (runUpdater.html)
- [x] ET USER_AGENTS Suspicious User-Agent (Session) - Possible Trojan-Clicker
- [x] ET USER_AGENTS Suspicious User-Agent (Loands) - Possible Trojan Downloader GET Request
- [ ] ET USER_AGENTS Suspicious User-Agent filled with System Details - GET Request
- [x] ET USER_AGENTS User-Agent (_TEST_)
- [x] ET USER_AGENTS Suspicious User-Agent (INet)
- [x] ET USER_AGENTS User-Agent (STEROID Download)
- [x] ET USER_AGENTS Suspicious User-Agent (XXX) Often Sony Update Related
- [ ] ET USER_AGENTS WindowsEnterpriseSuite FakeAV User-Agent TALWinHttpClient
- [x] ET USER_AGENTS Win32.OnLineGames User-Agent (BigFoot)
- [ ] ET USER_AGENTS badly formatted User-Agent string (no closing parenthesis)
- [ ] ET USER_AGENTS Suspicious User-Agent (InTeRNeT)
- [x] ET USER_AGENTS Suspicious User Agent (AskInstallChecker)
- [x] ET USER_AGENTS Suspicious User-Agent (InfoBot)
- [ ] ET USER_AGENTS Suspicious User Agent (GabPath)
- [x] ET USER_AGENTS Suspicious Win32 User Agent
- [x] ET USER_AGENTS suspicious user-agent (REKOM)
- [x] ET USER_AGENTS Suspicious User-Agent Moxilla
- [x] ET USER_AGENTS User-Agent (Internet Explorer)
- [ ] ET USER_AGENTS Suspicious User-Agent (Mozilla-web)
- [x] ET USER_AGENTS Suspicious User-Agent (IEMGR)
- [ ] ET USER_AGENTS Vapsup User-Agent (doshowmeanad loader v2.1)
- [x] ET USER_AGENTS Otwycal User-Agent (Downing)
- [x] ET USER_AGENTS Suspicious User-Agent (Installer)
- [ ] ET USER_AGENTS Suspicious User-Agent (TestAgent)
- [x] ET USER_AGENTS Suspicious User-Agent (WinProxy)
- [x] ET USER_AGENTS Suspicious User-Agent (up2dash updater)
- [ ] ET USER_AGENTS Suspicious User-Agent (Mozilla 1.02.45 biz)
- [x] ET USER_AGENTS Suspicious User-Agent (IE)
- [x] ET USER_AGENTS Suspicious User-Agent (WebForm 1)
- [ ] ET USER_AGENTS Suspicious User-Agent (Zilla)
- [x] ET USER_AGENTS Suspicious User-Agent (123)
- [x] ET USER_AGENTS Suspicious User-Agent (Accessing)
- [ ] ET USER_AGENTS Suspicious User-Agent (InetURL)
- [x] ET USER_AGENTS Suspicious User-Agent (svchost)
- [ ] ET USER_AGENTS Suspicious User-Agent (PcPcUpdater)
- [x] ET USER_AGENTS Suspicious User-Agent (CFS Agent)
- [ ] ET USER_AGENTS Suspicious User-Agent (AdiseExplorer)
- [x] ET USER_AGENTS Suspicious User-Agent (HttpDownload)
- [x] ET USER_AGENTS Downloader User-Agent (AutoDL\/1.0)
- [ ] ET USER_AGENTS Suspicious User-Agent (ieguideupdate)
- [ ] ET USER_AGENTS Suspicious User-Agent (dwplayer)
- [ ] ET USER_AGENTS Suspicious User-Agent (antispyprogram)
- [x] ET USER_AGENTS Suspicious User-Agent (msIE 7.0)
- [x] ET USER_AGENTS Suspicious User-Agent (winlogon)
- [x] ET USER_AGENTS Suspicious User-Agent Detected (RLMultySocket)
- [x] ET USER_AGENTS Suspicious User-Agent Detected (Downloader1.2)
- [x] ET USER_AGENTS Suspicious User-Agent Detected (GetUrlSize)
- [x] ET USER_AGENTS Suspicious User-Agent Detected (WINS_HTTP_SEND Program/1.0)
- [x] ET USER_AGENTS Suspicious User-Agent (checkonline)
- [ ] ET USER_AGENTS Kangkio User-Agent (lsosss)
- [x] ET USER_AGENTS Suspicious User-Agent (Mozil1a)
- [x] ET USER_AGENTS Suspicious User-Agent (Trojan.Hijack.IrcBot.457 related)
- [ ] ET USER_AGENTS Suspicious User-Agent (Yandesk)
- [x] ET USER_AGENTS Suspicious User-Agent (HELLO)
- [x] ET USER_AGENTS Suspicious User Agent (BlackSun)
- [x] ET USER_AGENTS Suspicious User-Agent (runPatch.html)
- [ ] ET USER_AGENTS Suspicious User-Agent (Poker)
- [x] ET USER_AGENTS Suspicious User-Agent (ms_ie) - Crypt.ZPACK Gen Trojan Downloader GET Request
- [ ] ET USER_AGENTS Suspicious User-Agent (InHold) - Possible Trojan Downloader GET Request
- [x] ET USER_AGENTS Suspicious User-Agent (Forthgoner) - Possible Trojan Downloader GET Request
- [x] ET USER_AGENTS Suspicious User-Agent (Mozilla/3.0 (compatible))
- [ ] ET USER_AGENTS Suspicious User-Agent (Sme32)
- [x] ET USER_AGENTS Suspicious User-Agent (ClickAdsByIE)
- [x] ET USER_AGENTS Suspicious User-Agent (My Session)
- [x] ET USER_AGENTS Suspicious User-Agent (FaceCooker)
- [x] ET USER_AGENTS Suspicious User-Agent (lineguide)
- [ ] ET USER_AGENTS Nine Ball User-Agent Detected (NQX315)
- [x] ET USER_AGENTS Observed Suspicious UA (NSIS_Inetc (Mozilla))
- [x] ET USER_AGENTS Suspicious User Agent (ScrapeBox)
- [ ] ET USER_AGENTS Suspicious User Agent no space
- [x] ET USER_AGENTS Suspicious User-Agent (Our_Agent)
- [x] ET USER_AGENTS Si25f_302 User-Agent
- [x] ET USER_AGENTS Suspicious User-Agent VCTestClient

- [ ] ET USER_AGENTS Suspicious User-Agent PrivacyInfoUpdate
- [x] ET USER_AGENTS Suspicious User-Agent (VMozilla)
- [ ] ET USER_AGENTS Lowercase User-Agent header purporting to be MSIE
- [x] ET USER_AGENTS Suspicious User-Agent Mozilla/3.0
- [x] ET USER_AGENTS Suspicious User-Agent String (AskPartnerCobranding)
- [x] ET USER_AGENTS suspicious user agent string (CholTBAgent)
- [x] ET USER_AGENTS Suspicious user agent (asd)
- [x] ET USER_AGENTS Suspicious User-Agent Fragment (WORKED)
- [x] ET USER_AGENTS EmailSiphon Suspicious User-Agent Inbound
- [x] ET USER_AGENTS Binget PHP Library User Agent Outbound
- [x] ET USER_AGENTS PyCurl Suspicious User Agent Outbound
- [x] ET USER_AGENTS Atomic_Email_Hunter User-Agent Outbound
- [x] ET USER_AGENTS Ufasoft bitcoin Related User-Agent
- [ ] ET USER_AGENTS Suspicious User-Agent (GUIDTracker)
- [x] ET USER_AGENTS Suspicious User-Agent (MadeByLc)
- [ ] ET USER_AGENTS Suspicious User-Agent (windsoft)
- [ ] ET USER_AGENTS Win32/OnLineGames User-Agent (Revolution Win32)
- [x] ET USER_AGENTS Suspicious User-Agent (NateFinder)
- [ ] ET USER_AGENTS Suspicious User-Agent (DARecover)
- [x] ET USER_AGENTS Unknown - Java Request - gt 60char hex-ascii
- [x] ET USER_AGENTS User-Agent (ChilkatUpload)
- [x] ET USER_AGENTS FOCA User-Agent
- [x] ET USER_AGENTS Suspicious User-Agent (hi)
- [x] ET USER_AGENTS MSF Meterpreter Default User Agent
- [x] ET USER_AGENTS BLEXBot User-Agent
- [x] ET USER_AGENTS Go HTTP Client User-Agent
- [x] ET USER_AGENTS VPNFilter Related UA (Gemini/2.0)
- [x] ET USER_AGENTS MSIL/Peppy User-Agent
- [x] ET USER_AGENTS Suspicious User-Agent (Windows XP)
- [x] ET USER_AGENTS Suspicious User-Agent (Windows 10)
- [x] ET USER_AGENTS Suspicious UA Observed (IEhook)
- [x] ET USER_AGENTS Peppy/KeeOIL Google User-Agent (google/dance)
- [x] ET USER_AGENTS Suspicious User-Agent (SomeTimes)
- [x] ET USER_AGENTS Suspicious User-Agent (Clever Internet Suite)
- [x] ET USER_AGENTS ESET Installer
- [x] ET USER_AGENTS Node XMLHTTP User-Agent
- [x] ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent
- [x] ET USER_AGENTS Observed Suspicious UA (Hello, World)
- [x] ET USER_AGENTS Fake Mozilla User-Agent String Observed (M0zilla)
- [x] ET USER_AGENTS Observed Suspicious UA (zwt)
- [x] ET USER_AGENTS Suspicious Custom Firefox UA Observed (Firefox...)
- [x] ET USER_AGENTS AnyDesk Remote Desktop Software User-Agent
- [x] ET USER_AGENTS Observed Suspicious UA (Chrome)
- [x] ET USER_AGENTS Steam HTTP Client User-Agent
- [x] ET USER_AGENTS Observed Suspicious UA (IExplorer 34)
- [x] ET USER_AGENTS Observed Suspicious UA (Client)
- [x] ET USER_AGENTS Observed Suspicious UA (DxD)
- [x] ET USER_AGENTS Suspicious User-Agent (VB OpenUrl)
- [x] ET USER_AGENTS Observed Suspicious UA (easyhttp client)
- [x] ET USER_AGENTS Suspicious User Agent (explorersvc)
- [x] ET USER_AGENTS Observed Suspicious UA (Http-connect)
- [x] ET USER_AGENTS Willowcoin Cryptocurrency UA Observed
- [x] ET USER_AGENTS Observed Suspicious UA (PhoneMonitor)
- [x] ET USER_AGENTS Observed Suspicious UA (h55u4u4u5uii5)
- [x] ET USER_AGENTS Suspicious User-Agent (MSIE)
- [x] ET USER_AGENTS Observed Suspicious UA (grab)
- [x] ET USER_AGENTS Observed Suspicious UA (justupdate)
- [x] ET USER_AGENTS Observed Suspicious UA (cctv.mtv)
- [x] ET USER_AGENTS Suspicious User-Agent (firefox)
- [x] ET USER_AGENTS Suspicious User-Agent (Presto)
- [x] ET USER_AGENTS Suspicious User-Agent Im Luo
- [x] ET USER_AGENTS Suspicious User-Agent Sample
- [x] ET USER_AGENTS suspicious User Agent (Lotto)
- [x] ET USER_AGENTS suspicious user agent string (changhuatong)
- [x] ET USER_AGENTS Suspicious user agent (mdms)
- [x] ET USER_AGENTS Suspicious User-Agent SimpleClient 1.0
- [x] ET USER_AGENTS MacShield User-Agent Likely Malware
- [x] ET USER_AGENTS EmailSiphon Suspicious User-Agent Outbound
- [x] ET USER_AGENTS pxyscand/ Suspicious User Agent Outbound
- [x] ET USER_AGENTS Atomic_Email_Hunter User-Agent Inbound
- [x] ET USER_AGENTS Long Fake wget 3.0 User-Agent Detected
- [x] ET USER_AGENTS Suspicious User-Agent _updater_agent
- [x] ET USER_AGENTS Downloader User-Agent HTTPGET
- [x] ET USER_AGENTS Win32/OnLineGames User-Agent (Revolution Win32)
- [x] ET USER_AGENTS W32/OnlineGames User-Agent (LockXLS)
- [x] ET USER_AGENTS Suspicious User-Agent (FULLSTUFF)
- [ ] ET USER_AGENTS Suspicious User-Agent (webfile)
- [x] ET USER_AGENTS Suspicious User-Agent (adlib)
- [x] ET USER_AGENTS Suspicious User-Agent (DownloadMR)
- [x] ET USER_AGENTS Suspicious user agent (Google page)
- [ ] ET USER_AGENTS MtGox Leak wallet stealer UA
- [x] ET USER_AGENTS Suspicious User-Agent (HardCore Software For)
- [x] ET USER_AGENTS WildTangent User-Agent (WT Games App)
- [x] ET USER_AGENTS Microsoft Edge on Windows 10 SET
- [x] ET USER_AGENTS Suspicious User-Agent (=Mozilla)
- [x] ET USER_AGENTS VPNFilter Related UA (Hakai/2.0)
- [x] ET USER_AGENTS VPNFilter Related UA (curl53)
- [x] ET USER_AGENTS Suspicious User-Agent (Windows 8)
- [x] ET USER_AGENTS Suspicious User-Agent (Windows 7)
- [x] ET USER_AGENTS WinRM User Agent Detected - Possible Lateral Movement
- [x] ET USER_AGENTS Peppy/KeeOIL User-Agent (ekeoil)
- [x] ET USER_AGENTS SFML User-Agent (libsfml-network)
- [x] ET USER_AGENTS Observed Suspicious UA (Mozilla 6.0)
- [x] ET USER_AGENTS Aria2 User-Agent
- [x] ET USER_AGENTS Microsoft Dr Watson User-Agent (MSDW)
- [x] ET USER_AGENTS Suspicious UA Observed (YourUserAgent)
- [x] ET USER_AGENTS Observed Suspicious UA (Hello-World)
- [x] ET USER_AGENTS Suspicious UA Observed (Ave, Caesar!)
- [x] ET USER_AGENTS Observed Suspicious UA (My Agent)
- [x] ET USER_AGENTS Suspicious UA Observed (Quick Macros)
- [x] ET USER_AGENTS Suspicious Generic Style UA Observed (My_App)
- [x] ET USER_AGENTS Observed Suspicious UA (Absent)
- [x] ET USER_AGENTS Steam HTTP Client User-Agent
- [x] ET USER_AGENTS Suspicious User Agent (reqwest/)
- [x] ET USER_AGENTS Observed Suspicious UA (system_file/2.0)
- [x] ET USER_AGENTS ABBCCoin Activity Observed
- [x] ET USER_AGENTS Observed Suspicious UA (\xa4)
- [x] ET USER_AGENTS Observed Suspicious UA (xPCAP)
- [x] ET USER_AGENTS Suspicious User Agent (KtulhuBrowser)
- [x] ET USER_AGENTS Shadowcoin Cryptocurrency UA Observed
- [x] ET USER_AGENTS Observed Malicious CASPER/Mirai UA
- [x] ET USER_AGENTS BeeMovie Related Activity
- [x] ET USER_AGENTS Possible QBot User-Agent
- [x] ET USER_AGENTS Observed Suspicious UA (CODE)
- [x] ET USER_AGENTS SAP CVE-2020-6287 PoC UA Observed
- [x] ET USER_AGENTS Observed Suspicious UA (.NET Framework Client)
- [x] ET USER_AGENTS Suspicious User-Agent (cso)
- [x] ET USER_AGENTS Suspicious User-Agent (chrome)

- [x] ET USER_AGENTS Suspected Mekotio User-Agent (MyCustomUser)
- [x] ET USER_AGENTS Suspected Mekotio User-Agent (4M5yC6u4stom5U8se3r)
- [x] ET USER_AGENTS Suspicious User-Agent (boostsoftware-urlexists)
- [ ] ET USER_AGENTS Microsoft Malware Protection User-Agent Observed
- [x] ET USER_AGENTS Microsoft Windows Vista UA - Commonly Abused
- [x] ET USER_AGENTS Suspicious User-Agent (Installed OK)
- [x] ET USER_AGENTS Suspicious User-Agent (Fire-Cloud)
- [x] ET USER_AGENTS Suspicious HttpSocket User-Agent Observed
- [x] ET USER_AGENTS Suspicious User-Agent Simple Bot
- [x] ET USER_AGENTS Suspicious User-Agent (aaaa)
- [x] ET USER_AGENTS Suspicious User-Agent (Collection Info)
- [x] ET USER_AGENTS Suspicious User-Agent (HaxerMen)
- [x] ET USER_AGENTS Non-standard User-Agent (PATCHER)
- [x] ET USER_AGENTS Observed Suspicious User-Agent (altera forma)
- [x] ET USER_AGENTS WaterDropX PRISM UA Observed
- [x] ET USER_AGENTS Observed Malicious User-Agent (Brute Force Attacks)
- [x] ET USER_AGENTS Observed Malicious User-Agent (Brute Force Attacks)
- [x] ET USER_AGENTS sysWeb User-Agent
- [x] ET USER_AGENTS Suspicious User-Agent (REBOL)
- [x] ET USER_AGENTS Suspicious User-Agent (USERAGENT)
- [x] ET USER_AGENTS Suspicious User-Agent (Embarcadero URI Client/1.0)
- [x] ET USER_AGENTS Suspicious User-Agent (Microsoft-ATL-Native/9.00)
- [x] ET USER_AGENTS Suspicious User-Agent (urlRequest)
- [x] ET USER_AGENTS Suspicious User-Agent (test-upload)
- [x] ET USER_AGENTS Suspicious User-Agent (dBrowser CallGetResponse)
- [x] ET USER_AGENTS Suspicious User-Agent (example/1.0)
- [x] ET USER_AGENTS Suspcious LeakIX User-Agent (l9explore)
- [x] ET USER_AGENTS Suspicious User-Agent (ItIsMe)
- [x] ET USER_AGENTS Suspicious User-Agent (HTTP-Test-Program)
- [x] ET USER_AGENTS Observed Malicious User-Agent (CobaltStrike)
- [x] ET USER_AGENTS Observed Malicious User-Agent (FastInvoice)
- [ ] ET USER_AGENTS Observed Bumblebee Loader User-Agent (bumblebee)
- [x] ET USER_AGENTS Observed DPRK Related APT User-Agent (dafom)
- [x] ET USER_AGENTS Suspicious User-Agent (Windows Explorer)
- [x] ET USER_AGENTS DanaBot Specific UA Observed
- [x] ET USER_AGENTS Suspicious User-Agent (kath)
- [x] ET USER_AGENTS Suspicious User-Agent (56)
- [x] ET USER_AGENTS ErbiumStealer UA Observed
- [x] ET USER_AGENTS Suspicious User-Agent (Hello World)
- [x] ET USER_AGENTS Suspicious User-Agent (RestoroMainExe)
- [x] ET USER_AGENTS Suspicious User-Agent (Testing)
- [x] ET USER_AGENTS Suspicious User-Agent (xfilesreborn)
- [x] ET USER_AGENTS Discord Bot User-Agent Observed (DiscordBot)
- [x] ET USER_AGENTS Suspicious User-Agent (RT/1.0)
- [x] ET USER_AGENTS Observed Uclient User-Agent
- [x] ET USER_AGENTS Observed Malicious VBS Related UA
- [x] ET USER_AGENTS Microsoft Office Existence Discovery User-Agent
- [x] ET USER_AGENTS Observed DonotGroup Related UA (Chrome Edge)
- [x] ET USER_AGENTS Observed Donot Group UA (Mozilla FireFox)
- [x] ET USER_AGENTS Win32/FakeAV InternetSecurityGuard User-Agent
- [x] ET USER_AGENTS Suspicious User Agent (Zadanie)
- [x] ET USER_AGENTS Kimsuky CnC Checkin User-Agent
- [x] ET USER_AGENTS Observed Reconnaissance Related UA
- [x] ET USER_AGENTS Seetrol Client Remote Administration Tool User-Agent
- [x] ET USER_AGENTS Observed Suspicious User-Agent (inflammable)
- [x] ET USER_AGENTS Observed Suspicious User-Agent (JWrapperDownloader)

- [x] **emerging-voip.rules** Hide
  - [ ] ET VOIP SIP UDP Softphone INVITE overflow
  - [x] ET VOIP INVITE Message Flood TCP
  - [x] ET VOIP REGISTER Message Flood TCP
  - [x] ET VOIP Multiple Unauthorized SIP Responses TCP
  - [ ] ET VOIP MultiTech SIP UDP Overflow
  - [ ] ET VOIP Centrality IP Phone (PA-168 Chipset) Session Hijacking
  - [ ] ET VOIP Asterisk Register with no URI or Version DOS Attempt
  - [x] ET VOIP INVITE Message Flood UDP
  - [x] ET VOIP REGISTER Message Flood UDP
  - [x] ET VOIP Multiple Unauthorized SIP Responses UDP
  - [x] ET VOIP Possible Modified Sipvicious OPTIONS Scan
  - [x] ET VOIP Modified Sipvicious Asterisk PBX User-Agent
  - [x] ET VOIP Possible Inbound VOIP Scan/Misuse With User-Agent Zoiper
  - [x] ET VOIP Possible Misuse Call from Cisco ooh323
  - [x] ET VOIP Possible Misuse Call from MERA RTU
  - [ ] ET VOIP Q.931 Call Setup - Inbound
  - [x] ET VOIP H.323 in Q.931 Call Setup - Inbound
  - [x] GPL VOIP SIP INVITE message flooding
  - [x] GPL VOIP SIP 401 Unauthorized Flood
  - [x] GPL VOIP SIP 407 Proxy Authentication Required Flood
  - [x] GPL VOIP EXPLOIT SIP UDP Softphone overflow attempt

- [x] **emerging-web_client.rules** Hide
  - [ ] ET WEB_CLIENT IE process injection iexplore.exe executable download
  - [ ] ET WEB_CLIENT Attempt to execute VBScript code
  - [ ] ET WEB_CLIENT Stealth attempt to execute Javascript code
  - [ ] ET WEB_CLIENT Stealth attempt to execute VBScript code
  - [ ] ET WEB_CLIENT Stealth attempt to access SHELL#=#=
  - [ ] ET WEB_CLIENT Javascript execution with expression eval
  - [ ] ET WEB_CLIENT Javascript execution with expression eval hex
  - [ ] ET WEB_CLIENT IE trojan Ants3set 1.exe - process injection
  - [x] ET WEB_CLIENT Encoded javascriptdocument.write - usually hostile
  - [ ] ET WEB_CLIENT RealPlayer/Helix Player Format String Exploit
  - [ ] ET WEB_CLIENT IE StructuredGraphicsControl SourceURL Bug MoBB#6
  - [ ] ET WEB_CLIENT MSIE WebViewFolderIcon setSlice invalid memory copy
  - [ ] ET WEB_CLIENT Microsoft IE FTP URL Arbitrary Command Injection
  - [x] ET WEB_CLIENT Apple Quicktime RTSP Overflow (1)
  - [x] ET WEB_CLIENT Apple Quicktime RTSP Overflow (2)
  - [ ] ET WEB_CLIENT Apple Quicktime RTSP Content-Type overflow attempt
  - [x] ET WEB_CLIENT Apple Quicktime RTSP Content-Type overflow attempt
  - [ ] ET WEB_CLIENT Microsoft Internet Explorer ieframe.dll Script Injection Vulnerability
  - [ ] ET WEB_CLIENT Iframe in Purported Image Download (jpeg) - Likely SQL Injection Attacks Related
  - [ ] ET WEB_CLIENT Iframe in Purported Image Download (gif) - Likely SQL Injection Attacks Related
  - [ ] ET WEB_CLIENT Internet Explorer javascript onUnload http spliting attempt (body)
  - [ ] ET WEB_CLIENT Internet Explorer javascript onUnload http spliting attempt (img)
  - [ ] ET WEB_CLIENT Internet Explorer javascript onURLFlip http spliting attempt (body)
  - [ ] ET WEB_CLIENT Internet Explorer javascript onURLFlip http spliting attempt

- [x] ET WEB_CLIENT Possible Adobe Multimedia Doc.media.newPlayer Memory Corruption Attempt
- [ ] ET WEB_CLIENT Possible HTTP 404 XSS Attempt (External Source)
- [x] ET WEB_CLIENT Possible HTTP 406 XSS Attempt (External Source)
- [x] ET WEB_CLIENT Possible HTTP 503 XSS Attempt (External Source)
- [x] ET WEB_CLIENT VLC Media Player Aegisub Advanced SubStation (.ass) File Request flowbit set
- [x] ET WEB_CLIENT Possible Microsoft Internet Explorer URI Validation Remote Code Execution Attempt
- [x] ET WEB_CLIENT VLC Media Player smb URI Handling Remote Buffer Overflow Attempt
- [ ] ET WEB_CLIENT PDF With Unescape Method Defined Possible Hostile Obfuscation Attempt
- [ ] ET WEB_CLIENT Wscript Shell Run Attempt - Likely Hostile
- [ ] ET WEB_CLIENT Possible Java Deployment Toolkit Launch Method Remote Code Execution Attempt
- [ ] ET WEB_CLIENT Mozilla Firefox Window.Open Document URI Spoofing Attempt
- [x] ET WEB_CLIENT Likely Malicious PDF Containing StrReverse
- [x] ET WEB_CLIENT FakeAV scanner page encountered Initializing Virus Protection System
- [ ] ET WEB_CLIENT Driveby bredolab hidden div served by nginx
- [x] ET WEB_CLIENT PROPFIND Flowbit Set
- [x] ET WEB_CLIENT Possible Microsoft Internet Explorer CSS Cross-Origin Theft Attempt
- [x] ET WEB_CLIENT PDF With Embedded Adobe Shockwave Flash Possibly Related to Remote Code Execution Attempt
- [ ] ET WEB_CLIENT Possible Adobe CoolType Smart INdependent Glyplets - SING - Table uniqueName Stack Buffer Overflow Attempt
- [ ] ET WEB_CLIENT PDF With eval Function - Possibly Hostile
- [x] ET WEB_CLIENT PDF Name Representation Obfuscation of /Subtype
- [ ] ET WEB_CLIENT PDF Name Representation Obfuscation of EmbeddedFile
- [ ] ET WEB_CLIENT PDF Name Representation Obfuscation of Javascript
- [ ] ET WEB_CLIENT PDF Name Representation Obfuscation of JS
- [ ] ET WEB_CLIENT PDF Name Representation Obfuscation of OpenAction
- [x] ET WEB_CLIENT Adobe Shockwave Director tSAC Chunk memory corruption Attempt
- [ ] ET WEB_CLIENT Possible Microsoft Internet Explorer Dynamic Object Tag/URLMON Sniffing Cross Domain Information Disclosure Attempt
- [ ] ET WEB_CLIENT Possible Microsoft Internet Explorer mshtml.dll Timer ID Memory Pointer Information Disclosure Attempt
- [x] ET WEB_CLIENT Possible Javascript obfuscation using app.setTimeOut in PDF in Order to Run Code
- [x] ET WEB_CLIENT Microsoft IE CSS Clip Attribute Memory Corruption (POC SPECIFIC)
- [x] ET WEB_CLIENT Possible Adobe Reader 9.4 this.printSeps Memory Corruption Attempt
- [x] ET WEB_CLIENT Hex Obfuscation of String.fromCharCode % Encoding
- [x] ET WEB_CLIENT Hex Obfuscation of charCodeAt % Encoding
- [x] ET WEB_CLIENT Winzip 15.0 WZFLDVW.OCX IconIndex Property Denial of Service
- [ ] ET WEB_CLIENT Flash Player Flash6.ocx AllowScriptAccess Denial of Service
- [x] ET WEB_CLIENT Hex Obfuscation of document.write %u UTF-8 Encoding
- [x] ET WEB_CLIENT Hex Obfuscation of arguments.callee %u UTF-8 Encoding
- [ ] ET WEB_CLIENT Possible Internet Explorer CSS Parser Remote Code Execution Attempt
- [ ] ET WEB_CLIENT Possible HTTP 403 XSS Attempt (External Source)
- [x] ET WEB_CLIENT Possible HTTP 405 XSS Attempt (External Source)
- [x] ET WEB_CLIENT Possible HTTP 500 XSS Attempt (External Source)
- [x] ET WEB_CLIENT Possible Adobe Reader and Acrobat Forms Data Format Remote Security Bypass Attempt
- [x] ET WEB_CLIENT VLC Media Player .ass File Buffer Overflow Attempt
- [x] ET WEB_CLIENT Possible Internet Explorer srcElement Memory Corruption Attempt
- [ ] ET WEB_CLIENT DX Studio Player Firefox Plug-in Command Injection Attempt
- [ ] ET WEB_CLIENT Possible IE iepeers.dll Use-after-free Code Execution Attempt
- [x] ET WEB_CLIENT Possible Foxit/Adobe PDF Reader Launch Action Remote Code Execution Attempt
- [ ] ET WEB_CLIENT Malvertising drive by kit encountered - Loading...
- [x] ET WEB_CLIENT PDF Containing Windows Commands Downloaded
- [x] ET WEB_CLIENT Possible PDF Launch Function Remote Code Execution Attempt with Name Representation Obfuscation
- [ ] ET WEB_CLIENT Possible String.FromCharCode Javascript Obfuscation Attempt
- [ ] ET WEB_CLIENT Possible Apple Quicktime Invalid SMIL URI Buffer Overflow Attempt
- [x] ET WEB_CLIENT DLL or EXE File From Possible WebDAV Share Possible DLL Preloading Exploit Attempt
- [x] ET WEB_CLIENT RealPlayer FLV Parsing Integer Overflow Attempt
- [x] ET WEB_CLIENT Possible Adobe Acrobat and Reader Pushstring Memory Corruption Attempt
- [x] ET WEB_CLIENT PDF With Embedded Flash Possible Remote Code Execution Attempt
- [x] ET WEB_CLIENT Possible Adobe Acrobat Reader Newclass Invalid Pointer Remote Code Execution Attempt
- [x] ET WEB_CLIENT PDF Name Representation Obfuscation of Action
- [ ] ET WEB_CLIENT PDF Name Representation Obfuscation of Type
- [ ] ET WEB_CLIENT PDF Name Representation Obfuscation of URL
- [x] ET WEB_CLIENT PDF Name Representation Obfuscation of Pages
- [x] ET WEB_CLIENT Firefox Plugin Parameter EnsureCachedAttrParamArrays Remote Code Execution Attempt
- [x] ET WEB_CLIENT Adobe Acrobat newfunction Remote Code Execution Attempt
- [x] ET WEB_CLIENT Java Web Start Command Injection (jar)
- [ ] ET WEB_CLIENT Possible Oracle Java APPLET Tag Children Property Memory Corruption Attempt
- [ ] ET WEB_CLIENT Possible Microsoft Internet Explorer CSS Tags Remote Code Execution Attempt
- [x] ET WEB_CLIENT Firefox Interleaving document.write and appendChild Overflow (POC SPECIFIC)
- [ ] ET WEB_CLIENT MALVERTISING Alureon JavaScript IFRAME Redirect
- [x] ET WEB_CLIENT Hex Obfuscation of String.fromCharCode %u UTF-8 Encoding
- [x] ET WEB_CLIENT Hex Obfuscation of charCodeAt %u UTF-8 Encoding
- [x] ET WEB_CLIENT Winzip 15.0 WZFLDVW.OCX Text Property Denial of Service
- [x] ET WEB_CLIENT Hex Obfuscation of document.write % Encoding
- [x] ET WEB_CLIENT Hex Obfuscation of arguments.callee % Encoding
- [x] ET WEB_CLIENT Foxit PDF Reader Title Stack Overflow
- [x] ET WEB_CLIENT Oracle Java 6 Object Tag launchjnlp docbase Parameters Flowbits Set

- [x] ET WEB_CLIENT Oracle Java 6 Object Tag launchjnlp docbase Parameters Buffer Overflow
- [x] ET WEB_CLIENT Hex Obfuscation of document.write %u UTF-16 Encoding
- [x] ET WEB_CLIENT Hex Obfuscation of String.fromCharCode %u UTF-16 Encoding
- [x] ET WEB_CLIENT AVI RIFF Chunk Access Flowbit Set
- [x] ET WEB_CLIENT DXF Extension File Detection Access Flowbit Set
- [x] ET WEB_CLIENT eval String.fromCharCode String Which May Be Malicious
- [ ] ET WEB_CLIENT Possible Malicious String.fromCharCode with charCodeAt String
- [x] ET WEB_CLIENT Possible %u UTF-8 Encoded Iframe Tag
- [x] ET WEB_CLIENT Possible # Encoded Iframe Tag
- [x] ET WEB_CLIENT Hex Obfuscation of parseInt % Encoding
- [x] ET WEB_CLIENT Hex Obfuscation of parseInt %u UTF-16 Encoding
- [x] ET WEB_CLIENT Hex Obfuscation of Script Tag %u UTF-8 Encoding
- [x] ET WEB_CLIENT Hex Obfuscation of unescape % Encoding
- [x] ET WEB_CLIENT Hex Obfuscation of unescape %u UTF-16 Encoding
- [x] ET WEB_CLIENT Hex Obfuscation of substr %u UTF-8 Encoding
- [x] ET WEB_CLIENT Hex Obfuscation of eval % Encoding
- [x] ET WEB_CLIENT Hex Obfuscation of eval %u UTF-16 Encoding
- [x] ET WEB_CLIENT Obfuscated Javascript // ptth (escaped)
- [x] ET WEB_CLIENT Hex Obfuscation of replace Javascript Function %u UTF-8 Encoding
- [ ] ET WEB_CLIENT Likely Hostile Eval CRYPT.obfuscate Usage
- [x] ET WEB_CLIENT Opera Window.Open document.cloneNode Null Pointer Deference Attempt
- [ ] ET WEB_CLIENT WindowsLive Imposter Site Landing Page
- [ ] ET WEB_CLIENT Likely Redirector to Exploit Page /in/rdrct/rckt/?
- [ ] ET WEB_CLIENT Windows Help and Support Center XSS Attempt
- [x] ET WEB_CLIENT PDF With Adobe Audition Session File Handling Buffer Overflow Flowbit Set
- [x] ET WEB_CLIENT Download of PDF With Uncompressed Flash Content flowbit set
- [x] ET WEB_CLIENT Adobe Audition Malformed Session File Buffer Overflow Attempt
- [ ] ET WEB_CLIENT Malicious PHP 302 redirect response with avtor URI and cookie
- [ ] ET WEB_CLIENT Adobe Shockwave rcsL Chunk Remote Code Execution Attempt
- [x] ET WEB_CLIENT Mozilla Firefox nsTreeSelection Element invalidateSelection Remote Code Execution Attempt
- [x] ET WEB_CLIENT Adobe Acrobat Reader FlateDecode Stream Predictor Exploit Attempt
- [ ] ET WEB_CLIENT Known Injected Credit Card Fraud Malvertisement Script
- [ ] ET WEB_CLIENT Microsoft Word RTF pFragments Stack Overflow Attempt (CVE-2010-3333)
- [x] ET WEB_CLIENT Adobe Flash Player Button Remote Code Execution Attempt
- [x] ET WEB_CLIENT Microsoft Visio 2003 mfc71enu.dll DLL Loading Arbitrary Code Execution Attempt
- [ ] ET WEB_CLIENT Wordpress possible Malicious DNS-Requests - picasa.com.*
- [ ] ET WEB_CLIENT Wordpress possible Malicious DNS-Requests - wordpress.com.*
- [ ] ET WEB_CLIENT Wordpress possible Malicious DNS-Requests - upload.wikimedia.com.*
- [ ] ET WEB_CLIENT Malicious 1px iframe related to Mass Wordpress Injections
- [ ] ET WEB_CLIENT Phoenix landing page JAVASMB
- [x] ET WEB_CLIENT Hex Obfuscation of arguments.callee %u UTF-16 Encoding
- [x] ET WEB_CLIENT Hex Obfuscation of charCodeAt %u UTF-16 Encoding
- [ ] ET WEB_CLIENT Possible Hex Obfuscation Usage On Webpage
- [x] ET WEB_CLIENT Microsoft Windows MPEG Layer-3 Audio Decoder Buffer Overflow
- [x] ET WEB_CLIENT Microsoft Office Visio DXF File Processing Remote Code Execution
- [x] ET WEB_CLIENT Adobe Reader and Acrobat U3D File Invalid Array Index Remote Code Execution Attempt
- [x] ET WEB_CLIENT Possible % Encoded Iframe Tag
- [x] ET WEB_CLIENT Possible %u UTF-16 Encoded Iframe Tag
- [x] ET WEB_CLIENT Hex Obfuscation of document.write # Encoding
- [x] ET WEB_CLIENT Hex Obfuscation of parseInt %u UTF-8 Encoding
- [x] ET WEB_CLIENT Hex Obfuscation of Script Tag % Encoding
- [x] ET WEB_CLIENT Hex Obfuscation of Script Tag %u UTF-16 Encoding
- [x] ET WEB_CLIENT Hex Obfuscation of unescape %u UTF-8 Encoding
- [x] ET WEB_CLIENT Hex Obfuscation of substr % Encoding
- [x] ET WEB_CLIENT Hex Obfuscation of substr %u UTF-16 Encoding
- [x] ET WEB_CLIENT Hex Obfuscation of eval %u UTF-8 Encoding
- [x] ET WEB_CLIENT Obfuscated Javascript // ptth
- [x] ET WEB_CLIENT Hex Obfuscation of replace Javascript Function % Encoding
- [x] ET WEB_CLIENT Hex Obfuscation of replace Javascript Function %u UTF-16 Encoding
- [x] ET WEB_CLIENT Android Webkit removeChild Use-After-Free Remote Code Execution Attempt
- [x] ET WEB_CLIENT Microsoft OLE Compound File Magic Bytes Flowbit Set
- [ ] ET WEB_CLIENT Office File With Embedded Executable
- [ ] ET WEB_CLIENT Unknown .ru Exploit Redirect Page
- [x] ET WEB_CLIENT QuickTime Remote Exploit (exploit specific)
- [x] ET WEB_CLIENT PDF With Adobe Audition Session File Handling Memory Corruption Attempt
- [x] ET WEB_CLIENT Download of PDF With Compressed Flash Content
- [ ] ET WEB_CLIENT Request to malicious info.php drive-by landing
- [ ] ET WEB_CLIENT Sidename.js Injected Script Served by Local WebServer
- [x] ET WEB_CLIENT Adobe Shockwave Director tSAC Chunk memory corruption Attempt
- [x] ET WEB_CLIENT Adobe Acrobat Util.printf Buffer Overflow Attempt
- [ ] ET WEB_CLIENT cssminibar.js Injected Script Served by Local WebServer
- [ ] ET WEB_CLIENT Microsoft Word RTF pFragments Stack Buffer Overflow Attempt (CVE-2010-3333)
- [x] ET WEB_CLIENT Adobe Authplay.dll NewClass Memory Corruption Attempt
- [ ] ET WEB_CLIENT Internet Explorer toStaticHTML HTML Sanitizing Information Disclosure Attempt
- [ ] ET WEB_CLIENT Wordpress possible Malicious DNS-Requests - flickr.com.*
- [ ] ET WEB_CLIENT Wordpress possible Malicious DNS-Requests - blogger.com.*
- [ ] ET WEB_CLIENT Wordpress possible Malicious DNS-Requests - img.youtube.com.*
- [ ] ET WEB_CLIENT Wordpress possible Malicious DNS-Requests - photobucket.com.*
- [x] ET WEB_CLIENT Mozilla Firefox mChannel Object Dangling Pointer Use-After-Free Memory Corruption Attempt
- [ ] ET WEB_CLIENT Google Chrome Multiple Iframe PDF File Handling Memory Corruption Attempt

- [ ] ET WEB_CLIENT Lilupophilupop Injected Script Being Served to Client
- [x] ET WEB_CLIENT PDF With Embedded U3D
- [ ] ET WEB_CLIENT MALVERTISING Alureon Malicious IFRAME
- [x] ET WEB_CLIENT Likely Driveby Delivered Malicious PDF
- [x] ET WEB_CLIENT Likely MS12-004 midiOutPlayNextPolyEvent Heap Overflow Midi Filename Requested baby.mid
- [ ] ET WEB_CLIENT Adobe Flash Player Malformed MP4 Remote Code Execution Attempt (CVE-2012-0754)
- [ ] ET WEB_CLIENT landing page with malicious Java applet
- [ ] ET WEB_CLIENT Nikjju Mass Injection Internal WebServer Compromised
- [ ] ET WEB_CLIENT MP4 Embedded in PDF File - Potential Flash Exploit (CVE-2012-0754)
- [ ] ET WEB_CLIENT Microsoft Internet Explorer SameID Use-After-Free (CVE-2012-1875)
- [x] ET WEB_CLIENT FoxxySoftware - Landing Page
- [ ] ET WEB_CLIENT FoxxySoftware - Landing Page Received - applet and 0px
- [ ] ET WEB_CLIENT Base64 - Landing Page Received - base64encode(GetOs()
- [x] ET WEB_CLIENT c3284d Malware Network Compromised Redirect (comments 1)
- [ ] ET WEB_CLIENT Unknown_s=1 - Landing Page - 10HexChar Title and applet
- [x] ET WEB_CLIENT c3284d malware network iframe
- [ ] ET WEB_CLIENT Fake-AV Conditional Redirect (Blackmuscats)
- [ ] ET WEB_CLIENT Potential MSXML2.DOMDocument.4-6.0 Uninitialized Memory Corruption (CVE-2012-1889)
- [ ] ET WEB_CLIENT Obfuscated Javascript redirecting to badness August 6 2012
- [ ] ET WEB_CLIENT Malicious Redirect n.php h=*&s=*
- [x] ET WEB_CLIENT Microsoft Rich Text File download - SET
- [ ] ET WEB_CLIENT MALVERTISING FlashPost - Redirection IFRAME
- [ ] ET WEB_CLIENT Hostile Gate landing seen with pamdql/Sweet Orange /in.php?q=
- [ ] ET WEB_CLIENT Drupal Mass Injection Campaign Outbound
- [x] ET WEB_CLIENT Injected iframe leading to Redkit Jan 02 2013
- [ ] ET WEB_CLIENT Malicious iframe
- [ ] ET WEB_CLIENT Exploit Specific Uncompressed Flash (CVE-2013-0634)
- [ ] ET WEB_CLIENT Flash Action Script Invalid Regex (CVE-2013-0634)
- [ ] ET WEB_CLIENT Nuclear landing with obfuscated plugindetect Apr 29 2013
- [ ] ET WEB_CLIENT Injection - var j=0
- [ ] ET WEB_CLIENT MALVERTISING Flash - URI - /loading?vkn=
- [ ] ET WEB_CLIENT Sweet Orange Landing with Applet July 08 2013
- [x] ET WEB_CLIENT Fake Adobe Flash Player malware binary requested
- [ ] ET WEB_CLIENT Probable FlimKit Redirect July 10 2013
- [ ] ET WEB_CLIENT Potential Internet Explorer Use After Free (CVE-2013-3163)
- [ ] ET WEB_CLIENT Microsoft Internet Explorer Use-After-Free (CVE-2013-3163)
- [x] ET WEB_CLIENT JS Browser Based Ransomware
- [ ] ET WEB_CLIENT FlimKit Landing 07/22/13 2
- [ ] ET WEB_CLIENT FlimKit Landing 07/22/13 4
- [x] ET WEB_CLIENT c0896 Hacked Site Response (Inbound) 2
- [x] ET WEB_CLIENT c0896 Hacked Site Response Octal (Inbound)
- [ ] ET WEB_CLIENT Lilupophilupop Injected Script Being Served from Local Server
- [ ] ET WEB_CLIENT MALVERTISING OpenX BrowserDetect.init Download
- [ ] ET WEB_CLIENT User-Agent used in Injection Attempts
- [x] ET WEB_CLIENT Microsoft Windows Media component specific exploit
- [ ] ET WEB_CLIENT Clickpayz redirection to *.clickpayz.com
- [x] ET WEB_CLIENT Internet Explorer CTableRowCellsCollectionCacheItem.GetNext Memory Use-After-Free Attempt
- [ ] ET WEB_CLIENT Nikjju Mass Injection Compromised Site Served To Local Client
- [ ] ET WEB_CLIENT FakeAV Landing Page - Viruses were found
- [ ] ET WEB_CLIENT RedKit - Landing Page Received - applet and code
- [ ] ET WEB_CLIENT Obfuscated Javascript redirecting to badness 21 June 2012
- [ ] ET WEB_CLIENT FoxxySoftware - Landing Page Received - foxxysoftware
- [ ] ET WEB_CLIENT Potential MSXML2.DOMDocument Uninitialized Memory Corruption (CVE-2012-1889)
- [ ] ET WEB_CLIENT Runforestrun Malware Campaign Infected Website Landing Page Obfuscated String JavaScript DGA
- [x] ET WEB_CLIENT c3284d Malware Network Compromised Redirect (comments 2)
- [ ] ET WEB_CLIENT Unknown_s=1 - Landing Page - 100HexChar value and applet
- [x] ET WEB_CLIENT c3284d Malware Network Compromised Redirect (comments 3)
- [ ] ET WEB_CLIENT Potential MSXML2.DOM Document.3.0 Uninitialized Memory Corruption Attempt (CVE-2012-1889)
- [x] ET WEB_CLIENT Potential MSXML2.FreeThreadedDOMDocument Uninitialized Memory Corruption Attempt
- [ ] ET WEB_CLIENT FlimKit/Other - Landing Page - 100HexChar value and applet
- [ ] ET WEB_CLIENT Internet Explorer execCommand function Use after free Vulnerability (CVE-2012-4969)
- [ ] ET WEB_CLIENT SofosFO/NeoSploit possible second stage landing page
- [x] ET WEB_CLIENT Possible Malvertising FlashPost - POST to *.stats
- [ ] ET WEB_CLIENT Drupal Mass Injection Campaign Inbound
- [ ] ET WEB_CLIENT RedKit - Landing Page
- [x] ET WEB_CLIENT Malicious iframe
- [x] ET WEB_CLIENT Microsoft OLE Compound File With Flash
- [ ] ET WEB_CLIENT Exploit Specific Uncompressed Flash Inside of OLE (CVE-2013-0634)
- [ ] ET WEB_CLIENT Flash Action Script Invalid Regex (CVE-2013-0634)
- [ ] ET WEB_CLIENT Possible Internet Explorer Use After Free Inbound (CVE-2013-1347)
- [ ] ET WEB_CLIENT Sweet Orange Landing Page May 16 2013
- [ ] ET WEB_CLIENT Malicious Redirect June 18 2013
- [x] ET WEB_CLIENT Fake Adobe Flash Player update warning enticing clicks to malware payload
- [x] ET WEB_CLIENT DRIVEBY Redirection - Wordpress Injection
- [ ] ET WEB_CLIENT FlimKit Landing July 10 2013
- [ ] ET WEB_CLIENT Potential Internet Explorer Use After Free CVE-2013-3163 2
- [ ] ET WEB_CLIENT DRIVEBY Redirection - phpBB Injection
- [ ] ET WEB_CLIENT FlimKit Landing 07/22/13
- [ ] ET WEB_CLIENT FlimKit Landing 07/22/13 3
- [x] ET WEB_CLIENT c0896 Hacked Site Response (Inbound) 1
- [x] ET WEB_CLIENT c0896 Hacked Site Response (Inbound) 3
- [x] ET WEB_CLIENT c0896 Hacked Site Response Hex (Inbound)

- [x] ET WEB_CLIENT c0896 Hacked Site Response (Inbound) 4
- [x] ET WEB_CLIENT Possible FortDisco Wordpress Brute-force Site list download 10+ wp-login.php
- [x] ET WEB_CLIENT CookieBomb Generic PHP Format
- [ ] ET WEB_CLIENT DRIVEBY Redirection - Forum Injection
- [ ] ET WEB_CLIENT Microsoft IE Memory Corruption Inbound (CVE-2013-3893)
- [ ] ET WEB_CLIENT Microsoft IE Memory Corruption Inbound (CVE-2013-3893)
- [ ] ET WEB_CLIENT Cushion Redirection
- [ ] ET WEB_CLIENT W32/Caphaw DriveBy Campaign Ping.html
- [ ] ET WEB_CLIENT Possible Microsoft Internet Explorer Use-After-Free (CVE-2013-3897)
- [ ] ET WEB_CLIENT Possible Cutwail Redirect to Magnitude EK
- [ ] ET WEB_CLIENT FaceBook IM & Web Driven Facebook Trojan Download
- [x] ET WEB_CLIENT DRIVEBY FakeUpdate - URI - /styles/javaupdate.css
- [ ] ET WEB_CLIENT Browlock Landing Page URI Struct
- [ ] ET WEB_CLIENT StyX Landing Jan 29 2014
- [x] ET WEB_CLIENT Malicious Redirect 8x8 script tag
- [x] ET WEB_CLIENT Possible BeEF Default SSL Cert
- [ ] ET WEB_CLIENT EXE Accessing Kaspersky System Driver (Possible Mask)
- [x] ET WEB_CLIENT EMET Detection Via XMLDOM
- [ ] ET WEB_CLIENT Malicious Spam Redirection Feb 28 2014
- [ ] ET WEB_CLIENT CritX/SafePack/FlashPack SilverLight Secondary Landing
- [ ] ET WEB_CLIENT Possible Word RTF Memory Corruption Payload Inbound (CVE-2014-1761)
- [x] ET WEB_CLIENT Microsoft Application Crash Report Indicates Potential VGX Memory Corruption
- [x] ET WEB_CLIENT Base64 Encoded Java Value
- [ ] ET WEB_CLIENT Sweet Orange WxH redirection
- [ ] ET WEB_CLIENT Possible GnuTLS Client ServerHello SessionID Overflow CVE-2014-3466
- [x] ET WEB_CLIENT Adobe Flash Player Rosetta Flash compressed CWS
- [x] ET WEB_CLIENT Adobe Flash Player Rosetta Flash compressed ZWS
- [x] ET WEB_CLIENT DRIVEBY Social Engineering Toolkit JAR Download
- [x] ET WEB_CLIENT DRIVEBY Social Engineering Toolkit Web Clone code detected
- [x] ET WEB_CLIENT Malicious iframe guessing router password 2
- [ ] ET WEB_CLIENT Upatre redirector GET Sept 29 2014
- [x] ET WEB_CLIENT DRIVEBY Generic URLENCODED CollectGarbage
- [ ] ET WEB_CLIENT Possible CVE-2014-4113 Exploit Download
- [ ] ET WEB_CLIENT FlashPack Secondary Landing Oct 29
- [x] ET WEB_CLIENT DRIVEBY FakeSupport - URI - windows-firewall.png
- [ ] ET WEB_CLIENT Possible Sweet Orange Landing Nov 3 2014
- [x] ET WEB_CLIENT GENERIC VB ShellExecute Function Inside of VBSCRIPT tag
- [x] ET WEB_CLIENT GENERIC Possible IE Memory Corruption CollectGarbage with DOM Reset
- [x] ET WEB_CLIENT Samsung Galaxy Knox Android Browser RCE smdm attempt
- [x] ET WEB_CLIENT PDF With Hidden Embedded File
- [ ] ET WEB_CLIENT Upatre Redirector Dec 16 2014 set
- [ ] ET WEB_CLIENT Upatre Download Redirection Dec 18 2014
- [x] ET WEB_CLIENT Internet Explorer execCommand function Use after free Vulnerability 0day Metasploit 2
- [ ] ET WEB_CLIENT Upatre IE Redirector Receiving Payload Jan 9 2015
- [ ] ET WEB_CLIENT Fake Trojan Dropper purporting to be missing application page landing
- [x] ET WEB_CLIENT Possible CookieBomb Generic JavaScript Format
- [x] ET WEB_CLIENT CookieBomb Generic HTML Format
- [ ] ET WEB_CLIENT MS13-055 CAnchorElement Use-After-Free
- [ ] ET WEB_CLIENT Internet Explorer Memory Corruption Inbound (CVE-2013-3893)
- [x] ET WEB_CLIENT Blatantly Evil JS Function
- [x] ET WEB_CLIENT W32/Caphaw DriveBy Campaign Statistic.js
- [ ] ET WEB_CLIENT Fake MS Security Update (Jar)
- [ ] ET WEB_CLIENT Unknown Malvertising Related EK Redirect Oct 14 2013
- [ ] ET WEB_CLIENT Malicious Cookie Set By Flash Malvertising
- [ ] ET WEB_CLIENT Magnitude Landing Nov 11 2013
- [ ] ET WEB_CLIENT DRIVEBY FakeUpdate - URI - Payload Requested
- [x] ET WEB_CLIENT DRIVEBY Redirection - Injection - Modified Edwards Packer Script
- [x] ET WEB_CLIENT CookieBomb 2.0 In Server Response Jan 29 2014
- [x] ET WEB_CLIENT BeEF Cookie Outbound
- [x] ET WEB_CLIENT Possible BeEF Module in use
- [ ] ET WEB_CLIENT Possible IE10 Use After Free CVE-2014-0322
- [ ] ET WEB_CLIENT Malicious Redirect Evernote Spam Campaign Feb 19 2014
- [ ] ET WEB_CLIENT Rawin Flash Landing URI Struct March 05 2014
- [x] ET WEB_CLIENT Generic HeapSpray Construct
- [x] ET WEB_CLIENT Microsoft Rich Text File .RTF File download with invalid listoverridecount
- [x] ET WEB_CLIENT Microsoft Application Crash Report Indicates Potential VGX Memory Corruption 2
- [ ] ET WEB_CLIENT Possible Malvertising Redirect URI Struct
- [ ] ET WEB_CLIENT Possible Malicious Injected Redirect June 02 2014
- [ ] ET WEB_CLIENT Trojan-Banker.JS.Banker fraudulent redirect boleto payment code
- [x] ET WEB_CLIENT Adobe Flash Player Rosetta Flash compressed FWS
- [ ] ET WEB_CLIENT Possible Malvertising Redirect URI Struct Jul 16 2014
- [x] ET WEB_CLIENT DRIVEBY Social Engineering Toolkit JAR filename detected
- [x] ET WEB_CLIENT Malicious iframe guessing router password 1
- [ ] ET WEB_CLIENT Flashpack Redirect Method 2
- [ ] ET WEB_CLIENT Upatre redirector 29 Sept 2014 - POST
- [ ] ET WEB_CLIENT Possible Sweet Orange redirection Oct 8 2014
- [x] ET WEB_CLIENT Possible CVE-2014-4113 Exploit Download with Hurricane Panda IOC
- [ ] ET WEB_CLIENT DRIVEBY FakeSupport - Landing Page - Windows Firewall Warning
- [ ] ET WEB_CLIENT DRIVEBY FakeSupport - Landing Page - Operating System Check
- [ ] ET WEB_CLIENT Sweet Orange Landing Nov 04 2013
- [x] ET WEB_CLIENT Possible Internet Explorer VBscript failure to handle error case information disclosure obfuscated CVE-2014-6332
- [ ] ET WEB_CLIENT Possible Internet Explorer VBscript failure to handle error case information disclosure CVE-2014-6332 Percent Hex Encode
- [x] ET WEB_CLIENT Possible Internet Explorer VBscript CVE-2014-6332 multiple redim preserve
- [ ] ET WEB_CLIENT HanJuan Landing Dec 10 2014
- [ ] ET WEB_CLIENT Upatre Redirector Dec 16 2014
- [ ] ET WEB_CLIENT Cushion Redirection URI Struct Mon Jan 05 2015
- [ ] ET WEB_CLIENT Upatre Redirector Jan 9 2015
- [ ] ET WEB_CLIENT Upatre Firefox/Chrome Redirector Receiving Payload Jan 9 2015

- [ ] ET WEB_CLIENT Upatre Redirector IE Requesting Payload Jan 19 2015
- [x] ET WEB_CLIENT Possible Android RCE via XSS and Play Store XFO
- [x] ET WEB_CLIENT DRIVEBY GENERIC ShellExecute in Hex No Seps
- [ ] ET WEB_CLIENT Possible Scam - FakeAV Alert Landing March 2 2015
- [x] ET WEB_CLIENT Microsoft Office RTF Stack Buffer Overflow
- [x] ET WEB_CLIENT Fake Windows Security Warning - png
- [x] ET WEB_CLIENT DRIVEBY EXE Embeded in Page Likely Evil M1
- [x] ET WEB_CLIENT Possible CVE-2013-1710/CVE-2012-3993 Firefox Exploit Attempt
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing June 4 2015 M1
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing June 4 2015 M3
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing June 8 2015 M2
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing June 11 2015 M2
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing June 16 2015 M1
- [x] ET WEB_CLIENT Fake AV Phone Scam Landing June 16 2015 M4
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing June 17 2015 M2
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing June 26 2015 M2
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing June 26 2015 M4
- [x] ET WEB_CLIENT Fake AV Phone Scam Landing June 26 2015 M5
- [x] ET WEB_CLIENT Fake AV Phone Scam Landing July 20 2015 M2
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing July 20 2015 M1
- [x] ET WEB_CLIENT Internet Explorer Memory Corruption Vulnerability (CVE-2015-2444)
- [x] ET WEB_CLIENT Evil JavaScript Injection Sep 29 2015
- [ ] ET WEB_CLIENT Evil Redirector from iframe Sep 29 2015
- [x] ET WEB_CLIENT Proxy - BurpSuite PortSwigger Proxy Certificate Seen
- [ ] ET WEB_CLIENT Fake Virus Phone Scam Landing Oct 19 M1
- [x] ET WEB_CLIENT Fake Virus Phone Scam Landing Oct 19 M3
- [ ] ET WEB_CLIENT Fake Virus Phone Scam Redirector Oct 19 M1
- [ ] ET WEB_CLIENT Fake Virus Phone Scam Redirector Oct 19 M3
- [x] ET WEB_CLIENT Fake Java Installer Landing Page Oct 21
- [ ] ET WEB_CLIENT Fake Virus Phone Scam Landing Oct 30
- [x] ET WEB_CLIENT Fake Video Player Update Scam Oct 30
- [ ] ET WEB_CLIENT Fake Virus Phone Scam JS Landing Nov 4
- [ ] ET WEB_CLIENT Fake Virus Phone Scam Landing Nov 4 M1
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing Nov 11
- [ ] ET WEB_CLIENT Fake Virus Phone Scam Landing Nov 16
- [x] ET WEB_CLIENT Possible eDellRoot Rogue Root CA
- [x] ET WEB_CLIENT Tech Support Phone Scam Landing Dec 30 M1
- [ ] ET WEB_CLIENT Fake Virus Phone Scam Landing Jan 13 M1
- [ ] ET WEB_CLIENT Fake Virus Phone Scam Landing Jan 13 M3
- [ ] ET WEB_CLIENT Chrome Tech Support Scam Landing Jan 26 2016
- [x] ET WEB_CLIENT Internet Explorer Memory Corruption Vulnerability (CVE-2016-0063)
- [ ] ET WEB_CLIENT Fake Hard Drive Delete Scam Landing Feb 16 M2
- [ ] ET WEB_CLIENT Fake Hard Drive Delete Scam Landing Feb 16 M4
- [ ] ET WEB_CLIENT Possible Fake AV Phone Scam Landing Feb 26
- [ ] ET WEB_CLIENT Possible Fake AV Phone Scam Long Domain M2 Feb 29
- [x] ET WEB_CLIENT Fake AV Phone Scam Domain M2 Mar 3
- [ ] ET WEB_CLIENT Microsoft Fake Support Phone Scam Mar 7
- [ ] ET WEB_CLIENT Generic Fake Support Phone Scam Mar 9 M1
- [x] ET WEB_CLIENT Generic Fake Support Phone Scam Mar 9 M3
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing Mar 15
- [ ] ET WEB_CLIENT Possible Fake AV Phone Scam Long Domain Mar 21 M1
- [ ] ET WEB_CLIENT Possible Fake AV Phone Scam Long Domain Mar 21 M3
- [ ] ET WEB_CLIENT Fake AV Phone Scam Mar 23
- [ ] ET WEB_CLIENT Possible Fake AV Phone Scam Long Domain Mar 30 M1
- [ ] ET WEB_CLIENT Upatre Redirector Jan 23 2015
- [x] ET WEB_CLIENT DRIVEBY GENERIC CollectGarbage in Hex String No Seps
- [x] ET WEB_CLIENT DRIVEBY GENERIC ShellExecute in URLENCODE
- [ ] ET WEB_CLIENT Possible Scam - FakeAV Alert Landing March 2 2015
- [ ] ET WEB_CLIENT Fake Windows Security Warning - Alert
- [x] ET WEB_CLIENT Firefox Proxy Prototype RCE Attempt (CVE-2014-8636)
- [x] ET WEB_CLIENT DRIVEBY EXE Embeded in Page Likely Evil M2
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing June 2 2015
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing June 4 2015 M2
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing June 8 2015 M1
- [x] ET WEB_CLIENT Fake AV Phone Scam Landing June 11 2015 M1
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing June 11 2015 M3
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing June 16 2015 M2
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing June 17 2015 M1
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing June 26 2015 M1
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing June 26 2015 M3
- [ ] ET WEB_CLIENT Fake AV Phone Scam Stylesheet June 26 2015
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing June 26 2015 M6
- [x] ET WEB_CLIENT Fake AV Phone Scam Landing July 20 2015 M4
- [x] ET WEB_CLIENT Possible Malicious Redirect 8x8 script tag URI struct
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing Sept 21 2015
- [x] ET WEB_CLIENT Evil Redirector Sep 29 2015
- [x] ET WEB_CLIENT Proxy - OWASP Zed Attack Proxy Certificate Seen
- [x] ET WEB_CLIENT Proxy - Fiddler Proxy Certificate Seen
- [ ] ET WEB_CLIENT Fake Virus Phone Scam Landing Oct 19 M2
- [ ] ET WEB_CLIENT Fake Virus Phone Scam Landing Oct 19 M4
- [ ] ET WEB_CLIENT Fake Virus Phone Scam Redirector Oct 19 M2
- [ ] ET WEB_CLIENT Fake Virus Phone Scam Landing Oct 19 M5
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing Oct 29
- [x] ET WEB_CLIENT Fake Virus Phone Scam Audio Oct 30
- [ ] ET WEB_CLIENT Fake Virus Phone Scam Landing Nov 4 M2
- [ ] ET WEB_CLIENT Fake Virus Phone Scam GET Nov 4
- [x] ET WEB_CLIENT Possible vBulletin object injection vulnerability Attempt
- [ ] ET WEB_CLIENT Fake Virus Phone Scam Landing Nov 16
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing Nov 20
- [ ] ET WEB_CLIENT Facebook password stealing inject Jan 04
- [ ] ET WEB_CLIENT Tech Support Phone Scam Landing Dec 30 M2
- [ ] ET WEB_CLIENT Fake Virus Phone Scam Landing Jan 13 M2
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing Jan 26 2016
- [x] ET WEB_CLIENT Evil Redirect Compromised WP Feb 01 2016
- [ ] ET WEB_CLIENT Fake Hard Drive Delete Scam Landing Feb 16 M1
- [ ] ET WEB_CLIENT Fake Hard Drive Delete Scam Landing Feb 16 M3
- [ ] ET WEB_CLIENT Fake Virus Phone Scam Landing Feb 17
- [x] ET WEB_CLIENT Possible Fake AV Phone Scam Long Domain M1 Feb 29
- [x] ET WEB_CLIENT Fake AV Phone Scam Domain M1 Mar 3
- [x] ET WEB_CLIENT Fake AV Phone Scam Domain M3 Mar 3
- [x] ET WEB_CLIENT Generic Fake Support Phone Scam Mar 8
- [ ] ET WEB_CLIENT Generic Fake Support Phone Scam Mar 9 M2
- [x] ET WEB_CLIENT Fake Virus Phone Scam Landing Mar 9 M2
- [ ] ET WEB_CLIENT Possible Fake AV Phone Scam Long Domain Mar 15
- [ ] ET WEB_CLIENT Possible Fake AV Phone Scam Long Domain Mar 21 M2
- [ ] ET WEB_CLIENT Possible Fake AV Phone Scam Long Domain Mar 23
- [x] ET WEB_CLIENT Fake Flash Update Mar 23
- [x] ET WEB_CLIENT Possible Fake AV Phone Scam Long Domain Mar 30 M2

- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing Apr 1
- [x] ET WEB_CLIENT Fake AV Phone Scam Landing Apr 4
- [ ] ET WEB_CLIENT Possible Fake AV Phone Scam Long Domain Apr 18 M1
- [ ] ET WEB_CLIENT Possible Fake AV Phone Scam Long Domain Apr 18 M3
- [ ] ET WEB_CLIENT Possible Fake AV Phone Scam Long Domain Apr 18 M5
- [ ] ET WEB_CLIENT Microsoft Fake Support Phone Scam May 10
- [x] ET WEB_CLIENT Tech Support Phone Scam Landing M5 Jun 3
- [ ] ET WEB_CLIENT Tech Support Phone Scam Landing M1 Jun 3
- [x] ET WEB_CLIENT Google Chrome Pdfium JPEG2000 Heap Overflow
- [ ] ET WEB_CLIENT Tech Support Phone Scam Landing Jun 29 M2
- [ ] ET WEB_CLIENT Tech Support Phone Scam Landing Jun 29 M4
- [ ] ET WEB_CLIENT Tech Support Phone Scam Landing M2 Jul 7
- [ ] ET WEB_CLIENT Tech Support Phone Scam Landing Jul 21 M2
- [x] ET WEB_CLIENT Tech Support Phone Scam Landing M2 Jul 29 2016
- [ ] ET WEB_CLIENT Tech Support Phone Scam Landing Jul 29 M4
- [ ] ET WEB_CLIENT Tech Support Phone Scam Landing Aug 10 M1
- [ ] ET WEB_CLIENT Tech Support Phone Scam Landing Aug 10 M3
- [ ] ET WEB_CLIENT Tech Support Phone Scam Landing Aug 10 M5
- [ ] ET WEB_CLIENT Tech Support Phone Scam Landing Aug 12 M2
- [x] ET WEB_CLIENT Tech Support Phone Scam Landing (msg.mp3) 2016-08-12
- [x] ET WEB_CLIENT Tech Support Phone Scam Landing M2 2016-08-12
- [ ] ET WEB_CLIENT Fake Mobile Virus Scam M1 Aug 18 2016
- [x] ET WEB_CLIENT Microsoft Tech Support Scam M1 2016-09-15
- [ ] ET WEB_CLIENT PC Support Tech Support Scam Sept 15 2016
- [x] ET WEB_CLIENT Tech Support Phone Scam Landing M1 Jan 20 2017
- [x] ET WEB_CLIENT Possible Chrome WebEx Extension RCE Attempt
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing Feb 2
- [x] ET WEB_CLIENT SUSPICIOUS Microsoft-Edge protocol in use (Observed in Magnitude EK)
- [x] ET WEB_CLIENT Possible MacOSX HelpViewer 10.12.1 XSS Arbitrary File Execution and Arbitrary File Read (CVE-2017-2361)
- [ ] ET WEB_CLIENT Lets Encrypt Free SSL Cert Observed in Tech Support Scams M1
- [ ] ET WEB_CLIENT Lets Encrypt Free SSL Cert Observed in Tech Support Scams M3
- [ ] ET WEB_CLIENT Lets Encrypt Free SSL Cert Observed in Tech Support Scams M5
- [ ] ET WEB_CLIENT Lets Encrypt Free SSL Cert Observed in Tech Support Scams M7
- [ ] ET WEB_CLIENT Lets Encrypt Free SSL Cert Observed in Tech Support Scams M9
- [x] ET WEB_CLIENT HTA File containing Wscript.Shell Call - Potential CVE-2017-0199
- [x] ET WEB_CLIENT Office UA FB SET
- [x] ET WEB_CLIENT Malicious SCF File Inbound
- [x] ET WEB_CLIENT Tech Support Phone Scam Landing (warning.mp3) Jan 24 2017
- [x] ET WEB_CLIENT BeEF HTTP Get Outbound
- [x] ET WEB_CLIENT Microsoft Tech Support Phone Scam M2 Jul 07 2017
- [x] ET WEB_CLIENT Microsoft Tech Support Phone Scam M3 Jul 07 2017
- [x] ET WEB_CLIENT Microsoft Tech Support Phone Scam M4 Jul 07 2017
- [x] ET WEB_CLIENT Fake Adobe Flash Update Landing - Title over non SSL
- [x] ET WEB_CLIENT Fake Adobe Flash Update Landing - Title over non SSL
- [x] ET WEB_CLIENT Fake Adobe Flash Update Landing - Title over non SSL
- [x] ET WEB_CLIENT Fake Adobe Flash Update Landing - Title over non SSL
- [x] ET WEB_CLIENT Possible Fake AV Phone Scam Long Domain Apr 4
- [ ] ET WEB_CLIENT Possible Fake AV Phone Scam Long Domain M3 Feb 29
- [ ] ET WEB_CLIENT Possible Fake AV Phone Scam Long Domain Apr 18 M2
- [ ] ET WEB_CLIENT Possible Fake AV Phone Scam Long Domain Apr 18 M4
- [ ] ET WEB_CLIENT Possible Fake AV Phone Scam Long Domain Apr 18 M6
- [ ] ET WEB_CLIENT Tech Support Phone Scam Landing M4 Jun 3
- [ ] ET WEB_CLIENT Tech Support Phone Scam Landing M3 Jun 3
- [ ] ET WEB_CLIENT Tech Support Phone Scam Landing M2 Jun 3
- [x] ET WEB_CLIENT Tech Support Phone Scam Landing M1 Jun 29 2016
- [x] ET WEB_CLIENT Tech Support Phone Scam Landing Jun 29 M3
- [ ] ET WEB_CLIENT Tech Support Phone Scam Landing M1 Jul 7
- [x] ET WEB_CLIENT Tech Support Phone Scam Landing 2016-07-21 M1
- [ ] ET WEB_CLIENT Tech Support Phone Scam Landing Jul 29 M1
- [ ] ET WEB_CLIENT Tech Support Phone Scam Landing Jul 29 M3
- [x] ET WEB_CLIENT Metasploit Browser Autopwn Aug1 2016
- [ ] ET WEB_CLIENT Tech Support Phone Scam Landing Aug 10 M2
- [ ] ET WEB_CLIENT Tech Support Phone Scam Landing Aug 10 M4
- [ ] ET WEB_CLIENT Tech Support Phone Scam Landing Aug 12 M1
- [x] ET WEB_CLIENT Tech Support Phone Scam Landing (err.mp3) 2016-08-12
- [x] ET WEB_CLIENT Tech Support Phone Scam Landing M1 2016-08-12
- [ ] ET WEB_CLIENT SMS Fake Mobile Virus Scam Aug 16 2016
- [ ] ET WEB_CLIENT Fake Mobile Virus Scam M2 Aug 18 2016
- [x] ET WEB_CLIENT Microsoft Tech Support Scam M2 2016-09-15
- [ ] ET WEB_CLIENT Microsoft Tech Support Scam M3 Sept 15 2016
- [ ] ET WEB_CLIENT Tech Support Phone Scam Landing M2 Jan 20 2017
- [ ] ET WEB_CLIENT Fake AV Phone Scam Landing Jan 24
- [x] ET WEB_CLIENT Tech Support Phone Scam Landing Feb 09 2017
- [x] ET WEB_CLIENT Android Fake AV Download Landing Mar 06 2017
- [x] ET WEB_CLIENT Fake Virus Phone Scam Landing Mar 09 2017
- [ ] ET WEB_CLIENT Lets Encrypt Free SSL Cert Observed in Tech Support Scams M2
- [ ] ET WEB_CLIENT Lets Encrypt Free SSL Cert Observed in Tech Support Scams M4
- [ ] ET WEB_CLIENT Lets Encrypt Free SSL Cert Observed in Tech Support Scams M6
- [ ] ET WEB_CLIENT Lets Encrypt Free SSL Cert Observed in Tech Support Scams M8
- [x] ET WEB_CLIENT HTA File Download Flowbit Set
- [x] ET WEB_CLIENT Office Requesting .HTA File Likely CVE-2017-0199 Request
- [x] ET WEB_CLIENT Office Discovery HTA file Likely CVE-2017-0199 Request M2
- [x] ET WEB_CLIENT Multibrowser Resource Exhaustion observed in Tech Support Scam
- [x] ET WEB_CLIENT Possible BeEF Module in use
- [x] ET WEB_CLIENT Watering Hole Redirect Inject Jun 28 2017
- [x] ET WEB_CLIENT Microsoft Tech Support Phone Scam M1 Jul 07 2017
- [x] ET WEB_CLIENT Apple Tech Support Phone Scam Jul 07 2017
- [x] ET WEB_CLIENT Tech Support Scam Landing Jul 19 2017
- [x] ET WEB_CLIENT Fake Adobe Flash Update Landing - Title over non SSL
- [x] ET WEB_CLIENT Fake Adobe Flash Update Landing - Title over non SSL
- [x] ET WEB_CLIENT Fake Adobe Flash Update Landing - Title over non SSL
- [x] ET WEB_CLIENT Tech Support Scam Sep 08 2017

- [x] ET WEB_CLIENT Download of Multimedia Content flowbit set
- [x] ET WEB_CLIENT Microsoft Tech Support Scam Landing M1 Oct 13 2017
- [x] ET WEB_CLIENT Tech Support Phone Scam Landing M2 Oct 16 2016
- [x] ET WEB_CLIENT Possible BadRabbit Driveby Download M2 Oct 24 2017
- [x] ET WEB_CLIENT pshell dl/execute primitives in wideb64 1
- [x] ET WEB_CLIENT pshell dl/execute primitives in wideb64 3
- [x] ET WEB_CLIENT pshell dl/execute primitives in wideb64 5
- [x] ET WEB_CLIENT SocEng Fake Font Download Template Nov 14 2017
- [x] ET WEB_CLIENT PWNJS JS Constructs
- [x] ET WEB_CLIENT Google Chrome XSS (CVE-2017-5124)
- [x] ET WEB_CLIENT PowerShell call in script 1
- [x] ET WEB_CLIENT Microsoft Rich Text File download with vulnerable ActiveX control flowbit set 1
- [x] ET WEB_CLIENT Microsoft Rich Text File download with vulnerable ActiveX control flowbit set 3
- [x] ET WEB_CLIENT Microsoft Excel file download - SET 1
- [x] ET WEB_CLIENT Malicious Fake JS Lib Inject
- [x] ET WEB_CLIENT Spectre Kernel Memory Leakage JavaScript
- [x] ET WEB_CLIENT Tech Support Phone Scam Landing 2018-01-10
- [x] ET WEB_CLIENT Malicious Chrome Extension Domain Request (stickies .pro in DNS Lookup)
- [x] ET WEB_CLIENT Fake AV Phone Scam Landing Feb 12
- [x] ET WEB_CLIENT [eSentire] Fake Flash Update 2018-07-09
- [x] ET WEB_CLIENT PolarisOffice Insecure Library Loading
- [x] ET WEB_CLIENT Fake 404 With Hidden Login Form
- [x] ET WEB_CLIENT Tech Support Phone Scam Landing 2017-07-26
- [x] ET WEB_CLIENT Tech Support Phone Scam Landing 2017-07-26
- [x] ET WEB_CLIENT VBscript UAF (CVE-2018-8373)
- [x] ET WEB_CLIENT Fake FlashPlayer Update Leading to CoinMiner M2 2018-10-12
- [x] ET WEB_CLIENT IE Double Free (CVE-2018-8460)
- [x] ET WEB_CLIENT Attempted WordPress GDPR Plugin Privilege Escalation M1 (Enable Registration)
- [x] ET WEB_CLIENT Tech Support Scam Landing M1 2019-04-15
- [x] ET WEB_CLIENT Attempted RCE in Wordpress Social Warfare Plugin Inbound (CVE-2019-9978)
- [x] ET WEB_CLIENT Possible JS Credit Card Stealer Inbound
- [x] ET WEB_CLIENT Possible FFSniff Inject Observed
- [x] ET WEB_CLIENT Possible Injected JS Form Stealer Checking Page Contents M2
- [x] ET WEB_CLIENT XHR POST Request - Possible Form Grabber Activity
- [x] ET WEB_CLIENT Great Cannon DDoS JS M2
- [x] ET WEB_CLIENT Great Cannon DDoS JS M4
- [x] ET WEB_CLIENT Tech Support Scam 2019-11-14
- [x] ET WEB_CLIENT Observed DNS Query to Malicious Cookie Monster Roulette JS Cookie Stealer Exfil Domain
- [x] ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
- [x] ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
- [x] ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
- [x] ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
- [x] ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
- [x] ET WEB_CLIENT Download of .MOV Content flowbit set
- [x] ET WEB_CLIENT Tech Support Phone Scam Landing M1 Oct 16 2016
- [x] ET WEB_CLIENT Possible BadRabbit Driveby Download M1 Oct 24 2017
- [x] ET WEB_CLIENT Fake Update/Installer ForceDL Template Nov 03 2017
- [x] ET WEB_CLIENT pshell dl/execute primitives in wideb64 2
- [ ] ET WEB_CLIENT pshell dl/execute primitives in wideb64 4
- [x] ET WEB_CLIENT pshell dl/execute primitives in wideb64 6
- [x] ET WEB_CLIENT Type Confusion Microsoft Edge (CVE-2017-11873)
- [x] ET WEB_CLIENT Apple Safari UXSS (CVE-2017-7089)
- [x] ET WEB_CLIENT Google Chrome Credential Stealing via SCF file Reflected Request
- [x] ET WEB_CLIENT PowerShell call in script 2
- [x] ET WEB_CLIENT Microsoft Rich Text File download with vulnerable ActiveX control flowbit set 2
- [x] ET WEB_CLIENT Hostile Microsoft Rich Text File (RTF) with corrupted listoverride
- [x] ET WEB_CLIENT Adobe Acrobat PDF Reader use after free JavaScript engine (CVE-2017-16393)
- [x] ET WEB_CLIENT Spectre Kernel Memory Leakage JavaScript (POC Based)
- [x] ET WEB_CLIENT Spectre Exploit Javascript
- [x] ET WEB_CLIENT Malicious Chrome Extension Domain Request (nyoogle .info in DNS Lookup)
- [x] ET WEB_CLIENT Malicious Chrome Extension Domain Request (lite-bookmarks .info in DNS Lookup)
- [x] ET WEB_CLIENT [Deepend Research] BestaBid FakeFlash Redirect
- [x] ET WEB_CLIENT Fake Adobe Software Update Landing
- [x] ET WEB_CLIENT Tech Support Scam Landing 2018-07-18
- [x] ET WEB_CLIENT Volexity - JS Sniffer Data Theft Beacon Detected
- [x] ET WEB_CLIENT Tech Support Phone Scam Landing 2017-07-26
- [x] ET WEB_CLIENT Microsoft Tech Support Phone Scam Landing 2018-09-12
- [x] ET WEB_CLIENT Fake FlashPlayer Update Leading to CoinMiner M1 2018-10-12
- [x] ET WEB_CLIENT Possible Microsoft Edge Remote Command Execution PoC (CVE-2018-8495)
- [x] ET WEB_CLIENT [Volex] Possible ColdFusion Unauthenticated Upload Attempt (CVE-2018-15961)
- [x] ET WEB_CLIENT Attempted WordPress GDPR Plugin Privilege Escalation M2 (Set as Administrator)
- [x] ET WEB_CLIENT Tech Support Scam Landing M2 2019-04-15
- [x] ET WEB_CLIENT Possible Confluence SSTI Exploitation Attempt - Leads to RCE/LFI (CVE-2019-3396)
- [x] ET WEB_CLIENT JS ShellWindows/AddInProcess Win10 DeviceGuardBypass Inbound
- [x] ET WEB_CLIENT Possible Injected JS Form Stealer Checking Page Contents M1
- [x] ET WEB_CLIENT Inbound JS with Possible 1px-1px Exfiltration Image
- [x] ET WEB_CLIENT Great Cannon DDoS JS M1
- [x] ET WEB_CLIENT Great Cannon DDoS JS M3
- [x] ET WEB_CLIENT Observed DNS Query to Malicious Cookie Monster Roulette JS Cookie Stealer Exfil Domain
- [x] ET WEB_CLIENT Tech Support Scam 2019-11-14
- [x] ET WEB_CLIENT Possible Embedded NTLM Hash Theft Code
- [x] ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
- [x] ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
- [x] ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
- [x] ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
- [x] ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)

☑ ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
☑ ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
☑ ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
☑ ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
☑ ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
☑ ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
☑ ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
☑ ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
☑ ET WEB_CLIENT Microsoft Tech Support Scam 2020-03-24
☑ ET WEB_CLIENT WSO 2.6 Webshell Accessed on External Compromised Server
☑ ET WEB_CLIENT X-Sec Webshell Accessed on External Compromised Server
☑ ET WEB_CLIENT WSO 4.2.5 Webshell Accessed on External Compromised Server
☑ ET WEB_CLIENT Kageyama Webshell Accessed on External Compromised Server
☑ ET WEB_CLIENT MINI MO Webshell Accessed on External Compromised Server
☑ ET WEB_CLIENT Generic WSO Webshell Password Prompt Accessed on External Compromised Server
☑ ET WEB_CLIENT Generic Mini Webshell Accessed on External Compromised Server
☑ ET WEB_CLIENT Generic Webshell Password Prompt Accessed on External Compromised Server
☑ ET WEB_CLIENT Leaf PHPMailer Accessed on External Server
☑ ET WEB_CLIENT Generic Webshell Password Prompt Accessed on External Compromised Server
☑ ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
☑ ET WEB_CLIENT Generic PHP Mailer Accessed on External Compromised Server
☑ ET WEB_CLIENT Generic PHP Mailer Accessed on External Compromised Server
☑ ET WEB_CLIENT Generic PHP Mailer Accessed on External Compromised Server
☑ ET WEB_CLIENT Generic PHP Mailer Accessed on External Compromised Server
☑ ET WEB_CLIENT Possible Apache DDos UA Observed (DDos Apache) Inbound
☑ ET WEB_CLIENT Generic Webshell Accessed on Compromised External Server
☑ ET WEB_CLIENT Generic Webshell Accessed on Compromised External Server
☑ ET WEB_CLIENT Generic Mailer Accessed on External Server
☑ ET WEB_CLIENT Generic Webshell Accessed on External Server
☑ ET WEB_CLIENT Generic Webshell Accessed on External Server
☑ ET WEB_CLIENT Generic Stolen Credentials Accessed on External Server
☑ ET WEB_CLIENT Cpanel Cracker Accessed on External Server
☑ ET WEB_CLIENT SEO Injection/Fraud DNS Lookup (count.trackstatisticss .com)
☑ ET WEB_CLIENT Generic PHP Uploader Accessed on External Server
☑ ET WEB_CLIENT SmailMax PHPMailer Accessed on External Server
☐ ET WEB_CLIENT Cushion Redirection
☑ ET WEB_CLIENT Generic Webshell Accessed on External Server
☑ ET WEB_CLIENT Generic Webshell Password Prompt Accessed on External Compromised Server
☑ ET WEB_CLIENT Generic Mailer Accessed on External Server

☑ ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
☑ ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
☑ ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
☑ ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
☑ ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
☑ ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
☑ ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
☑ ET WEB_CLIENT Observed Malicious SSL Cert (Charming Kitten Phishing Domain)
☑ ET WEB_CLIENT Tech Support Scam 2020-04-10
☑ ET WEB_CLIENT WSO 2.5 Webshell Accessed on External Compromised Server
☑ ET WEB_CLIENT ALFA TEaM Webshell Accessed on External Compromised Server
☑ ET WEB_CLIENT WSO 4.2.6 Webshell Accessed on External Compromised Server
☑ ET WEB_CLIENT Generic WSO Webshell Accessed on External Compromised Server
☑ ET WEB_CLIENT Generic WSO Webshell Password Prompt Accessed on External Compromised Server
☑ ET WEB_CLIENT Anonymous Webshell Accessed on External Compromised Server
☑ ET WEB_CLIENT Generic Webshell Password Prompt Accessed on External Compromised Server
☑ ET WEB_CLIENT WSO Webshell Password Prompt Accessed on External Compromised Server
☑ ET WEB_CLIENT Owl PHPMailer Accessed on External Server
☑ ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
☑ ET WEB_CLIENT WSO 2.6 Webshell Accessed on External Compromised Server
☑ ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
☑ ET WEB_CLIENT Generic PHP Mailer Accessed on External Compromised Server
☑ ET WEB_CLIENT Generic PHP Mailer Accessed on External Compromised Server
☑ ET WEB_CLIENT Generic PHP Mailer Accessed on External Compromised Server
☑ ET WEB_CLIENT Leaf PHPMailer Accessed on External Server
☑ ET WEB_CLIENT Generic Webshell Accessed on Compromised External Server
☑ ET WEB_CLIENT Generic Mailer Accessed on External Server
☑ ET WEB_CLIENT Generic Mailer Check Accessed on External Server
☑ ET WEB_CLIENT Generic Webshell Accessed on External Server
☑ ET WEB_CLIENT Generic Mailer Accessed on External Server
☑ ET WEB_CLIENT Generic Stolen Credentials Accessed on External Server
☑ ET WEB_CLIENT Generic Mailer Accessed on External Server
☑ ET WEB_CLIENT SEO Injection/Fraud Domain in DNS Lookup (stat.trackstatisticss .com)
☑ ET WEB_CLIENT Generic Webshell Accessed on External Server
☑ ET WEB_CLIENT Generic Email Spoofing Tool Accessed on External Compromised Server
☑ ET WEB_CLIENT Generic Webshell Accessed on External Server
☑ ET WEB_CLIENT Generic Webshell Accessed on External Server
☑ ET WEB_CLIENT Generic Webshell Password Prompt Accessed on External Compromised Server
☑ ET WEB_CLIENT Generic Mailer Accessed on Internal Server

- [x] ET WEB_CLIENT Predator the Thief Password Prompt Accessed on External Compromised Server
- [x] ET WEB_CLIENT FiercePhish Password Prompt Accessed on External Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Server
- [x] ET WEB_CLIENT Generic Webshell Password Prompt Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Mailer Accessed on External Server
- [x] ET WEB_CLIENT Generic Cpanel Cracker Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Password Prompt Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Tech Support Scam Landing 2020-08-19
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic File Upload Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Mailer Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Mailer Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Mailer Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Mailer Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Attempted Executable Drop via VBScript
- [x] ET WEB_CLIENT Generic Mailer Accessed on External Compromised Server
- [x] ET WEB_CLIENT Evil Keitaro Set-Cookie Inbound (9487d)
- [x] ET WEB_CLIENT Generic Uploader Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Mailer Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Mailer Accessed on External Compromised Server
- [x] ET WEB_CLIENT Exchange Webshell CnC Domain in DNS Lookup
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Tech Support Scam - Windows Firewall M2 2021-08-17
- [x] ET WEB_CLIENT Tech Support Scam - Windows Firewall M4 2021-08-17
- [x] ET WEB_CLIENT Tech Support Scam - Generic Components
- [x] ET WEB_CLIENT Generic Mailer Accessed on External Server
- [x] ET WEB_CLIENT Generic Webshell Password Prompt Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Password Prompt Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Password Prompt Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Mailer Accessed on External Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Server
- [x] ET WEB_CLIENT Generic Website Ransomnote Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Tech Support Scam Landing 2020-08-19
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Mailer Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Mailer Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Mailer Accessed on External Compromised Server
- [x] ET WEB_CLIENT Observed DNS Query to Malicious Cookie Monster Roulette JS Cookie Stealer Exfil Domain
- [x] ET WEB_CLIENT Generic Mailer Accessed on External Compromised Server
- [x] ET WEB_CLIENT APT/Hafnium SPORTSBALL Webshell Observed Outbound
- [x] ET WEB_CLIENT Leaf PHPMailer Accessed on External Server
- [x] ET WEB_CLIENT Generic Mailer Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Tech Support Scam - Windows Firewall M1 2021-08-17
- [x] ET WEB_CLIENT Tech Support Scam - Windows Firewall M3 2021-08-17
- [x] ET WEB_CLIENT Tech Support Scam - Windows Firewall M5 2021-08-17
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server

- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Generic Webshell Accessed on External Compromised Server
- [x] ET WEB_CLIENT Evil Keitaro Set-Cookie Inbound (85937)
- [x] ET WEB_CLIENT [TW] CAB From Possible WebDAV Share Possible DiagCab Abuse Attempt
- [x] ET WEB_CLIENT [TW] WEBDAV Requesting Startup Dir
- [x] ET WEB_CLIENT BeEF Style Request (GET)
- [x] ET WEB_CLIENT ALFA TEaM Shell Landing Page
- [x] ET WEB_CLIENT Observed Hunter Obfuscator Code M2
- [x] ET WEB_CLIENT PROPFIND Method Xbit Set
- [x] ET WEB_CLIENT WebDAV GET Request for .url Flowbit Set
- [x] ET WEB_CLIENT Request for search-ms file extension - Possible NTLM Hash Leak Attempt Attempt
- [x] ET WEB_CLIENT Zimbra zauthtoken Exfil Domain in DNS Lookup (zimbrauser .me)
- [ ] GPL WEB_CLIENT XMLHttpRequest attempt
- [ ] GPL WEB_CLIENT RealPlayer arbitrary javascript command attempt
- [ ] GPL WEB_CLIENT bitmap BitmapOffset integer overflow attempt
- [ ] GPL WEB_CLIENT web bug 0x0 gif attempt
- [ ] GPL WEB_CLIENT winamp .cda file name overflow attempt
- [ ] GPL WEB_CLIENT PNG large image height download attempt
- [ ] GPL WEB_CLIENT object type overflow attempt
- [x] ET WEB_CLIENT Suspicious PHP UNZIP Tool Accessed on External Possibly Compromised Server
- [x] ET WEB_CLIENT Observed JavaScript Event Listener with Clipboard Data
- [x] ET WEB_CLIENT [TW] WEBDAV UA
- [x] ET WEB_CLIENT [TW] CAB From Possible WebDAV Share Possible DiagCab Abuse Attempt
- [x] ET WEB_CLIENT BeEF Cookie (BEEFHOOK)
- [x] ET WEB_CLIENT BeEF Framework Comment In Response
- [x] ET WEB_CLIENT Observed Hunter Obfuscator Code M1
- [ ] ET WEB_CLIENT Suspected Credit Card Stealer Related Domain Domain in DNS Lookup (byvlsa .com)
- [x] ET WEB_CLIENT WebDAV Retrieving an .url
- [x] ET WEB_CLIENT WebDAV PUT Request for .url Flowbit Set
- [x] ET WEB_CLIENT Zimbra zauthtoken Value Extraction Script Requested (Inbound)
- [x] ET WEB_CLIENT Observed Zimbra zauthtoken Exfil Domain (zimbrauser .me in TLS SNI)
- [ ] GPL WEB_CLIENT Javascript document.domain attempt
- [ ] GPL WEB_CLIENT local resource redirection attempt
- [ ] GPL WEB_CLIENT libpng tRNS overflow attempt
- [ ] GPL WEB_CLIENT Microsoft ANI file parsing overflow
- [ ] GPL WEB_CLIENT PNG large image width download attempt
- [ ] GPL WEB_CLIENT PNG large colour depth download attempt
- [ ] GPL WEB_CLIENT Windows Media Player directory traversal via Content-Disposition attempt

- [ ] **emerging-web_server.rules** Show
- [ ] **emerging-web_specific_apps.rules** Show
- [x] **emerging-worm.rules** Hide

- [ ] ET WORM Potential MySQL bot scanning for SQL server
- [ ] ET WORM Shell Bot Code Download
- [ ] ET WORM Allaple ICMP Sweep Reply Inbound
- [ ] ET WORM Allaple ICMP Sweep Reply Outbound
- [x] ET WORM Win32.Socks.s HTTP Post Checkin
- [x] ET WORM Rimecud Worm checkin
- [x] ET WORM W32/Rimecud wg.txt Checkin
- [x] ET WORM TheMoon.linksys.router 1
- [x] ET WORM TheMoon.linksys.router 3
- [ ] GPL WORM mydoom.a backdoor upload/execute attempt
- [ ] ET WORM shell bot perl code download
- [ ] ET WORM Allaple ICMP Sweep Ping Outbound
- [ ] ET WORM Allaple ICMP Sweep Ping Inbound
- [ ] ET WORM SDBot HTTP Checkin
- [x] ET WORM Possible Worm Sohanad.Z or Other Infection Request for setting.nql
- [ ] ET WORM W32/Rimecud /qvod/ff.txt Checkin
- [x] ET WORM W32/Njw0rm CnC Beacon
- [x] ET WORM TheMoon.linksys.router 2
- [x] GPL WORM Slammer Worm propagation attempt OUTBOUND

Back Apply