IPFire_ - ipfire.localdomain

Intrusion Prevention System

Ruleset

- [x] **community-community.rules** Hide
  - [ ] MALWARE-BACKDOOR - Dagger_1.4.0
  - [ ] MALWARE-BACKDOOR netbus getinfo
  - [ ] MALWARE-BACKDOOR Infector.1.x
  - [ ] MALWARE-BACKDOOR Doly 2.0 access
  - [ ] MALWARE-BACKDOOR HackAttack 1.20 Connect
  - [ ] MALWARE-BACKDOOR NetSphere access
  - [ ] MALWARE-BACKDOOR BackConstruction 2.1 Connection
  - [ ] MALWARE-BACKDOOR BackConstruction 2.1 Server FTP Open Reply
  - [ ] MALWARE-BACKDOOR Matrix 2.0 Server access
  - [ ] MALWARE-BACKDOOR CDK
  - [ ] MALWARE-BACKDOOR PhaseZero Server Active on Network
  - [ ] MALWARE-BACKDOOR attempt
  - [ ] MALWARE-BACKDOOR MISC rewt attempt
  - [ ] MALWARE-BACKDOOR MISC Linux rootkit attempt lrkr0x
  - [ ] MALWARE-BACKDOOR MISC Linux rootkit satori attempt
  - [ ] MALWARE-BACKDOOR MISC Solaris 2.5 attempt
  - [ ] MALWARE-BACKDOOR HideSource backdoor attempt
  - [ ] PROTOCOL-ICMP tfn2k icmp possible communication
  - [ ] PROTOCOL-ICMP Stacheldraht server spoof
  - [ ] PROTOCOL-ICMP Stacheldraht server response
  - [ ] PROTOCOL-ICMP TFN client command BE
  - [ ] MALWARE-OTHER shaft client login to handler
  - [ ] MALWARE-OTHER Trin00 Daemon to Master *HELLO* message detected
  - [ ] MALWARE-OTHER Trin00 Attacker to Master default password
  - [ ] PROTOCOL-ICMP Stacheldraht client check gag
  - [ ] PROTOCOL-ICMP TFN server response
  - [ ] MALWARE-OTHER shaft agent to handler
  - [ ] MALWARE-OTHER mstream handler to agent
  - [ ] MALWARE-OTHER mstream agent pong to handler
  - [ ] MALWARE-OTHER mstream handler to client
  - [ ] PROTOCOL-ICMP - TFN client command LE
  - [ ] PROTOCOL-DNS SPOOF query response with TTL of 1 min. and no authority
  - [ ] PROTOCOL-DNS named authors attempt
  - [ ] SERVER-OTHER Bind Buffer Overflow via NXT records
  - [ ] SERVER-OTHER Bind Buffer Overflow via NXT records named overflow ADMROCKS
  - [ ] OS-LINUX x86 Linux overflow attempt
  - [ ] OS-LINUX x86 Linux overflow attempt ADMv2
  - [ ] OS-SOLARIS EXPLOIT sparc overflow attempt
  - [ ] OS-WINDOWS Microsoft WIndows IGMP dos attack
  - [ ] SERVER-OTHER RealNetworks Audio Server denial of service attempt
  - [ ] SERVER-OTHER RealNetworks Server template.html
  - [ ] SERVER-OTHER Ascend Route
  - [ ] PROTOCOL-POP EXPLOIT x86 BSD overflow
  - [ ] PROTOCOL-POP EXPLOIT x86 Linux overflow
  - [ ] PROTOCOL-POP EXPLOIT qpopper overflow
  - [ ] MALWARE-BACKDOOR QAZ Worm Client Login access
  - [ ] MALWARE-BACKDOOR NetBus Pro 2.0 connection established
  - [ ] MALWARE-BACKDOOR SatansBackdoor.2.0.Beta
  - [ ] MALWARE-BACKDOOR Infector 1.6 Client to Server Connection Request
  - [ ] PROTOCOL-FTP ADMw0rm ftp login attempt
  - [ ] MALWARE-BACKDOOR GateCrasher
  - [ ] MALWARE-BACKDOOR BackConstruction 2.1 Client FTP Open Request
  - [ ] MALWARE-BACKDOOR Matrix 2.0 Client connect
  - [ ] MALWARE-BACKDOOR WinCrash 1.0 Server Active
  - [ ] MALWARE-BACKDOOR DeepThroat 3.1 Server Response
  - [ ] MALWARE-BACKDOOR w00w00 attempt
  - [ ] MALWARE-BACKDOOR MISC r00t attempt
  - [ ] MALWARE-BACKDOOR MISC Linux rootkit attempt
  - [ ] MALWARE-BACKDOOR MISC Linux rootkit attempt
  - [ ] MALWARE-BACKDOOR MISC sm4ck attempt
  - [ ] MALWARE-BACKDOOR HidePak backdoor attempt
  - [ ] PROTOCOL-ICMP TFN Probe
  - [ ] MALWARE-OTHER Trin00 Daemon to Master PONG message detected
  - [ ] PROTOCOL-ICMP Stacheldraht gag server response
  - [ ] PROTOCOL-ICMP Stacheldraht client spoofworks
  - [ ] PROTOCOL-ICMP Stacheldraht client check skillz
  - [ ] MALWARE-OTHER Trin00 Daemon to Master message detected
  - [ ] MALWARE-OTHER Trin00 Attacker to Master default startup password
  - [ ] MALWARE-OTHER Trin00 Attacker to Master default mdie password
  - [ ] MALWARE-OTHER Trin00 Master to Daemon default password attempt
  - [ ] MALWARE-OTHER shaft handler to agent
  - [ ] MALWARE-OTHER mstream agent to handler
  - [ ] MALWARE-OTHER mstream handler ping to agent
  - [ ] MALWARE-OTHER mstream client to handler
  - [ ] MALWARE-OTHER mstream handler to client
  - [ ] PROTOCOL-DNS SPOOF query response PTR with TTL of 1 min. and no authority
  - [ ] PROTOCOL-DNS dns zone transfer via TCP detected
  - [ ] PROTOCOL-DNS named version attempt
  - [ ] SERVER-OTHER Bind Buffer Overflow via NXT records named overflow ADM
  - [ ] SERVER-OTHER Bind named overflow attempt
  - [ ] OS-LINUX x86 Linux overflow attempt
  - [ ] OS-OTHER x86 FreeBSD overflow attempt
  - [ ] SERVER-OTHER UDP echo+chargen bomb
  - [ ] PROTOCOL-ICMP ath
  - [ ] SERVER-OTHER RealNetworks Server template.html
  - [ ] SERVER-OTHER Bay/Nortel Nautica Marlin
  - [ ] BROWSER-OTHER Netscape 4.7 client overflow
  - [ ] PROTOCOL-POP EXPLOIT x86 BSD overflow
  - [ ] PROTOCOL-POP EXPLOIT x86 SCO overflow
  - [ ] OS-LINUX x86 Linux samba overflow

- [ ] OS-SOLARIS Oracle Solaris npls x86 overflow
- [ ] OS-LINUX Redhat 7.0 lprd overflow
- [ ] SERVER-OTHER SCO calserver overflow
- [ ] SERVER-OTHER VQServer admin
- [ ] SERVER-OTHER NextFTP client overflow
- [ ] SERVER-MAIL x86 windows MailMax overflow
- [ ] OS-LINUX ntalkd x86 Linux overflow
- [ ] OS-LINUX x86 Linux mountd overflow
- [ ] OS-LINUX x86 Linux mountd overflow
- [ ] PROTOCOL-FINGER account enumeration attempt
- [ ] PROTOCOL-FINGER root query
- [ ] PROTOCOL-FINGER remote command execution attempt
- [ ] PROTOCOL-FINGER bomb attempt
- [ ] PROTOCOL-FINGER cybercop query
- [ ] PROTOCOL-FINGER . query
- [ ] PROTOCOL-FTP .rhosts
- [ ] PROTOCOL-FTP CEL overflow attempt
- [ ] PROTOCOL-FTP iss scan
- [ ] PROTOCOL-FTP passwd retrieval attempt
- [ ] PROTOCOL-FTP saint scan
- [ ] PROTOCOL-FTP serv-u directory traversal
- [ ] PROTOCOL-FTP tar parameters
- [ ] PROTOCOL-ICMP IRDP router selection
- [ ] PROTOCOL-ICMP PING Unix
- [ ] PROTOCOL-ICMP PING BayRS Router
- [ ] PROTOCOL-ICMP PING Cisco Type.x
- [ ] PROTOCOL-ICMP PING Flowpoint2200 or Network Management Software
- [ ] PROTOCOL-ICMP PING LINUX/*BSD
- [ ] PROTOCOL-ICMP PING Network Toolbox 3 Windows
- [ ] PROTOCOL-ICMP PING Pinger Windows
- [ ] PROTOCOL-ICMP PING Oracle Solaris
- [ ] PROTOCOL-ICMP PING
- [ ] PROTOCOL-ICMP Address Mask Reply
- [ ] PROTOCOL-ICMP Address Mask Request
- [ ] PROTOCOL-ICMP Alternate Host Address
- [ ] PROTOCOL-ICMP Datagram Conversion Error
- [ ] PROTOCOL-ICMP Destination Unreachable Destination Host Unknown
- [ ] PROTOCOL-ICMP Destination Unreachable Fragmentation Needed and DF bit was set
- [ ] PROTOCOL-ICMP Destination Unreachable Host Unreachable for Type of Service
- [ ] PROTOCOL-ICMP Destination Unreachable Network Unreachable for Type of Service
- [ ] PROTOCOL-ICMP destination unreachable port unreachable packet detected
- [ ] PROTOCOL-ICMP Destination Unreachable Protocol Unreachable
- [ ] PROTOCOL-ICMP Destination Unreachable Source Route Failed
- [ ] PROTOCOL-ICMP Echo Reply
- [ ] PROTOCOL-ICMP Fragment Reassembly Time Exceeded
- [ ] PROTOCOL-ICMP IPV6 I-Am-Here undefined code
- [ ] PROTOCOL-ICMP IPV6 Where-Are-You undefined code
- [ ] PROTOCOL-ICMP Information Reply undefined code
- [ ] PROTOCOL-ICMP Information Request undefined code
- [ ] PROTOCOL-ICMP Mobile Host Redirect undefined code
- [ ] PROTOCOL-ICMP Mobile Registration Reply undefined code
- [ ] PROTOCOL-ICMP Mobile Registration Request undefined code
- [ ] PROTOCOL-ICMP Parameter Problem Missing a Required Option
- [ ] PROTOCOL-ICMP Parameter Problem undefined Code
- [ ] PROTOCOL-ICMP Photuris Unknown Security Parameters Index
- [ ] PROTOCOL-ICMP Photuris Valid Security Parameters, But Decryption Failed
- [ ] PROTOCOL-ICMP Redirect for TOS and Host
- [ ] PROTOCOL-ICMP Redirect undefined code
- [ ] SERVER-OTHER LPRng overflow
- [ ] SERVER-OTHER Bind Buffer Overflow named tsig overflow attempt
- [ ] SERVER-OTHER delegate proxy overflow
- [ ] SERVER-OTHER CHAT IRC topic overflow
- [ ] SERVER-MAIL sniffit overflow
- [ ] BROWSER-OTHER Netscape 4.7 unsucessful overflow
- [ ] SERVER-OTHER Bind Buffer Overflow named tsig overflow attempt
- [ ] OS-LINUX x86 Linux mountd overflow
- [ ] PROTOCOL-FINGER cmd_rootsh backdoor attempt
- [ ] PROTOCOL-FINGER search query
- [ ] PROTOCOL-FINGER null request
- [ ] PROTOCOL-FINGER remote command pipe execution attempt
- [ ] PROTOCOL-FINGER redirection attempt
- [ ] PROTOCOL-FINGER 0 query
- [ ] PROTOCOL-FTP .forward
- [ ] PROTOCOL-FTP CWD ~root attempt
- [ ] PROTOCOL-FTP adm scan
- [ ] PROTOCOL-FTP pass wh00t
- [ ] PROTOCOL-FTP piss scan
- [ ] PROTOCOL-FTP satan scan
- [ ] PROTOCOL-FTP SITE EXEC attempt
- [ ] PROTOCOL-ICMP IRDP router advertisement
- [ ] PROTOCOL-ICMP PING undefined code
- [ ] PROTOCOL-ICMP PING BSDtype
- [ ] PROTOCOL-ICMP PING BeOS4.x
- [ ] PROTOCOL-ICMP PING Delphi-Piette Windows
- [ ] PROTOCOL-ICMP PING IP NetMonitor Macintosh
- [ ] PROTOCOL-ICMP PING Microsoft Windows
- [ ] PROTOCOL-ICMP PING Ping-O-MeterWindows
- [ ] PROTOCOL-ICMP PING Seer Windows
- [ ] PROTOCOL-ICMP PING Windows
- [ ] PROTOCOL-ICMP traceroute
- [ ] PROTOCOL-ICMP Address Mask Reply undefined code
- [ ] PROTOCOL-ICMP Address Mask Request undefined code
- [ ] PROTOCOL-ICMP Alternate Host Address undefined code
- [ ] PROTOCOL-ICMP Datagram Conversion Error undefined code
- [ ] PROTOCOL-ICMP Destination Unreachable Destination Network Unknown
- [ ] PROTOCOL-ICMP Destination Unreachable Host Precedence Violation
- [ ] PROTOCOL-ICMP Destination Unreachable Host Unreachable
- [ ] PROTOCOL-ICMP Destination Unreachable Network Unreachable
- [ ] PROTOCOL-ICMP Destination Unreachable Precedence Cutoff in effect
- [ ] PROTOCOL-ICMP Destination Unreachable Source Host Isolated
- [ ] PROTOCOL-ICMP Destination Unreachable cndefined code
- [ ] PROTOCOL-ICMP Echo Reply undefined code
- [ ] PROTOCOL-ICMP IPV6 I-Am-Here
- [ ] PROTOCOL-ICMP IPV6 Where-Are-You
- [ ] PROTOCOL-ICMP Information Reply
- [ ] PROTOCOL-ICMP Information Request
- [ ] PROTOCOL-ICMP Mobile Host Redirect
- [ ] PROTOCOL-ICMP Mobile Registration Reply
- [ ] PROTOCOL-ICMP Mobile Registration Request
- [ ] PROTOCOL-ICMP Parameter Problem Bad Length
- [ ] PROTOCOL-ICMP Parameter Problem Unspecified Error
- [ ] PROTOCOL-ICMP Photuris Reserved
- [ ] PROTOCOL-ICMP Photuris Valid Security Parameters, But Authentication Failed
- [ ] PROTOCOL-ICMP Photuris undefined code!
- [ ] PROTOCOL-ICMP Redirect for TOS and Network
- [ ] PROTOCOL-ICMP Reserved for Security Type 19

- [ ] PROTOCOL-ICMP Reserved for Security Type 19 undefined code
- [ ] PROTOCOL-ICMP Router Advertisement
- [ ] PROTOCOL-ICMP Router Selection
- [ ] PROTOCOL-ICMP SKIP
- [ ] PROTOCOL-ICMP SKIP undefined code
- [ ] PROTOCOL-ICMP Source Quench undefined code
- [ ] PROTOCOL-ICMP Time-To-Live Exceeded in Transit
- [ ] PROTOCOL-ICMP Time-To-Live Exceeded in Transit undefined code
- [ ] PROTOCOL-ICMP Timestamp Reply
- [ ] PROTOCOL-ICMP Timestamp Reply undefined code
- [ ] PROTOCOL-ICMP Timestamp Request
- [ ] PROTOCOL-ICMP Timestamp Request undefined code
- [ ] PROTOCOL-ICMP Traceroute
- [ ] PROTOCOL-ICMP Traceroute undefined code
- [ ] PROTOCOL-ICMP unassigned type 1
- [ ] PROTOCOL-ICMP unassigned type 1 undefined code
- [ ] PROTOCOL-ICMP unassigned type 2
- [ ] PROTOCOL-ICMP unassigned type 2 undefined code
- [ ] PROTOCOL-ICMP unassigned type 7
- [ ] PROTOCOL-ICMP unassigned type 7 undefined code
- [ ] PROTOCOL-ICMP ISS Pinger
- [ ] PROTOCOL-ICMP L3retriever Ping
- [ ] PROTOCOL-ICMP Nemesis v1.1 Echo
- [ ] PROTOCOL-ICMP superscan echo
- [ ] PROTOCOL-ICMP webtrends scanner
- [ ] PROTOCOL-ICMP PING speedera
- [ ] PROTOCOL-ICMP TJPingPro1.1Build 2 Windows
- [ ] PROTOCOL-ICMP PING WhatsupGold Windows
- [ ] PROTOCOL-ICMP PING CyberKit 2.2 Windows
- [ ] PROTOCOL-ICMP PING Sniffer Pro/NetXRay network scan
- [ ] PROTOCOL-FTP no password
- [ ] SERVER-MAIL battle-mail traffic
- [ ] PROTOCOL-FTP Bad login
- [ ] PROTOCOL-TELNET login failed
- [ ] APP-DETECT psyBNC access
- [ ] INDICATOR-COMPROMISE command completed
- [ ] INDICATOR-COMPROMISE command error
- [ ] INDICATOR-COMPROMISE file copied ok
- [ ] INDICATOR-COMPROMISE id check returned root
- [ ] SERVER-OTHER Insecure TIMBUKTU Password
- [ ] PUA-OTHER PCAnywhere Attempted Administrator Login
- [ ] SERVER-OTHER gopher proxy
- [ ] SERVER-WEBAPP PCCS mysql database admin tool access
- [ ] POLICY-OTHER HP JetDirect LCD modification attempt
- [ ] PUA-OTHER PCAnywhere Failed Login
- [ ] SERVER-OTHER ramen worm
- [ ] PROTOCOL-SNMP NT UserList
- [ ] X11 xdmcp query
- [ ] PROTOCOL-TFTP Put
- [ ] PROTOCOL-TFTP parent directory
- [ ] PROTOCOL-TFTP root directory
- [ ] NETBIOS DCERPC NCACN-IP-TCP srvsvc NetrShareEnum null policy handle attempt
- [ ] OS-WINDOWS NT NULL session
- [ ] NETBIOS SMB CD..
- [ ] NETBIOS SMB CD...
- [ ] POLICY-SOCIAL Microsoft MSN message
- [ ] POLICY-SOCIAL ICQ access
- [ ] POLICY-SOCIAL IRC nick change
- [ ] INDICATOR-COMPROMISE FTP 'STOR 1MB' possible warez site
- [ ] INDICATOR-COMPROMISE FTP 'RETR 1MB' possible warez site
- [ ] INDICATOR-COMPROMISE FTP 'CWD / ' possible warez site
- [ ] INDICATOR-COMPROMISE FTP 'CWD ' possible warez site
- [ ] INDICATOR-COMPROMISE FTP 'MKD ' possible warez site
- [ ] INDICATOR-COMPROMISE FTP 'MKD .' possible warez site
- [ ] POLICY-OTHER FTP anonymous login attempt
- [ ] INDICATOR-COMPROMISE FTP 'MKD / ' possible warez site
- [ ] POLICY-OTHER WinGate telnet server response
- [ ] PUA-P2P Outbound GNUTella client request
- [ ] PUA-P2P GNUTella client request
- [ ] APP-DETECT VNC server response
- [ ] APP-DETECT PCAnywhere server response
- [ ] SERVER-MAIL SMTP relaying denied
- [ ] POLICY-OTHER HP JetDirect LCD modification attempt
- [ ] PROTOCOL-RPC snmpXdmi overflow attempt TCP
- [ ] PROTOCOL-RPC DOS ttdbserv Solaris
- [ ] PROTOCOL-RPC mountd TCP export request
- [ ] PROTOCOL-RPC portmap admind request UDP
- [ ] PROTOCOL-RPC portmap amountd request UDP
- [ ] PROTOCOL-RPC portmap bootparam request UDP
- [ ] PROTOCOL-RPC portmap cmsd request UDP
- [ ] PROTOCOL-RPC portmap mountd request UDP
- [ ] PROTOCOL-RPC portmap nisd request UDP
- [ ] PROTOCOL-RPC portmap pcnfsd request UDP
- [ ] PROTOCOL-RPC portmap rexd request UDP
- [ ] PROTOCOL-RPC portmap rstatd request UDP
- [ ] PROTOCOL-RPC portmap rusers request UDP
- [ ] PROTOCOL-RPC Solaris UDP portmap sadmin port query request attempt
- [ ] PROTOCOL-RPC portmap selection_svc request UDP
- [ ] PROTOCOL-RPC portmap status request UDP
- [ ] PROTOCOL-RPC portmap ttdbserv request UDP
- [ ] PROTOCOL-RPC portmap yppasswd request UDP
- [ ] PROTOCOL-RPC portmap ypserv request UDP
- [ ] PROTOCOL-RPC portmap ypupdated request TCP
- [ ] PROTOCOL-RPC portmap snmpXdmi request TCP
- [ ] PROTOCOL-RPC portmap espd request TCP
- [ ] PROTOCOL-RPC portmap listing TCP 111
- [ ] PROTOCOL-RPC portmap listing TCP 32771
- [ ] PROTOCOL-SERVICES rlogin LinuxNIS
- [ ] PROTOCOL-SERVICES rlogin bin
- [ ] PROTOCOL-SERVICES rlogin echo++
- [ ] PROTOCOL-SERVICES Unix rlogin froot parameter root access attempt
- [ ] PROTOCOL-SERVICES rlogin login failure
- [ ] PROTOCOL-SERVICES rlogin root
- [ ] PROTOCOL-SERVICES rsh bin
- [ ] PROTOCOL-SERVICES rsh echo + +
- [ ] PROTOCOL-SERVICES rsh froot
- [ ] PROTOCOL-SERVICES rsh root
- [ ] PROTOCOL-SERVICES rlogin login failure
- [ ] PROTOCOL-RPC rusers query UDP
- [ ] INDICATOR-SCAN myscan
- [ ] MALWARE-BACKDOOR hack-a-tack attempt
- [ ] INDICATOR-SCAN ident version request
- [ ] INDICATOR-SCAN cybercop os probe
- [ ] INDICATOR-SCAN ipEye SYN scan
- [ ] INDICATOR-SCAN cybercop os PA12 attempt
- [ ] INDICATOR-SCAN cybercop os SFU12 probe
- [ ] INDICATOR-SCAN synscan portscan
- [ ] SERVER-MAIL ehlo cybercop attempt
- [ ] SERVER-MAIL expn cybercop attempt
- [ ] INDICATOR-SCAN Amanda client-version request
- [ ] INDICATOR-SCAN XTACACS logout
- [ ] INDICATOR-SCAN cybercop udp bomb
- [ ] INDICATOR-SCAN Webtrends Scanner UDP Probe
- [ ] INDICATOR-SHELLCODE SGI NOOP
- [ ] INDICATOR-SHELLCODE SGI NOOP
- [ ] INDICATOR-SHELLCODE AIX NOOP

- ☐ INDICATOR-SHELLCODE Digital UNIX NOOP
- ☐ INDICATOR-SHELLCODE HP-UX NOOP
- ☐ INDICATOR-SHELLCODE sparc NOOP
- ☐ INDICATOR-SHELLCODE Oracle sparc setuid 0
- ☐ INDICATOR-SHELLCODE x86 setgid 0
- ☐ INDICATOR-SHELLCODE Linux shellcode
- ☐ SERVER-MAIL Sendmail 8.6.9 exploit
- ☐ SERVER-MAIL Microsoft Windows Exchange Server 5.5 mime DOS
- ☐ SERVER-MAIL expn root
- ☐ SERVER-MAIL Sendmail 5.5.5 exploit
- ☐ SERVER-MAIL Sendmail RCPT TO decode attempt
- ☐ SERVER-MAIL Sendmail 8.6.10 exploit
- ☐ SERVER-MAIL Sendmail 8.6.9 exploit
- ☐ SERVER-MAIL Sendmail 8.6.9c exploit
- ☐ SQL sp_start_job - program execution
- ☐ SQL sp_password password change
- ☐ SQL sp_adduser database user creation
- ☐ SQL sp_password - password change
- ☐ SQL sp_adduser - database user creation
- ☐ SQL xp_cmdshell - program execution
- ☐ SERVER-MSSQL xp_reg* registry access
- ☐ INDICATOR-SHELLCODE shellcode attempt
- ☐ INDICATOR-SHELLCODE shellcode attempt
- ☐ SERVER-MSSQL xp_sprintf possible buffer overflow
- ☐ PROTOCOL-TELNET EZsetup account attempt
- ☐ PROTOCOL-TELNET ld_library_path
- ☐ PROTOCOL-TELNET resolv_host_conf
- ☐ PROTOCOL-TELNET not on console
- ☐ PROTOCOL-TELNET root login
- ☐ SERVER-WEBAPP SWSoft ASPSeek Overflow attempt
- ☐ SERVER-WEBAPP yabb directory traversal attempt
- ☐ SERVER-WEBAPP webdriver access
- ☐ SERVER-WEBAPP whois_raw.cgi access
- ☐ SERVER-WEBAPP webplus version access
- ☐ SERVER-WEBAPP websendmail access
- ☐ SERVER-WEBAPP dcforum.cgi access
- ☐ SERVER-WEBAPP anaconda directory traversal attempt
- ☐ SERVER-WEBAPP cvsweb.cgi access
- ☐ SERVER-WEBAPP glimpse access
- ☐ SERVER-WEBAPP info2www access
- ☐ SERVER-WEBAPP nph-test-cgi access
- ☐ SERVER-WEBAPP rguest.exe access
- ☐ SERVER-WEBAPP test-cgi access
- ☐ SERVER-WEBAPP uploader.exe access
- ☐ SERVER-WEBAPP finger access
- ☐ SERVER-WEBAPP aglimpse access
- ☐ SERVER-WEBAPP args.bat access
- ☐ SERVER-WEBAPP bnbform.cgi access
- ☐ SERVER-WEBAPP view-source directory traversal
- ☐ SERVER-WEBAPP wais.pl access
- ☐ SERVER-WEBAPP wguest.exe access
- ☐ SERVER-WEBAPP classifieds.cgi access
- ☐ SERVER-WEBAPP faxsurvey access
- ☐ SERVER-WEBAPP man.sh access
- ☐ SERVER-WEBAPP w3-msql access
- ☐ SERVER-WEBAPP day5datacopier.cgi access
- ☐ SERVER-WEBAPP ksh access
- ☐ SERVER-WEBAPP visadmin.exe access
- ☐ SERVER-WEBAPP dumpenv.pl access
- ☐ SERVER-WEBAPP survey.cgi access
- ☐ SERVER-WEBAPP win-c-sample.exe access
- ☐ SERVER-WEBAPP w3tvars.pm access
- ☐ SERVER-WEBAPP LWGate access
- ☐ SERVER-WEBAPP calendar access
- ☐ INDICATOR-SHELLCODE HP-UX NOOP
- ☐ INDICATOR-SHELLCODE sparc NOOP
- ☐ INDICATOR-SHELLCODE sparc NOOP
- ☐ INDICATOR-SHELLCODE x86 NOOP
- ☐ INDICATOR-SHELLCODE x86 setuid 0
- ☐ SERVER-MAIL RCPT TO overflow
- ☐ SERVER-MAIL Netmanager chameleon SMTPd buffer overflow attempt
- ☐ SERVER-MAIL Sendmail expn decode
- ☐ SERVER-MAIL Majordomo ifs
- ☐ SERVER-MAIL Sendmail rcpt to command attempt
- ☐ SERVER-MAIL Sendmail 5.6.5 exploit
- ☐ SERVER-MAIL Sendmail 8.6.10 exploit
- ☐ SERVER-MAIL Sendmail 8.6.9 exploit
- ☐ SERVER-MAIL vrfy decode
- ☐ SQL sp_start_job - program execution
- ☐ SQL sp_delete_alert log file deletion
- ☐ SQL xp_cmdshell program execution
- ☐ SQL sp_delete_alert log file deletion
- ☐ SERVER-MSSQL xp_reg* - registry access
- ☐ SQL sa login failed
- ☐ INDICATOR-SHELLCODE shellcode attempt
- ☐ INDICATOR-SHELLCODE shellcode attempt
- ☐ SERVER-MSSQL xp_sprintf possible buffer overflow
- ☐ PROTOCOL-TELNET 4Dgifts SGI account attempt
- ☐ PROTOCOL-TELNET SGI telnetd format bug
- ☐ PROTOCOL-TELNET livingston DOS
- ☐ PROTOCOL-TELNET Attempted SU from wrong group
- ☐ PROTOCOL-TELNET login incorrect
- ☐ SERVER-WEBAPP HyperSeek hsx.cgi directory traversal attempt
- ☐ SERVER-WEBAPP Progress webspeed access
- ☐ SERVER-WEBAPP /wwwboard/passwd.txt access
- ☐ SERVER-WEBAPP whois_raw.cgi arbitrary command execution attempt
- ☐ SERVER-WEBAPP websitepro path access
- ☐ SERVER-WEBAPP webplus directory traversal
- ☐ SERVER-WEBAPP dcboard.cgi invalid user addition attempt
- ☐ SERVER-WEBAPP mmstdod.cgi access
- ☐ SERVER-WEBAPP imagemap.exe overflow attempt
- ☐ SERVER-WEBAPP php.cgi access
- ☐ SERVER-WEBAPP htmlscript access
- ☐ SERVER-WEBAPP maillist.pl access
- ☐ SERVER-WEBAPP perl.exe access
- ☐ SERVER-WEBAPP rwwwshell.pl access
- ☐ SERVER-WEBAPP textcounter.pl access
- ☐ SERVER-WEBAPP webgais access
- ☐ SERVER-WEBAPP perlshop.cgi access
- ☐ SERVER-WEBAPP anform2 access
- ☐ SERVER-WEBAPP AT-admin.cgi access
- ☐ SERVER-WEBAPP campas access
- ☐ SERVER-WEBAPP view-source access
- ☐ SERVER-WEBAPP files.pl access
- ☐ SERVER-WEBAPP wrap access
- ☐ SERVER-WEBAPP environ.cgi access
- ☐ SERVER-WEBAPP filemail access
- ☐ SERVER-WEBAPP snork.bat access
- ☐ SERVER-WEBAPP csh access
- ☐ SERVER-WEBAPP day5datanotifier.cgi access
- ☐ SERVER-WEBAPP post-query access
- ☐ SERVER-WEBAPP rsh access
- ☐ SERVER-WEBAPP snorkerz.cmd access
- ☐ SERVER-WEBAPP tcsh access
- ☐ SERVER-WEBAPP rksh access
- ☐ SERVER-WEBAPP admin.pl access
- ☐ SERVER-WEBAPP archie access
- ☐ SERVER-WEBAPP flexform access

- SERVER-WEBAPP bash access
- SERVER-WEBAPP www-sql access
- SERVER-WEBAPP ppdscgi.exe access
- SERVER-WEBAPP upload.pl access
- SERVER-WEBAPP bb-hist.sh access
- SERVER-WEBAPP way-board access
- SERVER-WEBAPP commerce.cgi access
- SERVER-WEBAPP webspirs.cgi directory traversal attempt
- SERVER-WEBAPP tstisapi.dll access
- SERVER-OTHER Adobe Coldfusion exampleapp application.cfm
- SERVER-OTHER Adobe Coldfusion getfile.cfm access
- SERVER-OTHER Adobe Coldfusion administrator access
- SERVER-OTHER Adobe Coldfusion fileexists.cfm access
- SERVER-OTHER Adobe Coldfusion parks access
- SERVER-OTHER Adobe Coldfusion beaninfo access
- SERVER-OTHER Adobe Coldfusion getodbcdsn access
- SERVER-OTHER Adobe Coldfusion expeval access
- SERVER-OTHER Adobe Coldfusion datasource attempt
- SERVER-OTHER Adobe Coldfusion displayfile access
- SERVER-OTHER Adobe Coldfusion admin decrypt attempt
- SERVER-OTHER Adobe Coldfusion set odbc ini attempt
- SERVER-OTHER Adobe Coldfusion exampleapp access
- SERVER-OTHER Adobe Coldfusion snippets attempt
- SERVER-OTHER Adobe Coldfusion application.cfm access
- SERVER-OTHER Adobe Coldfusion startstop DOS access
- SERVER-OTHER Microsoft Frontpage _vti_rpc access
- SERVER-OTHER Microsoft Frontpage shtml.dll access
- SERVER-OTHER Microsoft Frontpage orders.htm access
- SERVER-OTHER Microsoft Frontpage fpremadm.exe access
- SERVER-OTHER Microsoft Frontpage fpadmcgi.exe access
- SERVER-OTHER Microsoft Frontpage form_results access
- SERVER-OTHER Microsoft Frontpage cfgwiz.exe access
- SERVER-OTHER Microsoft Frontpage author.exe access
- SERVER-OTHER Microsoft Frontpage form_results.htm access
- SERVER-OTHER Microsoft Frontpage register.txt access
- SERVER-OTHER Microsoft Frontpage service.cnf access
- SERVER-OTHER Microsoft Frontpage service.stp access
- SERVER-OTHER Microsoft Frontpage shtml.exe access
- SERVER-OTHER Microsoft Frontpage users.pwd access
- SERVER-OTHER Microsoft Frontpage .... request
- SERVER-OTHER Microsoft Frontpage register.htm access
- SERVER-IIS ISAPI .printer access
- SERVER-IIS Microsoft Windows IIS directory traversal attempt
- SERVER-WEBAPP .bat? access
- SERVER-IIS ASP contents view
- SERVER-IIS CGImail.exe access
- SERVER-IIS JET VBA access
- FILE-IDENTIFY .htr access file download request
- SERVER-OTHER Microsoft Frontpage _vti_inf.html access
- SERVER-IIS adctest.asp access
- SERVER-IIS /scripts/iisadmin/default.htm access
- SERVER-IIS anot.htr access
- SERVER-IIS asp-srch attempt
- SERVER-IIS bdir.htr access
- SERVER-IIS cmd.exe access
- SERVER-IIS codebrowser Exair access
- SERVER-IIS Form_JScript.asp access
- SERVER-IIS directory listing
- SERVER-IIS exec-src access
- SERVER-IIS fpcount access
- SERVER-IIS global.asa access
- SERVER-IIS iisadmpwd attempt
- SERVER-IIS isc$data attempt
- SERVER-IIS jet vba access
- SERVER-WEBAPP phf access
- SERVER-WEBAPP wwwadmin.pl access
- SERVER-WEBAPP sendform.cgi access
- SERVER-WEBAPP AnyForm2 access
- SERVER-WEBAPP redirect access
- SERVER-WEBAPP pals-cgi access
- SERVER-WEBAPP Amaya templates sendtemp.pl directory traversal attempt
- SERVER-WEBAPP webspirs.cgi access
- SERVER-OTHER Adobe Coldfusion cfcache.map access
- SERVER-OTHER Adobe Coldfusion application.cfm access
- SERVER-OTHER Adobe Coldfusion addcontent.cfm access
- SERVER-OTHER Adobe Coldfusion datasource username attempt
- SERVER-OTHER Adobe Coldfusion exprcalc access
- SERVER-OTHER Adobe Coldfusion cfappman access
- SERVER-OTHER Adobe Coldfusion evaluate.cfm access
- SERVER-OTHER Adobe Coldfusion db connections flush attempt
- SERVER-OTHER Adobe Coldfusion datasource passwordattempt
- SERVER-OTHER Adobe Coldfusion admin encrypt attempt
- SERVER-OTHER Adobe Coldfusion getodbcin attempt
- SERVER-OTHER Adobe Coldfusion mainframeset access
- SERVER-OTHER Adobe Coldfusion settings refresh attempt
- SERVER-OTHER Adobe Coldfusion CFUSION_VERIFYMAIL access
- SERVER-OTHER Adobe Coldfusion cfmlsyntaxcheck.cfm access
- SERVER-OTHER Adobe Coldfusion onrequestend.cfm access
- SERVER-OTHER Adobe Coldfusion gettempdirectory.cfm access
- SERVER-OTHER Microsoft Frontpage posting
- SERVER-OTHER Microsoft Frontpage contents.htm access
- SERVER-OTHER Microsoft Frontpage fpsrvadm.exe access
- SERVER-OTHER Microsoft Frontpage fpadmin.htm access
- SERVER-OTHER Microsoft Frontpage orders.txt access
- SERVER-OTHER Microsoft Frontpage registrations.htm access
- SERVER-OTHER Microsoft Frontpage authors.pwd access
- SERVER-OTHER Microsoft Frontpage administrators.pwd access
- SERVER-OTHER Microsoft Frontpage access.cnf access
- SERVER-OTHER Microsoft Frontpage registrations.txt access
- SERVER-OTHER Microsoft Frontpage service.pwd
- SERVER-OTHER Microsoft Frontpage services.cnf access
- SERVER-OTHER Microsoft Frontpage svcacl.cnf access
- SERVER-OTHER Microsoft Frontpage writeto.cnf access
- SERVER-OTHER Microsoft Frontpage dvwssr.dll access
- SERVER-IIS WebDAV file lock attempt
- SERVER-IIS *.idc attempt
- SERVER-IIS Alternate Data streams ASP file access attempt
- SERVER-IIS .cnf access
- SERVER-IIS ASP contents view
- SERVER-IIS JET VBA access
- SERVER-IIS MSProxy access
- MALWARE-CNC sensepost.exe command shell
- SERVER-IIS achg.htr access
- SERVER-IIS iisadmin access
- SERVER-IIS ism.dll access
- SERVER-IIS asp-dot attempt
- SERVER-IIS bdir access
- SERVER-WEBAPP carbo.dll access
- SERVER-IIS cmd? access
- SERVER-IIS codebrowser SDK access
- SERVER-IIS del attempt
- SERVER-IIS encoding access
- SERVER-IIS fpcount attempt
- SERVER-IIS getdrvs.exe access
- SERVER-IIS idc-srch attempt
- SERVER-IIS Malformed Hit-Highlighting Argument File Access Attempt
- SERVER-IIS ism.dll attempt
- SERVER-IIS msadcs.dll access

- SERVER-IIS newdsn.exe access
- SERVER-IIS perl access
- SERVER-IIS perl-browse newline attempt
- SERVER-IIS perl-browse space attempt
- SERVER-IIS query.asp access
- SERVER-IIS scripts-browse access
- SERVER-IIS search97.vts access
- SERVER-IIS /SiteServer/Publishing/viewcode.asp access
- SERVER-IIS showcode access
- SERVER-IIS viewcode access
- SERVER-IIS viewcode access
- SERVER-IIS viewcode access
- SERVER-IIS viewcode access
- SERVER-IIS showcode.asp access
- SERVER-IIS site server config access
- SERVER-IIS srch.htm access
- SERVER-IIS srchadm access
- SERVER-IIS uploadn.asp access
- SERVER-IIS view source via translate header
- SERVER-IIS viewcode.asp access
- SERVER-IIS webhits access
- SERVER-IIS Unauthorized IP Access Attempt
- SERVER-IIS site/iisamples access
- SERVER-WEBAPP Netscape Enterprise DOS
- SERVER-WEBAPP Netscape Enterprise directory listing attempt
- SERVER-WEBAPP iPlanet GETPROPERTIES attempt
- FILE-OTHER technote main.cgi file directory traversal attempt
- SERVER-WEBAPP technote print.cgi directory traversal attempt
- SERVER-WEBAPP ads.cgi command execution attempt
- SERVER-WEBAPP weblogic/tomcat .jsp view source attempt
- SERVER-APACHE Apache Tomcat view source attempt
- SQL ftp attempt
- SQL xp_enumdsn attempt
- SQL xp_filelist attempt
- SQL xp_availablemedia attempt
- SQL xp_cmdshell attempt
- SERVER-WEBAPP nc.exe attempt
- SERVER-WEBAPP wsh attempt
- SERVER-WEBAPP rcmd attempt
- SERVER-WEBAPP telnet attempt
- SERVER-WEBAPP net attempt
- SERVER-WEBAPP tftp attempt
- SQL xp_regread attempt
- SERVER-WEBAPP WebDAV search access
- SERVER-WEBAPP .htpasswd access attempt
- SERVER-WEBAPP Lotus Domino directory traversal
- SERVER-WEBAPP webhits.exe access
- SERVER-IIS postinfo.asp access
- SERVER-IIS repost.asp access
- SQL queryhit.htm access
- SQL counter.exe access
- OS-WINDOWS Microsoft Windows WebDAV propfind access
- SERVER-WEBAPP unify eWave ServletExec upload
- SERVER-WEBAPP Netscape Servers suite DOS
- SERVER-WEBAPP amazon 1-click cookie theft
- SERVER-WEBAPP unify eWave ServletExec DOS
- SERVER-WEBAPP Allaire JRUN DOS attempt
- SERVER-WEBAPP strings overflow
- SERVER-WEBAPP strings overflow
- SERVER-WEBAPP eXtropia webstore directory traversal
- SERVER-WEBAPP shopping cart directory traversal
- SERVER-WEBAPP Allaire Pro Web Shell attempt
- SERVER-WEBAPP ICQ Webfront HTTP DOS
- SERVER-WEBAPP Armada Style Master Index directory traversal
- SERVER-WEBAPP cached_feed.cgi moreover shopping cart directory traversal
- SERVER-WEBAPP Talentsoft Web+ Source Code view access
- SERVER-WEBAPP Talentsoft Web+ internal IP Address access
- SERVER-WEBAPP Talentsoft Web+ exploit attempt
- SERVER-WEBAPP SmartWin CyberOffice Shopping Cart access
- SERVER-WEBAPP cybercop scan
- INDICATOR-SCAN L3retriever HTTP Probe
- INDICATOR-SCAN Webtrends HTTP probe
- SERVER-WEBAPP nessus 1.X 404 probe
- SERVER-WEBAPP Netscape admin passwd
- SERVER-WEBAPP BigBrother access
- SERVER-WEBAPP Poll-it access
- SERVER-WEBAPP ftp.pl access
- SERVER-APACHE Apache Tomcat server snoop access
- SERVER-WEBAPP ROXEN directory list attempt
- SERVER-WEBAPP apache source.asp file access
- SERVER-APACHE Apache Tomcat server exploit access
- SERVER-WEBAPP ICQ webserver DOS
- SERVER-WEBAPP Lotus DelDoc attempt
- SERVER-WEBAPP Lotus EditDoc attempt
- SERVER-WEBAPP ls 20-l
- SERVER-WEBAPP mlog.phtml access
- SERVER-WEBAPP mylog.phtml access
- SERVER-WEBAPP /etc/passwd file access attempt
- SERVER-WEBAPP ?PageServices access
- SERVER-WEBAPP Ecommerce check.txt access
- SERVER-WEBAPP webcart access
- SERVER-WEBAPP AuthChangeUrl access
- SERVER-WEBAPP convert.bas access
- SERVER-WEBAPP cpshost.dll access
- SERVER-WEBAPP .htaccess access
- SERVER-WEBAPP .wwwacl access
- SERVER-WEBAPP .wwwacl access
- SERVER-WEBAPP Netscape Unixware overflow
- INDICATOR-SCAN cybercop os probe
- SERVER-WEBAPP Phorum admin access
- SERVER-WEBAPP cd..
- SERVER-WEBAPP Phorum authentication access
- SERVER-WEBAPP whisker HEAD/./
- SERVER-WEBAPP guestbook.pl access
- SERVER-WEBAPP handler access
- SERVER-WEBAPP /.... access
- SERVER-WEBAPP root access
- SERVER-WEBAPP Ecommerce import.txt access
- SERVER-WEBAPP cat_ access
- SERVER-WEBAPP Ecommerce import.txt access
- SERVER-WEBAPP count.cgi access
- SERVER-WEBAPP Domino catalog.nsf access
- SERVER-WEBAPP Domino domcfg.nsf access
- SERVER-WEBAPP Domino domlog.nsf access
- SERVER-WEBAPP Domino log.nsf access
- SERVER-WEBAPP Domino names.nsf access
- SERVER-WEBAPP Ecommerce checks.txt access
- SERVER-WEBAPP apache directory disclosure attempt
- SERVER-WEBAPP Netscape PublishingXpert access
- SERVER-WEBAPP windmail.exe access
- SERVER-WEBAPP webplus access
- SERVER-WEBAPP Netscape dir index wp
- SERVER-WEBAPP piranha passwd.php3 access
- SERVER-WEBAPP cart 32 AdminPwd access
- SERVER-WEBAPP webdist.cgi access
- SERVER-WEBAPP shopping cart access
- SERVER-WEBAPP Novell Groupwise gwweb.exe access
- SERVER-WEBAPP ws_ftp.ini access

- SERVER-WEBAPP rpm_query access
- SERVER-WEBAPP bigconf.cgi access
- SERVER-WEBAPP /cgi-bin/jj access
- SERVER-WEBAPP Netscape Enterprise Server directory view
- SERVER-WEBAPP Phorum violation access
- SERVER-WEBAPP Annex Terminal DOS attempt
- SERVER-WEBAPP Netscape Enterprise Server directory view
- SERVER-WEBAPP Netscape Enterprise Server directory view
- SERVER-WEBAPP Netscape Enterprise Server directory view
- SERVER-WEBAPP Netscape Enterprise Server directory view
- SERVER-WEBAPP Trend Micro OfficeScan access
- SERVER-WEBAPP sojourn.cgi File attempt
- SERVER-WEBAPP SGI InfoSearch fname attempt
- SERVER-WEBAPP Netscape Enterprise Server directory view
- INDICATOR-COMPROMISE Invalid URL
- SERVER-WEBAPP search.vts access
- SERVER-WEBAPP axs.cgi access
- SERVER-WEBAPP htgrep access
- SERVER-WEBAPP .nsconfig access
- SERVER-WEBAPP Admin_files access
- SERVER-WEBAPP intranet access
- SERVER-WEBAPP filemail access
- SERVER-WEBAPP adminlogin access
- SERVER-WEBAPP ultraboard access
- SERVER-WEBAPP pals-cgi arbitrary file access attempt
- X11 MIT Magic Cookie detected
- PROTOCOL-FTP CWD ...
- SERVER-WEBAPP VirusWall catinfo access
- SERVER-WEBAPP VirusWall FtpSaveCSP access
- OS-WINDOWS RFParalyze Attempt
- SERVER-WEBAPP SWEditServlet directory traversal attempt
- SERVER-IIS ISAPI .ida attempt
- SERVER-IIS ISAPI .idq access
- SERVER-OTHER Microsoft Frontpage rad fp4areg.dll access
- PROTOCOL-TELNET bsd telnet exploit response
- SERVER-WEBAPP PHPLIB remote command attempt
- SERVER-IIS CodeRed v2 root.exe access
- SERVER-WEBAPP SWEditServlet access
- PROTOCOL-RPC portmap admind request TCP
- PROTOCOL-RPC portmap bootparam request TCP
- PROTOCOL-RPC portmap nisd request TCP
- PROTOCOL-RPC portmap rexd request TCP
- PROTOCOL-RPC portmap rusers request TCP
- PROTOCOL-RPC portmap selection_svc request TCP
- PROTOCOL-RPC portmap yppasswd request TCP
- PROTOCOL-RPC portmap ypupdated request UDP
- PROTOCOL-RPC portmap listing UDP 111
- SERVER-IIS Microsoft Office Outlook web dos
- SERVER-IIS msdac access
- SERVER-OTHER Microsoft Frontpage /_vti_bin/ access
- FILE-OTHER readme.eml autoload attempt
- INDICATOR-COMPROMISE directory listing
- SERVER-WEBAPP admin.php file upload attempt
- SERVER-WEBAPP console.exe access
- SERVER-WEBAPP txt2html.cgi access
- SERVER-WEBAPP store.cgi access
- SERVER-WEBAPP zsh access
- INDICATOR-SHELLCODE ssh CRC32 overflow /bin/sh
- INDICATOR-SHELLCODE ssh CRC32 overflow NOOP
- SERVER-WEBAPP .htgroup access
- SERVER-WEBAPP jrun directory browse attempt
- PROTOCOL-FTP wu-ftp bad file completion attempt
- SERVER-IIS Form_VBScript.asp access
- SERVER-OTHER CHAT IRC Ettercap parse overflow attempt
- SERVER-WEBAPP mod-plsql administration access
- SERVER-WEBAPP mall log order access
- SERVER-WEBAPP architext_query.pl access
- SERVER-WEBAPP wwwboard.pl access
- SERVER-WEBAPP Phorum read access
- SERVER-WEBAPP get32.exe access
- SERVER-WEBAPP Netscape Enterprise Server directory view
- SERVER-WEBAPP bizdbsearch attempt
- SERVER-WEBAPP SalesLogix Eviewer web command attempt
- SERVER-WEBAPP Netscape Enterprise Server directory view
- SERVER-WEBAPP Netscape Enterprise Server directory view
- SERVER-WEBAPP oracle web arbitrary command execution attempt
- SERVER-WEBAPP sojourn.cgi access
- SERVER-WEBAPP Phorum code access
- SERVER-WEBAPP Compaq Insight directory traversal
- INDICATOR-COMPROMISE 403 Forbidden
- SERVER-WEBAPP ax-admin.cgi access
- SERVER-WEBAPP cachemgr.cgi access
- SERVER-WEBAPP responder.cgi access
- SERVER-WEBAPP web-map.cgi access
- SERVER-WEBAPP backup access
- SERVER-WEBAPP ministats admin access
- SERVER-WEBAPP plusmail access
- SERVER-WEBAPP dfire.cgi access
- SERVER-WEBAPP Muscat Empower cgi access
- SERVER-WEBAPP ROADS search.pl attempt
- X11 xopen
- SERVER-WEBAPP VirusWall FtpSave access
- SERVER-WEBAPP VirusWall catinfo access
- SERVER-WEBAPP VirusWall FtpSaveCVP access
- SERVER-OTHER MDBMS overflow
- SERVER-IIS ISAPI .ida access
- SERVER-IIS ISAPI .idq attempt
- SERVER-OTHER Microsoft Frontpage rad fp30reg.dll access
- OS-OTHER Cisco IOS HTTP configuration attempt
- PROTOCOL-TELNET bsd exploit client finishing
- SERVER-WEBAPP PHPLIB remote command attempt
- SERVER-OTHER Winnuke attack
- SERVER-OTHER AIX pdnsd overflow
- PROTOCOL-RPC portmap amountd request TCP
- PROTOCOL-RPC portmap cmsd request TCP
- PROTOCOL-RPC portmap pcnfsd request TCP
- PROTOCOL-RPC portmap rstatd request TCP
- PROTOCOL-RPC portmap sadmind request TCP
- PROTOCOL-RPC portmap ttdbserv request TCP
- PROTOCOL-RPC portmap ypserv request TCP
- PROTOCOL-RPC portmap snmpXdmi request UDP
- PROTOCOL-RPC portmap listing UDP 32771
- SERVER-OTHER readme.eml download attempt
- SERVER-IIS _mem_bin access
- PROTOCOL-TFTP GET Admin.dll
- SERVER-WEBAPP sml3com access
- INDICATOR-COMPROMISE nimda RICHED20.DLL
- SERVER-WEBAPP admin.php access
- SERVER-WEBAPP cs.exe access
- SERVER-WEBAPP txt2html.cgi directory traversal attempt
- SERVER-WEBAPP sendmessage.cgi access
- SERVER-OTHER rwhoisd format string attempt
- INDICATOR-SHELLCODE ssh CRC32 overflow filler
- INDICATOR-SHELLCODE ssh CRC32 overflow
- SERVER-WEBAPP sadmind worm access
- PROTOCOL-FTP wu-ftp bad file completion attempt
- PROTOCOL-FTP STAT overflow attempt
- SERVER-WEBAPP Trend Micro OfficeScan attempt
- OS-WINDOWS Microsoft Windows UPnP malformed advertisement
- SERVER-MSSQL raiserror possible buffer overflow

- [ ] SQL raiserror possible buffer overflow
- [ ] INDICATOR-SHELLCODE x86 inc ebx NOOP
- [ ] INDICATOR-SHELLCODE x86 inc ecx NOOP
- [ ] SERVER-WEBAPP zml.cgi access
- [ ] SERVER-OTHER CDE dtspcd exploit attempt
- [ ] SERVER-IIS /scripts/samples/ access
- [ ] SERVER-IIS iissamples access
- [ ] SERVER-WEBAPP agora.cgi access
- [ ] SERVER-OTHER MSDTC attempt
- [ ] SERVER-WEBAPP dcboard.cgi access
- [ ] PROTOCOL-SNMP public access tcp
- [ ] PROTOCOL-SNMP private access tcp
- [ ] PROTOCOL-SNMP broadcast trap
- [ ] PROTOCOL-SNMP request tcp
- [ ] PROTOCOL-SNMP trap tcp
- [ ] PROTOCOL-SNMP community string buffer overflow attempt with evasion
- [ ] SERVER-WEBAPP content-disposition file upload attempt
- [ ] PROTOCOL-SNMP PROTOS test-suite-trap-app attempt
- [ ] PUA-P2P GNUTella client request
- [ ] SERVER-WEBAPP .bash_history access
- [ ] POLICY-MULTIMEDIA Apple Quicktime User Agent access
- [ ] POLICY-MULTIMEDIA Shoutcast playlist redirection
- [ ] PROTOCOL-TFTP GET nc.exe
- [ ] PROTOCOL-TFTP GET passwd
- [ ] INDICATOR-COMPROMISE FTP file_id.diz access possible warez site
- [ ] POLICY-OTHER Microsoft Windows Terminal server RDP attempt
- [ ] SERVER-MAIL Vintra Mailserver expn *@
- [ ] SERVER-WEBAPP args.cmd access
- [ ] SERVER-WEBAPP wwwwais access
- [ ] SERVER-WEBAPP calender_admin.pl access
- [ ] SERVER-WEBAPP user_update_passwd.pl access
- [ ] SERVER-WEBAPP bb-histsvc.sh access
- [ ] SERVER-WEBAPP bb-replog.sh access
- [ ] INDICATOR-COMPROMISE oracle one hour install
- [ ] SERVER-WEBAPP cgiforum.pl access
- [ ] SERVER-WEBAPP Web Shopper shopper.cgi attempt
- [ ] SERVER-WEBAPP listrec.pl access
- [ ] SERVER-WEBAPP book.cgi access
- [ ] SERVER-WEBAPP cal_make.pl access
- [ ] SERVER-WEBAPP sdbsearch.cgi access
- [ ] SERVER-WEBAPP ttawebtop.cgi arbitrary file attempt
- [ ] SERVER-WEBAPP upload.cgi access
- [ ] SERVER-WEBAPP ustorekeeper.pl access
- [ ] SERVER-IIS ctss.idc access
- [ ] SERVER-WEBAPP store.cgi directory traversal attempt
- [ ] SERVER-WEBAPP Phorum /support/common.php attempt
- [ ] SERVER-WEBAPP RBS ISP /newuser directory traversal attempt
- [ ] SERVER-WEBAPP SIX webboard generate.cgi attempt
- [ ] SERVER-WEBAPP spin_client.cgi access
- [ ] SERVER-WEBAPP ExAir access
- [ ] SERVER-WEBAPP a1stats a1disp3.cgi access
- [ ] POLICY-OTHER AFS access
- [ ] SERVER-WEBAPP alchemy http server NUL arbitrary command execution attempt
- [ ] SERVER-WEBAPP alibaba.pl access
- [ ] SERVER-WEBAPP test.bat arbitrary command execution attempt
- [ ] SERVER-WEBAPP input.bat arbitrary command execution attempt
- [ ] SERVER-WEBAPP input2.bat arbitrary command execution attempt
- [ ] SERVER-WEBAPP envout.bat arbitrary command execution attempt
- [ ] SERVER-WEBAPP nstelemetry.adp access
- [ ] SERVER-WEBAPP server-info access
- [ ] SERVER-WEBAPP ans.pl attempt
- [ ] SERVER-WEBAPP Axis Storpoint CD attempt
- [ ] OS-WINDOWS Microsoft Windows UPnP Location overflow attempt
- [ ] SERVER-WEBAPP lastlines.cgi access
- [ ] SERVER-WEBAPP zml.cgi attempt
- [ ] SERVER-WEBAPP wayboard attempt
- [ ] SERVER-WEBAPP PHP-Nuke remote file include attempt
- [ ] SERVER-IIS /msadc/samples/ access
- [ ] SERVER-WEBAPP AHG search.cgi access
- [ ] SERVER-WEBAPP smssend.php access
- [ ] PROTOCOL-SNMP community string buffer overflow attempt
- [ ] PROTOCOL-SNMP public access udp
- [ ] PROTOCOL-SNMP private access udp
- [ ] PROTOCOL-SNMP Broadcast request
- [ ] PROTOCOL-SNMP request udp
- [ ] PROTOCOL-SNMP trap udp
- [ ] PROTOCOL-SNMP AgentX/tcp request
- [ ] SERVER-WEBAPP content-disposition memchr overflow
- [ ] PROTOCOL-SNMP PROTOS test-suite-req-app attempt
- [ ] POLICY-MULTIMEDIA audio galaxy keepalive
- [ ] SERVER-WEBAPP .history access
- [ ] PROTOCOL-DNS named authors attempt
- [ ] FILE-IDENTIFY Microsoft Windows Media download detected
- [ ] POLICY-MULTIMEDIA Icecast playlist redirection
- [ ] PROTOCOL-TFTP GET shadow
- [ ] PROTOCOL-TFTP Get
- [ ] SERVER-MAIL vrfy root
- [ ] POLICY-OTHER Microsoft Windows Terminal server request attempt
- [ ] SERVER-WEBAPP NPH-maillist access
- [ ] SERVER-WEBAPP AT-generated.cgi access
- [ ] SERVER-WEBAPP calendar.pl access
- [ ] SERVER-WEBAPP user_update_admin.pl access
- [ ] SERVER-WEBAPP bb-histlog.sh access
- [ ] SERVER-WEBAPP bb-rep.sh access
- [ ] POLICY-SOCIAL IRC message
- [ ] SERVER-WEBAPP auktion.cgi access
- [ ] SERVER-WEBAPP directorypro.cgi access
- [ ] SERVER-WEBAPP Web Shopper shopper.cgi access
- [ ] SERVER-WEBAPP mailnews.cgi access
- [ ] SERVER-WEBAPP newsdesk.cgi access
- [ ] SERVER-WEBAPP mailit.pl access
- [ ] SERVER-WEBAPP Simple Web Counter URI Parameter Buffer Overflow attempt
- [ ] SERVER-WEBAPP ttawebtop.cgi access
- [ ] SERVER-WEBAPP view_source access
- [ ] SERVER-IIS mkilog.exe access
- [ ] SERVER-IIS /iisadmpwd/aexp2.htr access
- [ ] SERVER-WEBAPP nobody access
- [ ] SERVER-WEBAPP Phorum /support/common.php access
- [ ] SERVER-WEBAPP RBS ISP /newuser access
- [ ] SERVER-WEBAPP SIX webboard generate.cgi access
- [ ] SERVER-WEBAPP SiteScope Service access
- [ ] SERVER-WEBAPP a1stats a1disp3.cgi directory traversal attempt
- [ ] SERVER-WEBAPP admentor admin.asp access
- [ ] SERVER-WEBAPP alchemy http server PRN arbitrary command execution attempt
- [ ] SERVER-WEBAPP alibaba.pl arbitrary command execution attempt
- [ ] SERVER-WEBAPP AltaVista Intranet Search directory traversal attempt
- [ ] SERVER-WEBAPP test.bat access
- [ ] SERVER-WEBAPP input.bat access
- [ ] SERVER-WEBAPP input2.bat access
- [ ] SERVER-WEBAPP envout.bat access
- [ ] SERVER-WEBAPP apache ?M=D directory list attempt
- [ ] SERVER-WEBAPP server-status access
- [ ] SERVER-WEBAPP ans.pl access
- [ ] SERVER-WEBAPP Axis Storpoint CD access

- ☐ SERVER-WEBAPP basilix sendmail.inc access
- ☐ SERVER-WEBAPP BBoard access
- ☐ SERVER-WEBAPP bb-hist.sh attempt
- ☐ SERVER-WEBAPP bb-hostscv.sh access
- ☐ SERVER-WEBAPP bizdbsearch access
- ☐ SERVER-WEBAPP calendar_admin.pl access
- ☐ SERVER-WEBAPP /cgi-bin/ls access
- ☐ PROTOCOL-FINGER version query
- ☐ SERVER-WEBAPP cgiwrap access
- ☐ SERVER-OTHER Cisco denial of service attempt
- ☐ SERVER-WEBAPP csSearch.cgi arbitrary command execution attempt
- ☐ SERVER-MAIL HELO overflow attempt
- ☐ SERVER-WEBAPP /CVS/Entries access
- ☐ SERVER-WEBAPP dbman db.cgi access
- ☐ SERVER-WEBAPP DCShop orders.txt access
- ☐ SERVER-WEBAPP Delegate whois overflow attempt
- ☐ SERVER-WEBAPP /doc/ access
- ☐ SERVER-WEBAPP login.htm attempt
- ☐ SERVER-WEBAPP eshop.pl arbitrary command execution attempt
- ☐ SERVER-IIS /exchange/root.asp attempt
- ☐ SERVER-WEBAPP loadpage.cgi directory traversal attempt
- ☐ SERVER-WEBAPP dcforum.cgi directory traversal attempt
- ☐ SERVER-WEBAPP cgiforum.pl attempt
- ☐ SERVER-WEBAPP Domino mab.nsf access
- ☐ SERVER-WEBAPP Domino setup.nsf access
- ☐ SERVER-WEBAPP Domino webadmin.nsf access
- ☐ SERVER-WEBAPP Domino ntsync4.nsf access
- ☐ SERVER-WEBAPP Domino mailw46.nsf access
- ☐ SERVER-WEBAPP Domino agentrunner.nsf access
- ☐ SERVER-WEBAPP cgitest.exe access
- ☐ SERVER-WEBAPP musicat empower attempt
- ☐ SERVER-WEBAPP faqmanager.cgi access
- ☐ SERVER-WEBAPP FormHandler.cgi external site redirection attempt
- ☐ SERVER-IIS htimage.exe access
- ☐ SERVER-WEBAPP Home Free search.cgi directory traversal attempt
- ☐ SERVER-WEBAPP htsearch arbitrary configuration file attempt
- ☐ SERVER-WEBAPP htsearch access
- ☐ SERVER-WEBAPP iChat directory traversal attempt
- ☐ SERVER-WEBAPP icat access
- ☐ SERVER-WEBAPP htmlscript attempt
- ☐ SERVER-WEBAPP eXtropia webstore access
- ☐ SERVER-WEBAPP handler attempt
- ☐ SERVER-WEBAPP htgrep attempt
- ☐ SERVER-WEBAPP Bugzilla doeditvotes.cgi access
- ☐ PROTOCOL-FTP CMD overflow attempt
- ☐ PROTOCOL-FTP invalid MODE
- ☐ PROTOCOL-FTP SYST overflow attempt
- ☐ SERVER-WEBAPP FormHandler.cgi directory traversal attempt
- ☐ PROTOCOL-POP APOP overflow attempt
- ☐ SERVER-WEBAPP yabb access
- ☐ POLICY-SOCIAL IRC DCC file transfer request
- ☐ SERVER-OTHER DB2 dos attempt
- ☐ SERVER-WEBAPP db2www access
- ☐ SERVER-WEBAPP testcgi access
- ☐ SERVER-WEBAPP perl.exe command attempt
- ☐ SERVER-WEBAPP tst.bat access
- ☐ SERVER-WEBAPP campas attempt
- ☐ SERVER-WEBAPP pfdispaly.cgi arbitrary command execution attempt
- ☐ SERVER-WEBAPP pagelog.cgi directory traversal attempt
- ☐ SERVER-OTHER Adobe Coldfusion sendmail.cfm access
- ☐ SERVER-IIS cmd32.exe access
- ☐ SERVER-WEBAPP *%20.pl access
- ☐ INDICATOR-COMPROMISE index of /cgi-bin/ response
- ☐ SERVER-WEBAPP basilix mysql.class access
- ☐ PROTOCOL-FTP SITE overflow attempt
- ☐ SERVER-WEBAPP bb-hostscv.sh attempt
- ☐ SERVER-WEBAPP agora.cgi attempt
- ☐ SERVER-WEBAPP calendar_admin.pl arbitrary command execution attempt
- ☐ PROTOCOL-NNTP AUTHINFO USER overflow attempt
- ☐ SERVER-OTHER Adobe Coldfusion ?Mode=debug attempt
- ☐ SERVER-WEBAPP cgimail access
- ☐ SERVER-WEBAPP Cisco Catalyst command execution attempt
- ☐ SERVER-WEBAPP Cisco HTTP double-percent DOS attempt
- ☐ SERVER-WEBAPP csSearch.cgi access
- ☐ SERVER-MAIL ETRN overflow attempt
- ☐ SERVER-WEBAPP cvsweb version access
- ☐ SERVER-WEBAPP DCShop access
- ☐ SERVER-WEBAPP DCShop auth_user_file.txt access
- ☐ SERVER-WEBAPP /doc/packages access
- ☐ PROTOCOL-FTP SITE CHOWN overflow attempt
- ☐ SERVER-WEBAPP login.htm access
- ☐ SERVER-WEBAPP eshop.pl access
- ☐ SERVER-IIS /exchange/root.asp access
- ☐ SERVER-WEBAPP loadpage.cgi access
- ☐ SERVER-WEBAPP commerce.cgi arbitrary file access attempt
- ☐ SERVER-WEBAPP directorypro.cgi attempt
- ☐ SERVER-WEBAPP Domino cersvr.nsf access
- ☐ SERVER-WEBAPP Domino statrep.nsf access
- ☐ SERVER-WEBAPP Domino events4.nsf access
- ☐ SERVER-WEBAPP Domino collect4.nsf access
- ☐ SERVER-WEBAPP Domino bookmark.nsf access
- ☐ SERVER-WEBAPP Domino mail.box access
- ☐ SERVER-WEBAPP SalesLogix Eviewer access
- ☐ SERVER-WEBAPP faqmanager.cgi arbitrary file access attempt
- ☐ SERVER-WEBAPP /fcgi-bin/echo.exe access
- ☐ SERVER-WEBAPP FormHandler.cgi access
- ☐ SERVER-WEBAPP guestbook.cgi access
- ☐ SERVER-WEBAPP search.cgi access
- ☐ SERVER-WEBAPP htsearch arbitrary file read attempt
- ☐ SERVER-WEBAPP DELETE attempt
- ☐ SERVER-OTHER iParty DOS attempt
- ☐ SERVER-WEBAPP HyperSeek hsx.cgi access
- ☐ SERVER-WEBAPP formmail arbitrary command execution attempt
- ☐ SERVER-WEBAPP ftp.pl attempt
- ☐ SERVER-WEBAPP Novell Groupwise gwweb.exe attempt
- ☐ PROTOCOL-DNS named version attempt
- ☐ SERVER-IIS .asp chunked Transfer-Encoding
- ☐ PROTOCOL-FTP RNFR ././ attempt
- ☐ PROTOCOL-FTP PWD overflow attempt
- ☐ SERVER-IIS /StoreCSVS/InstantOrder.asmx request
- ☐ PROTOCOL-POP PASS overflow attempt
- ☐ SERVER-OTHER Xtramail Username overflow attempt
- ☐ INDICATOR-SCAN SSH Version map attempt
- ☐ POLICY-SOCIAL IRC DCC chat request
- ☐ SERVER-WEBAPP document.d2w access
- ☐ SERVER-WEBAPP test-cgi attempt
- ☐ SERVER-WEBAPP test.cgi access
- ☐ SERVER-WEBAPP perl command attempt
- ☐ SERVER-WEBAPP environ.pl access
- ☐ SERVER-WEBAPP cart32.exe access
- ☐ SERVER-WEBAPP pfdispaly.cgi access
- ☐ SERVER-WEBAPP pagelog.cgi access
- ☐ SERVER-IIS trace.axd access
- ☐ SERVER-WEBAPP /~ftp access
- ☐ SERVER-WEBAPP mkplog.exe access
- ☐ SERVER-WEBAPP cross site scripting HTML Image tag set to javascript attempt

- SERVER-WEBAPP /cgi-bin/ access
- SERVER-WEBAPP /cgi-dos/ access
- SERVER-WEBAPP /home/ftp access
- SERVER-WEBAPP /home/www access
- PROTOCOL-FTP CWD ~ attempt
- SERVER-ORACLE EXECUTE_SYSTEM attempt
- SERVER-ORACLE connect_data remote version detection attempt
- SERVER-ORACLE misparsed login response
- SERVER-ORACLE select union attempt
- SERVER-ORACLE select like '%' attempt
- SERVER-ORACLE select like '%' attempt backslash escaped
- SERVER-ORACLE describe attempt
- SERVER-ORACLE all_constraints access
- SERVER-ORACLE all_views access
- SERVER-ORACLE all_source access
- SERVER-ORACLE all_tables access
- SERVER-ORACLE all_tab_columns access
- SERVER-ORACLE all_tab_privs access
- SERVER-ORACLE dba_tablespace access
- SERVER-ORACLE dba_tables access
- SERVER-ORACLE user_tablespace access
- SERVER-ORACLE sys.all_users access
- SERVER-ORACLE grant attempt
- SERVER-ORACLE ALTER USER attempt
- SERVER-ORACLE drop table attempt
- SERVER-ORACLE create table attempt
- SERVER-ORACLE alter table attempt
- SERVER-ORACLE truncate table attempt
- SERVER-ORACLE create database attempt
- SERVER-ORACLE alter database attempt
- SERVER-WEBAPP imagemap.exe access
- SERVER-WEBAPP calendar-admin.pl access
- SERVER-WEBAPP Amaya templates sendtemp.pl access
- SERVER-WEBAPP auktion.cgi directory traversal attempt
- SERVER-WEBAPP cal_make.pl directory traversal attempt
- SERVER-WEBAPP echo.bat arbitrary command execution attempt
- SERVER-WEBAPP echo.bat access
- SERVER-WEBAPP hello.bat arbitrary command execution attempt
- SERVER-WEBAPP hello.bat access
- SERVER-WEBAPP ad.cgi access
- SERVER-WEBAPP bbs_forum.cgi access
- SERVER-WEBAPP bsguest.cgi access
- SERVER-WEBAPP bslist.cgi access
- SERVER-WEBAPP cgforum.cgi access
- SERVER-WEBAPP newdesk access
- SERVER-WEBAPP register.cgi access
- SERVER-WEBAPP gbook.cgi access
- SERVER-WEBAPP simplestguest.cgi access
- SERVER-WEBAPP statsconfig.pl access
- SERVER-WEBAPP talkback.cgi directory traversal attempt
- SERVER-WEBAPP talkback.cgi access
- SERVER-WEBAPP adcycle access
- SERVER-WEBAPP MachineInfo access
- SERVER-WEBAPP emumail.cgi NULL attempt
- SERVER-WEBAPP emumail.cgi access
- SERVER-IIS +.htr code fragment attempt
- SERVER-IIS doctodep.btr access
- SERVER-WEBAPP SGI InfoSearch fname access
- POLICY-SOCIAL IRC channel join
- SERVER-WEBAPP ustorekeeper.pl directory traversal attempt
- SERVER-WEBAPP a1stats access
- PROTOCOL-RPC portmap rwalld request UDP
- PROTOCOL-RPC portmap rwalld request TCP
- PROTOCOL-FTP USER overflow attempt
- BROWSER-OTHER Mozilla Netscape XMLHttpRequest local file read attempt
- SERVER-WEBAPP squirrel mail spell-check arbitrary command attempt
- SERVER-WEBAPP squirrel mail theme arbitrary command attempt
- SERVER-WEBAPP global.inc access
- SERVER-WEBAPP DNSTools administrator authentication bypass attempt
- SERVER-WEBAPP DNSTools authentication bypass attempt
- SERVER-WEBAPP DNSTools access
- SERVER-WEBAPP Blahz-DNS dostuff.php modify user attempt
- SERVER-WEBAPP Blahz-DNS dostuff.php access
- SERVER-WEBAPP SecureSite authentication bypass attempt
- SERVER-WEBAPP Messagerie supp_membre.php access
- PROTOCOL-RPC portmap cachefsd request UDP
- PROTOCOL-RPC portmap cachefsd request TCP
- SERVER-IIS users.xml access
- SERVER-OTHER cachefsd buffer overflow attempt
- SERVER-IIS as_web.exe access
- SERVER-IIS as_web4.exe access
- PROTOCOL-IMAP partial body buffer overflow attempt
- SERVER-IIS NewsPro administration authentication attempt
- SERVER-WEBAPP b2 arbitrary command execution attempt
- SQL xp_cmdshell program execution 445
- SERVER-WEBAPP phf arbitrary command execution attempt
- SERVER-WEBAPP Nortel Contivity cgiproc DOS attempt
- SERVER-WEBAPP Nortel Contivity cgiproc DOS attempt
- SERVER-WEBAPP Nortel Contivity cgiproc access
- SERVER-WEBAPP search.dll directory listing attempt
- SERVER-WEBAPP search.dll access
- SERVER-WEBAPP .DS_Store access
- SERVER-WEBAPP .FBCIndex access
- POLICY-OTHER IPSec PGPNet connection attempt
- SERVER-IIS pbserver access
- SERVER-WEBAPP php.exe access
- SERVER-WEBAPP bb_smilies.php access
- SERVER-MYSQL root login attempt
- SERVER-MYSQL show databases attempt
- PROTOCOL-FTP EXPLOIT STAT asterisk dos attempt
- PROTOCOL-FTP EXPLOIT STAT ? dos attempt
- SERVER-WEBAPP csPassword.cgi access
- SERVER-WEBAPP csPassword password.cgi.tmp access
- POLICY-SOCIAL IRC dns request
- POLICY-SOCIAL IRC dns response
- PROTOCOL-NNTP return code buffer overflow attempt
- SERVER-IIS .asa HTTP header buffer overflow attempt
- SERVER-IIS .cer HTTP header buffer overflow attempt
- SERVER-IIS .cdx HTTP header buffer overflow attempt
- SERVER-WEBAPP Oracle Reports CGI access
- SERVER-IIS .htr chunked Transfer-Encoding
- POLICY-OTHER Chunked-Encoding transfer with no data attempt
- SERVER-WEBAPP Apache chunked-encoding memory corruption exploit attempt
- SERVER-APACHE Apache chunked-encoding worm attempt
- SERVER-OTHER successful gobbles ssh exploit GOBBLE
- SERVER-OTHER successful gobbles ssh exploit uname
- SERVER-OTHER gobbles SSH exploit attempt
- PROTOCOL-ICMP digital island bandwidth query
- SERVER-WEBAPP CISCO VoIP DOS ATTEMPT
- SERVER-WEBAPP directory.php arbitrary command attempt
- SERVER-WEBAPP directory.php access
- SERVER-IIS MS Site Server default login attempt
- SERVER-IIS MS Site Server admin attempt
- SERVER-OTHER Alcatel PABX 4400 connection attempt
- SERVER-WEBAPP IBM Net.Commerce orderdspc.d2w access
- SERVER-OTHER LPD dvips remote command execution attempt

- [ ] SERVER-WEBAPP AlienForm alienform.cgi directory traversal attempt
- [ ] SERVER-WEBAPP AlienForm alienform.cgi access
- [ ] SERVER-WEBAPP WEB-INF access
- [ ] SERVER-WEBAPP iPlanet Search directory traversal attempt
- [ ] SERVER-APACHE Apache Tomcat SnoopServlet servlet access
- [ ] POLICY-SOCIAL ICQ forced user addition
- [ ] SERVER-WEBAPP Macromedia SiteSpring cross site scripting attempt
- [ ] SERVER-WEBAPP mailman cross site scripting attempt
- [ ] BROWSER-FIREFOX Mozilla 1.0 Javascript arbitrary cookie access attempt
- [ ] MALWARE-BACKDOOR trinity connection attempt
- [ ] PROTOCOL-IMAP list literal overflow attempt
- [ ] SERVER-WEBAPP webalizer access
- [ ] SERVER-WEBAPP webfind.exe access
- [ ] SERVER-WEBAPP active.log access
- [ ] MALWARE-BACKDOOR win-trin00 connection attempt
- [ ] PROTOCOL-ICMP Stacheldraht agent->handler skillz
- [ ] SERVER-WEBAPP robot.txt access
- [ ] SERVER-WEBAPP Oracle JavaServer default password login attempt
- [ ] SERVER-WEBAPP Linksys router default username and password login attempt
- [ ] PROTOCOL-FTP SITE NEWER attempt
- [ ] PROTOCOL-POP USER overflow attempt
- [ ] SERVER-WEBAPP Interactive Story story.pl arbitrary file read attempt
- [ ] SERVER-WEBAPP siteUserMod.cgi access
- [ ] SERVER-WEBAPP Oracle Dynamic Monitoring Services dms access
- [ ] SERVER-WEBAPP Oracle Java Process Manager access
- [ ] SERVER-WEBAPP nph-publish.cgi access
- [ ] SERVER-WEBAPP sdbsearch.cgi access
- [ ] SERVER-WEBAPP oracle web application server access
- [ ] INDICATOR-COMPROMISE id check returned userid
- [ ] PROTOCOL-FTP SITE CPWD overflow attempt
- [ ] PROTOCOL-RPC status GHBN format string attack
- [ ] PROTOCOL-SNMP null community string attempt
- [ ] INDICATOR-SHELLCODE kadmind buffer overflow attempt
- [ ] INDICATOR-SHELLCODE kadmind buffer overflow attempt
- [ ] INDICATOR-SHELLCODE kadmind buffer overflow attempt
- [ ] SERVER-OTHER successful kadmind buffer overflow attempt
- [ ] PROTOCOL-IMAP lsub literal overflow attempt
- [ ] PROTOCOL-IMAP find overflow attempt
- [ ] PROTOCOL-RPC AMD TCP amqproc_mount plog overflow attempt
- [ ] PROTOCOL-RPC CMSD TCP CMSD_CREATE buffer overflow attempt
- [ ] PROTOCOL-RPC CMSD udp CMSD_INSERT buffer overflow attempt
- [ ] PROTOCOL-RPC sadmind TCP NETMGT_PROC_SERVICE CLIENT_DOMAIN overflow attempt
- [ ] PROTOCOL-RPC STATD TCP stat mon_name format string exploit attempt
- [ ] PROTOCOL-RPC STATD TCP monitor mon_name format string exploit attempt
- [ ] PROTOCOL-ICMP SolarWinds IP scan attempt
- [ ] PROTOCOL-FTP SITE NEWER overflow attempt
- [ ] PROTOCOL-RPC portmap proxy attempt TCP
- [ ] PROTOCOL-RPC mountd UDP export request
- [ ] PROTOCOL-RPC mountd UDP exportall request
- [ ] PROTOCOL-FTP shadow retrieval attempt
- [ ] SERVER-WEBAPP rpc-nlog.pl access
- [ ] SERVER-WEBAPP cart.cgi access
- [ ] PROTOCOL-POP LIST overflow attempt
- [ ] SERVER-OTHER bootp hardware address length overflow
- [ ] PROTOCOL-TFTP GET filename overflow attempt
- [ ] SERVER-WEBAPP /Carello/add.exe access
- [ ] SERVER-WEBAPP answerbook2 admin attempt
- [ ] PROTOCOL-DNS dns zone transfer via UDP detected
- [ ] SERVER-WEBAPP AlienForm af.cgi directory traversal attempt
- [ ] SERVER-WEBAPP AlienForm af.cgi access
- [ ] SERVER-APACHE Apache Tomcat servlet mapping cross site scripting attempt
- [ ] SERVER-APACHE Apache Tomcat TroubleShooter servlet access
- [ ] SERVER-WEBAPP jigsaw dos attempt
- [ ] SERVER-WEBAPP PHP-Wiki cross site scripting attempt
- [ ] SERVER-OTHER SSH server banner overflow
- [ ] FILE-JAVA Oracle Javascript document.domain attempt
- [ ] PROTOCOL-IMAP login buffer overflow attempt
- [ ] PROTOCOL-IMAP authenticate overflow attempt
- [ ] POLICY-MULTIMEDIA vncviewer Java applet download attempt
- [ ] SERVER-WEBAPP webcart-lite access
- [ ] SERVER-WEBAPP way-board.cgi access
- [ ] SERVER-WEBAPP robots.txt access
- [ ] PROTOCOL-ICMP Stacheldraht handler->agent niggahbitch
- [ ] PROTOCOL-ICMP Stacheldraht handler->agent ficken
- [ ] SERVER-WEBAPP CISCO PIX Firewall Manager directory traversal attempt
- [ ] SERVER-WEBAPP Linksys router default password login attempt
- [ ] SERVER-WEBAPP mrtg.cgi directory traversal attempt
- [ ] SERVER-WEBAPP webdist.cgi arbitrary command attempt
- [ ] X11 xdmcp info query
- [ ] SERVER-WEBAPP Interactive Story story.pl access
- [ ] SERVER-WEBAPP Oracle XSQLConfig.xml access
- [ ] SERVER-WEBAPP globals.jsa access
- [ ] SERVER-WEBAPP cgicso access
- [ ] SERVER-WEBAPP printenv access
- [ ] SERVER-WEBAPP book.cgi arbitrary command execution attempt
- [ ] SERVER-WEBAPP bad HTTP 1.1 request - potential worm attack
- [ ] SERVER-OTHER OpenSSL Worm traffic
- [ ] MALWARE-CNC slapper worm admin traffic
- [ ] PROTOCOL-RPC status GHBN format string attack
- [ ] PROTOCOL-SNMP missing community string attempt
- [ ] INDICATOR-SHELLCODE kadmind buffer overflow attempt
- [ ] INDICATOR-SHELLCODE kadmind buffer overflow attempt
- [ ] INDICATOR-SHELLCODE kadmind buffer overflow attempt
- [ ] SERVER-OTHER successful kadmind buffer overflow attempt
- [ ] PROTOCOL-IMAP rename overflow attempt
- [ ] PROTOCOL-RPC AMD UDP amqproc_mount plog overflow attempt
- [ ] PROTOCOL-RPC CMSD UDP CMSD_CREATE buffer overflow attempt
- [ ] PROTOCOL-RPC CMSD TCP CMSD_INSERT buffer overflow attempt
- [ ] PROTOCOL-RPC sadmind UDP NETMGT_PROC_SERVICE CLIENT_DOMAIN overflow attempt
- [ ] PROTOCOL-RPC STATD UDP stat mon_name format string exploit attempt
- [ ] PROTOCOL-RPC STATD UDP monitor mon_name format string exploit attempt
- [ ] INDICATOR-SCAN UPnP service discover attempt
- [ ] PROTOCOL-FTP CWD overflow attempt
- [ ] PROTOCOL-FTP SITE ZIPCHK overflow attempt
- [ ] PROTOCOL-RPC portmap proxy attempt UDP
- [ ] PROTOCOL-RPC mountd TCP exportall request
- [ ] PROTOCOL-FTP authorized_keys
- [ ] PROTOCOL-IMAP auth literal overflow attempt
- [ ] SERVER-WEBAPP rpc-smb.pl access
- [ ] PROTOCOL-POP AUTH overflow attempt
- [ ] PROTOCOL-POP XTND overflow attempt
- [ ] SERVER-OTHER bootp invalid hardware type
- [ ] PROTOCOL-FTP RMDIR overflow attempt
- [ ] SERVER-WEBAPP /ecscripts/ecware.exe access
- [ ] SERVER-WEBAPP answerbook2 arbitrary command execution attempt
- [ ] PROTOCOL-RPC portmap SET attempt TCP 111

- PROTOCOL-RPC portmap SET attempt UDP 111
- PROTOCOL-RPC mountd UDP mount request
- PROTOCOL-RPC AMD UDP pid request
- PROTOCOL-RPC AMD UDP version request
- PROTOCOL-RPC sadmind TCP PING
- PROTOCOL-RPC portmap NFS request TCP
- PROTOCOL-RPC portmap RQUOTA request TCP
- PROTOCOL-RPC tooltalk UDP overflow attempt
- SERVER-OTHER GlobalSunTech Access Point Information Disclosure attempt
- SERVER-WEBAPP phpbb quick-reply.php access
- SERVER-IIS MDAC Content-Type overflow attempt
- PROTOCOL-FTP PASS overflow attempt
- PROTOCOL-FTP REST overflow attempt
- PROTOCOL-FTP RMD overflow attempt
- SERVER-WEBAPP xp_regdeletekey attempt
- MALWARE-BACKDOOR DeepThroat 3.1 Connection
- MALWARE-BACKDOOR DeepThroat 3.1 Server Response on port 3150
- MALWARE-BACKDOOR DeepThroat 3.1 Server Response on port 4120
- POLICY-SOCIAL Microsoft MSN outbound file transfer request
- POLICY-SOCIAL Microsoft MSN outbound file transfer accept
- POLICY-SOCIAL Microsoft MSN user search
- PROTOCOL-FTP LIST directory traversal attempt
- SERVER-WEBAPP vpasswd.cgi access
- SERVER-WEBAPP viralator.cgi access
- SERVER-WEBAPP calendar.php access
- SERVER-WEBAPP readmsg.php access
- SERVER-WEBAPP remote include path attempt
- SQL Worm propagation attempt OUTBOUND
- PROTOCOL-RPC portmap kcms_server request TCP
- INDICATOR-COMPROMISE CVS invalid user authentication response
- INDICATOR-COMPROMISE CVS double free exploit attempt response
- INDICATOR-COMPROMISE CVS missing cvsroot response
- PROTOCOL-RPC portmap UNSET attempt TCP 111
- PROTOCOL-RPC portmap status request TCP
- PROTOCOL-RPC mountd TCP dump request
- PROTOCOL-RPC mountd TCP unmount request
- PROTOCOL-RPC mountd TCP unmountall request
- PROTOCOL-RPC RQUOTA getquota overflow attempt TCP
- PROTOCOL-RPC yppasswd username overflow attempt TCP
- PROTOCOL-RPC yppasswd old password overflow attempt TCP
- PROTOCOL-RPC yppasswd new password overflow attempt TCP
- PROTOCOL-RPC yppasswd user update TCP
- PROTOCOL-RPC ypserv maplist request TCP
- PROTOCOL-RPC portmap network-status-monitor request TCP
- PROTOCOL-RPC network-status-monitor mon-callback request TCP
- POLICY-OTHER xtacacs login attempt
- POLICY-OTHER xtacacs accepted login response
- POLICY-OTHER PPTP Start Control Request attempt
- PROTOCOL-IMAP partial body.peek buffer overflow attempt
- SQL ping attempt
- SERVER-WEBAPP cached_feed.cgi moreover shopping cart access
- SERVER-WEBAPP Bugtraq process_bug.cgi access
- SERVER-WEBAPP Bugtraq enter_bug.cgi access
- SERVER-WEBAPP helpout.exe access
- SERVER-WEBAPP MsmMask.exe access
- SERVER-APACHE Apache Tomcat null byte directory listing attempt
- SERVER-WEBAPP Demarc SQL injection attempt
- SERVER-WEBAPP Lotus Notes .pl script source download attempt
- SERVER-WEBAPP BitKeeper arbitrary command attempt
- SERVER-WEBAPP post32.exe arbitrary command attempt
- SERVER-WEBAPP lyris.pl access
- SERVER-WEBAPP Mambo uploadimage.php upload php file attempt
- SERVER-WEBAPP Mambo uploadimage.php access
- PROTOCOL-RPC mountd TCP mount request
- PROTOCOL-RPC AMD TCP pid request
- PROTOCOL-RPC AMD TCP version request
- PROTOCOL-RPC sadmind UDP PING
- PROTOCOL-RPC portmap NFS request UDP
- PROTOCOL-RPC portmap RQUOTA request UDP
- PROTOCOL-RPC RQUOTA getquota overflow attempt UDP
- PROTOCOL-RPC tooltalk TCP overflow attempt
- SERVER-WEBAPP phpbb quick-reply.php arbitrary command attempt
- SERVER-WEBAPP ion-p access
- PROTOCOL-FTP SITE EXEC format string attempt
- PROTOCOL-FTP MKD overflow attempt
- PROTOCOL-FTP DELE overflow attempt
- SERVER-WEBAPP xp_regwrite attempt
- SERVER-WEBAPP perl post attempt
- MALWARE-BACKDOOR DeepThroat 3.1 Connection attempt on port 3150
- MALWARE-BACKDOOR DeepThroat 3.1 Connection attempt on port 4120
- MALWARE-BACKDOOR Doly variant outbound connection attempt
- SERVER-OTHER xfs overflow attempt
- POLICY-SOCIAL Microsoft MSN outbound file transfer rejected
- POLICY-SOCIAL Microsoft MSN login attempt
- PROTOCOL-IMAP login literal buffer overflow attempt
- SERVER-WEBAPP alya.cgi access
- SERVER-WEBAPP read_body.php access attempt
- SERVER-WEBAPP edit_image.php access
- SERVER-WEBAPP smartsearch.cgi access
- SQL Worm propagation attempt
- PROTOCOL-RPC portmap kcms_server request UDP
- PROTOCOL-RPC kcms_server directory traversal attempt
- INDICATOR-COMPROMISE CVS invalid repository response
- INDICATOR-COMPROMISE CVS invalid directory response
- INDICATOR-COMPROMISE CVS invalid module response
- PROTOCOL-RPC portmap UNSET attempt UDP 111
- PROTOCOL-RPC portmap espd request UDP
- PROTOCOL-RPC mountd UDP dump request
- PROTOCOL-RPC mountd UDP unmount request
- PROTOCOL-RPC mountd UDP unmountall request
- PROTOCOL-RPC yppasswd username overflow attempt UDP
- PROTOCOL-RPC yppasswd old password overflow attempt UDP
- PROTOCOL-RPC yppasswd new password overflow attempt UDP
- PROTOCOL-RPC yppasswd user update UDP
- PROTOCOL-RPC ypserv maplist request UDP
- PROTOCOL-RPC portmap network-status-monitor request UDP
- PROTOCOL-RPC network-status-monitor mon-callback request UDP
- SERVER-OTHER bootp hostname format string attempt
- INDICATOR-SCAN xtacacs failed login response
- INDICATOR-SCAN isakmp login failed
- PROTOCOL-RPC snmpXdmi overflow attempt UDP
- SERVER-OTHER rsyncd module list access
- SERVER-MSSQL version overflow attempt
- SERVER-WEBAPP overflow.cgi access
- SERVER-WEBAPP Bugtraq enter_bug.cgi arbitrary command attempt
- SERVER-WEBAPP TRACE attempt
- SERVER-WEBAPP MsmMask.exe attempt
- SERVER-WEBAPP DB4Web access
- SERVER-WEBAPP iPlanet .perf access
- SERVER-WEBAPP Lotus Notes .csp script source download attempt
- SERVER-WEBAPP Lotus Notes .exe script source download attempt
- SERVER-WEBAPP chip.ini access
- SERVER-WEBAPP post32.exe access
- SERVER-WEBAPP globals.pl access
- SERVER-WEBAPP Mambo upload.php upload php file attempt
- SERVER-WEBAPP Mambo upload.php access

- [ ] SERVER-WEBAPP phpBB privmsg.php access
- [ ] PROTOCOL-RPC portmap nlockmgr request TCP
- [ ] PROTOCOL-RPC portmap rpc.xfsmd request TCP
- [ ] PROTOCOL-RPC rpc.xfsmd xfs_export attempt TCP
- [ ] SERVER-WEBAPP streaming server parse_xml.cgi access
- [ ] PROTOCOL-RPC ypupdated arbitrary command attempt UDP
- [ ] SERVER-IIS WEBDAV exploit attempt
- [ ] PROTOCOL-RPC portmap proxy integer overflow attempt UDP
- [ ] PROTOCOL-RPC CMSD UDP CMSD_CREATE array buffer overflow attempt
- [ ] MALWARE-BACKDOOR SubSeven 2.1 Gold server connection response
- [ ] NETBIOS SMB Trans2 OPEN2 unicode maximum param count overflow attempt
- [ ] PROTOCOL-IMAP authenticate literal overflow attempt
- [ ] PROTOCOL-IMAP create buffer overflow attempt
- [ ] PROTOCOL-POP TOP overflow attempt
- [ ] PROTOCOL-POP DELE overflow attempt
- [ ] PROTOCOL-SERVICES rexec username overflow attempt
- [ ] SERVER-WEBAPP album.pl access
- [ ] SERVER-IIS Battleaxe Forum login.asp access
- [ ] PROTOCOL-IMAP rename literal overflow attempt
- [ ] PROTOCOL-POP DELE negative argument attempt
- [ ] INDICATOR-COMPROMISE Microsoft cmd.exe banner
- [ ] PROTOCOL-FTP CWD Root directory traversal attempt
- [ ] SERVER-WEBAPP ikonboard.cgi access
- [ ] SERVER-IIS nsiislog.dll access
- [ ] SERVER-IIS IISProtect access
- [ ] SERVER-IIS MS BizTalk server access
- [ ] SERVER-WEBAPP philboard.mdb access
- [ ] SERVER-WEBAPP philboard_admin.asp access
- [ ] SERVER-WEBAPP /*.shtml access
- [ ] SERVER-WEBAPP shoutbox.php directory traversal attempt
- [ ] SERVER-WEBAPP b2 cafelog gm-2-b2.php remote file include attempt
- [ ] SERVER-WEBAPP TextPortal admin.php default password admin attempt
- [ ] SERVER-WEBAPP BLNews objects.inc.php4 remote file include attempt
- [ ] SERVER-WEBAPP Turba status.php access
- [ ] SERVER-WEBAPP ttCMS header.php access
- [ ] SERVER-WEBAPP autohtml.php directory traversal attempt
- [ ] SERVER-WEBAPP ttforum remote file include attempt
- [ ] SERVER-IIS IISProtect globaladmin.asp access
- [ ] SERVER-OTHER BGP invalid type 0
- [ ] OS-WINDOWS Microsoft Windows SMB startup folder unicode access
- [ ] PROTOCOL-FTP PASS format string attempt
- [ ] PUA-P2P BitTorrent transfer
- [ ] PROTOCOL-RPC mountd TCP mount path overflow attempt
- [ ] NETBIOS SMB DCERPC invalid bind attempt
- [ ] SERVER-WEBAPP alert.cgi access
- [ ] SERVER-WEBAPP cvsview2.cgi access
- [ ] SERVER-WEBAPP multidiff.cgi access
- [ ] SERVER-WEBAPP Matt Wright download.cgi access
- [ ] SERVER-WEBAPP Leif M. Wright everythingform.cgi access
- [ ] SERVER-WEBAPP EasyBoard 2000 ezboard.cgi access
- [ ] SERVER-WEBAPP FileSeek fileseek.cgi access
- [ ] SERVER-WEBAPP Infonautics getdoc.cgi access
- [ ] SERVER-WEBAPP Lars Ellingsen guestserver.cgi access
- [ ] SERVER-WEBAPP Oatmeal Studios Mail File mailfile.cgi access
- [ ] SERVER-WEBAPP Alabanza Control Panel nsManager.cgi access
- [ ] SERVER-WEBAPP Ipswitch IMail printmail.cgi access
- [ ] SERVER-WEBAPP Trend Micro Interscan VirusWall setpasswd.cgi access
- [ ] PROTOCOL-RPC portmap nlockmgr request UDP
- [ ] PROTOCOL-RPC portmap rpc.xfsmd request UDP
- [ ] PROTOCOL-RPC rpc.xfsmd xfs_export attempt UDP
- [ ] SERVER-WEBAPP parse_xml.cgi access
- [ ] SERVER-MAIL From comment overflow attempt
- [ ] PROTOCOL-RPC ypupdated arbitrary command attempt TCP
- [ ] SERVER-IIS WEBDAV nessus safe scan attempt
- [ ] PROTOCOL-RPC portmap proxy integer overflow attempt TCP
- [ ] PROTOCOL-RPC CMSD TCP CMSD_CREATE array buffer overflow attempt
- [ ] OS-WINDOWS Microsoft Windows SMB Trans Max Param/Count OS-WINDOWS attempt
- [ ] INDICATOR-COMPROMISE rexec username too long response
- [ ] PROTOCOL-IMAP lsub overflow attempt
- [ ] PROTOCOL-POP CAPA overflow attempt
- [ ] PROTOCOL-POP STAT overflow attempt
- [ ] PROTOCOL-POP RSET overflow attempt
- [ ] PROTOCOL-SERVICES rexec password overflow attempt
- [ ] SERVER-WEBAPP chipcfg.cgi access
- [ ] PROTOCOL-IMAP list overflow attempt
- [ ] PROTOCOL-IMAP create literal buffer overflow attempt
- [ ] PROTOCOL-POP UIDL negative argument attempt
- [ ] MALWARE-BACKDOOR Remote PC Access connection
- [ ] OS-WINDOWS Microsoft Windows PPTP Start Control Request buffer overflow attempt
- [ ] SERVER-WEBAPP swsrv.cgi access
- [ ] SERVER-IIS IISProtect siteadmin.asp access
- [ ] SERVER-IIS Synchrologic Email Accelerator userid list access attempt
- [ ] SERVER-IIS register.asp access
- [ ] SERVER-WEBAPP philboard_admin.asp authentication bypass attempt
- [ ] SERVER-WEBAPP logicworks.ini access
- [ ] SERVER-WEBAPP p-news.php access
- [ ] SERVER-WEBAPP shoutbox.php access
- [ ] SERVER-WEBAPP b2 cafelog gm-2-b2.php access
- [ ] SERVER-WEBAPP TextPortal admin.php default password 12345 attempt
- [ ] SERVER-WEBAPP BLNews objects.inc.php4 access
- [ ] SERVER-WEBAPP ttCMS header.php remote file include attempt
- [ ] SERVER-WEBAPP test.php access
- [ ] SERVER-WEBAPP autohtml.php access
- [ ] SERVER-WEBAPP mod_gzip_status access
- [ ] SERVER-OTHER BGP invalid length
- [ ] OS-WINDOWS Microsoft Windows SMB startup folder access
- [ ] PROTOCOL-FTP USER format string attempt
- [ ] PUA-P2P BitTorrent announce request
- [ ] SERVER-MAIL Sendmail Content-Transfer-Encoding overflow attempt
- [ ] NETBIOS DCERPC invalid bind attempt
- [ ] SERVER-WEBAPP CSMailto.cgi access
- [ ] SERVER-WEBAPP catgy.cgi access
- [ ] SERVER-WEBAPP cvslog.cgi access
- [ ] SERVER-WEBAPP dnewsweb.cgi access
- [ ] SERVER-WEBAPP Webmin Directory edit_action.cgi access
- [ ] SERVER-WEBAPP EasyBoard 2000 ezadmin.cgi access
- [ ] SERVER-WEBAPP EasyBoard 2000 ezman.cgi access
- [ ] SERVER-WEBAPP Faq-O-Matic fom.cgi access
- [ ] SERVER-WEBAPP Multiple Vendors global.cgi access
- [ ] SERVER-WEBAPP cgiCentral WebStore imageFolio.cgi access
- [ ] SERVER-WEBAPP 3R Soft MailStudio 2000 mailview.cgi access
- [ ] SERVER-WEBAPP Ipswitch IMail readmail.cgi access
- [ ] SERVER-WEBAPP Oracle Cobalt RaQ service.cgi access
- [ ] SERVER-WEBAPP Leif M. Wright simplestmail.cgi access

- SERVER-WEBAPP cgiCentral WebStore ws_mail.cgi access
- SERVER-WEBAPP Infinity CGI exploit scanner nph-exploitscanget.cgi access
- SERVER-WEBAPP CGIScript.net csNews.cgi access
- SERVER-WEBAPP Psunami Bulletin Board psunami.cgi access
- SERVER-WEBAPP Linksys BEFSR41 gozila.cgi access
- SERVER-WEBAPP pmachine remote file include attempt
- SERVER-WEBAPP forum_details.php access
- SERVER-WEBAPP phpMyAdmin db_details_importdocsql.php access
- SERVER-WEBAPP viewtopic.php access
- SERVER-WEBAPP NetGear router default password login attempt admin/password
- SERVER-WEBAPP register.dll access
- SERVER-WEBAPP ContentFilter.dll access
- SERVER-WEBAPP SFNofitication.dll access
- SERVER-WEBAPP TOP10.dll access
- SERVER-WEBAPP SpamExcp.dll access
- SERVER-WEBAPP spamrule.dll access
- SERVER-WEBAPP cgiWebupdate.exe access
- SERVER-WEBAPP WebLogic ConsoleHelp view source attempt
- SERVER-WEBAPP redirect.exe access
- SERVER-WEBAPP changepw.exe access
- SERVER-WEBAPP cwmail.exe access
- SERVER-WEBAPP ddicgi.exe access
- SERVER-WEBAPP ndcgi.exe access
- SERVER-WEBAPP VsSetCookie.exe access
- SERVER-WEBAPP Webnews.exe access
- SERVER-WEBAPP webadmin.dll access
- SERVER-IIS UploadScript11.asp access
- SERVER-IIS DirectoryListing.asp access
- SERVER-IIS /pcadmin/login.asp access
- PROTOCOL-POP USER format string attempt
- OS-WINDOWS Microsoft Windows SMB-DS DCERPC Remote Activation bind attempt
- SERVER-MAIL XEXCH50 overflow attempt
- PROTOCOL-RPC sadmind query with root credentials attempt TCP
- PROTOCOL-RPC sadmind query with root credentials attempt UDP
- OS-WINDOWS DCERPC Messenger Service buffer overflow attempt
- OS-WINDOWS Microsoft Windows SMB-DS DCERPC Messenger Service buffer overflow attempt
- SERVER-MAIL EXPN overflow attempt
- SERVER-MAIL VRFY overflow attempt
- SERVER-MAIL Sendmail SEND FROM prescan too many addresses overflow
- SERVER-MAIL Sendmail SEND FROM prescan too long addresses overflow
- SERVER-MAIL Sendmail SAML FROM prescan too many addresses overflow
- SERVER-MAIL Sendmail SAML FROM prescan too long addresses overflow
- SERVER-MAIL Sendmail SOML FROM prescan too many addresses overflow
- SERVER-MAIL Sendmail SOML FROM prescan too long addresses overflow
- SERVER-MAIL Sendmail MAIL FROM prescan too many addresses overflow
- SERVER-MAIL Sendmail MAIL FROM prescan too long addresses overflow
- SERVER-MAIL Sendmail RCPT TO prescan too many addresses overflow
- SERVER-MAIL Sendmail RCPT TO prescan too long addresses overflow
- MALWARE-BACKDOOR FsSniffer connection attempt
- PROTOCOL-FTP LIST integer overflow attempt
- PROTOCOL-IMAP login brute force attempt
- PROTOCOL-POP login brute force attempt
- SERVER-MAIL AUTH LOGON brute force attempt
- SERVER-WEBAPP oracle portal demo access
- SERVER-WEBAPP PeopleSoft PeopleBooks psdoccgi access
- SERVER-WEBAPP HTTP request with negative Content-Length attempt
- SERVER-WEBAPP UpdateClasses.php access
- SERVER-WEBAPP Title.php access
- SERVER-WEBAPP Setup.php access
- SERVER-WEBAPP GlobalFunctions.php access
- SERVER-WEBAPP DatabaseFunctions.php access
- SERVER-WEBAPP rolis guestbook remote file include attempt
- SERVER-WEBAPP rolis guestbook access
- SERVER-WEBAPP friends.php access
- SERVER-WEBAPP Advanced Poll admin_comment.php access
- SERVER-WEBAPP Advanced Poll admin_edit.php access
- SERVER-WEBAPP Advanced Poll admin_embed.php access
- SERVER-WEBAPP Advanced Poll admin_help.php access
- SERVER-WEBAPP Advanced Poll admin_license.php access
- SERVER-WEBAPP Advanced Poll admin_logout.php access
- SERVER-WEBAPP Advanced Poll admin_password.php access
- SERVER-WEBAPP Advanced Poll admin_preview.php access
- SERVER-WEBAPP Advanced Poll admin_settings.php access
- SERVER-WEBAPP Advanced Poll admin_stats.php access
- SERVER-WEBAPP Advanced Poll admin_templates_misc.php access
- SERVER-WEBAPP Advanced Poll admin_templates.php access
- SERVER-WEBAPP Advanced Poll admin_tpl_misc_new.php access
- SERVER-WEBAPP Advanced Poll admin_tpl_new.php access
- SERVER-WEBAPP Advanced Poll booth.php access
- SERVER-WEBAPP Advanced Poll poll_ssi.php access
- SERVER-WEBAPP Advanced Poll popup.php access
- SERVER-WEBAPP files.inc.php access
- SERVER-WEBAPP chatbox.php access
- SERVER-WEBAPP gallery remote file include attempt
- SERVER-WEBAPP PayPal Storefront remote file include attempt
- INDICATOR-COMPROMISE CVS non-relative path error response
- SERVER-OTHER CVS non-relative path access attempt
- SERVER-OTHER ebola PASS overflow attempt
- SERVER-OTHER ebola USER overflow attempt
- SERVER-IIS foxweb.exe access
- SERVER-IIS foxweb.dll access
- SERVER-WEBAPP iSoft-Solutions QuickStore shopping cart quickstore.cgi access
- SERVER-IIS VP-ASP shopsearch.asp access
- SERVER-IIS VP-ASP ShopDisplayProducts.asp access
- SERVER-IIS sgdynamo.exe access
- SERVER-WEBAPP bsml.pl access
- SERVER-WEBAPP authentication_index.php access
- SERVER-MSSQL probe response overflow attempt
- PROTOCOL-IMAP auth overflow attempt
- SERVER-WEBAPP MatrikzGB privilege escalation attempt
- PROTOCOL-FTP MKD format string attempt
- PROTOCOL-FTP RENAME format string attempt
- PROTOCOL-FTP Yak! FTP server default account login attempt
- PROTOCOL-FTP RMD / attempt
- PROTOCOL-TFTP PUT filename overflow attempt
- PROTOCOL-FTP LIST buffer overflow attempt
- PROTOCOL-TFTP NULL command attempt
- PROTOCOL-FTP SITE CHMOD overflow attempt
- SERVER-WEBAPP DCP-Portal remote file include editor script attempt
- SERVER-WEBAPP DCP-Portal remote file include lib script attempt

- [ ] PROTOCOL-FTP STOR overflow attempt
- [ ] SERVER-WEBAPP PhpGedView search.php access
- [ ] SERVER-WEBAPP myPHPNuke partner.php access
- [ ] SERVER-WEBAPP IdeaBox notification.php file include
- [ ] SERVER-WEBAPP WebChat db_mysql.php file include
- [ ] SERVER-WEBAPP Typo3 translations.php file include
- [ ] SERVER-WEBAPP myphpPagetool pt_config.inc file include
- [ ] SERVER-WEBAPP YaBB SE packages.php file include
- [ ] SERVER-WEBAPP Cyboards options_form.php access
- [ ] SERVER-WEBAPP PhpGedView PGV authentication_index.php base directory manipulation attempt
- [ ] SERVER-WEBAPP PhpGedView PGV config_gedcom.php base directory manipulation attempt
- [ ] SERVER-WEBAPP BugPort config.conf file access
- [ ] SERVER-WEBAPP Photopost PHP Pro showphoto.php access
- [ ] PROTOCOL-FTP NLST overflow attempt
- [ ] SERVER-OTHER ISAKMP first payload certificate request length overflow attempt
- [ ] SERVER-OTHER ISAKMP third payload certificate request length overflow attempt
- [ ] SERVER-OTHER ISAKMP fifth payload certificate request length overflow attempt
- [ ] SERVER-IIS NTLM ASN1 vulnerability scan attempt
- [ ] PROTOCOL-FTP RNTO overflow attempt
- [ ] PROTOCOL-FTP APPE overflow attempt
- [ ] SERVER-WEBAPP /_admin access
- [ ] SERVER-WEBAPP InteractiveQuery.jsp access
- [ ] SERVER-WEBAPP CCBill whereami.cgi access
- [ ] SERVER-WEBAPP WAnewsletter db_type.php access
- [ ] NETBIOS SMB Session Setup andx username overflow attempt
- [ ] NETBIOS SMB Session Setup unicode username overflow attempt
- [ ] SERVER-WEBAPP phptest.php access
- [ ] SERVER-WEBAPP util.pl access
- [ ] PROTOCOL-POP APOP USER overflow attempt
- [ ] SERVER-WEBAPP RealNetworks RealSystem Server DESCRIBE buffer overflow attempt
- [ ] SERVER-OTHER ISAKMP delete hash with empty hash attempt
- [ ] SERVER-OTHER ISAKMP second payload initial contact notification without SPI attempt
- [ ] PROTOCOL-FTP format string attempt
- [x] FILE-IDENTIFY RealNetworks Realplayer .ram playlist file download request
- [x] FILE-IDENTIFY RealNetworks Realplayer .rt playlist file download request
- [ ] PROTOCOL-NNTP sendsys overflow attempt
- [ ] PROTOCOL-NNTP version overflow attempt
- [ ] PROTOCOL-NNTP ihave overflow attempt
- [ ] PROTOCOL-NNTP newgroup overflow attempt
- [ ] PROTOCOL-NNTP article post without path attempt
- [ ] SERVER-WEBAPP MDaemon form2raw.cgi access
- [x] FILE-IDENTIFY Microsoft Windows Audio wmf file download request
- [ ] FILE-MULTIMEDIA RealNetworks RealPlayer playlist file URL overflow attempt
- [ ] FILE-MULTIMEDIA RealNetworks RealPlayer playlist rtsp URL overflow attempt
- [ ] SERVER-OTHER ICQ SRV_MULTI/SRV_META_USER overflow attempt - ISS Witty Worm
- [ ] SERVER-WEBAPP setinfo.hts access
- [ ] POLICY-SOCIAL Yahoo IM successful logon
- [ ] POLICY-SOCIAL Yahoo IM ping
- [ ] POLICY-SOCIAL Yahoo IM conference logon success
- [ ] PROTOCOL-FTP XCWD overflow attempt
- [ ] SERVER-WEBAPP myPHPNuke chatheader.php access
- [ ] SERVER-WEBAPP IdeaBox cord.php file include
- [ ] SERVER-WEBAPP Invision Board emailer.php file include
- [ ] SERVER-WEBAPP WebChat english.php file include
- [ ] SERVER-WEBAPP Invision Board ipchat.php file include
- [ ] SERVER-WEBAPP news.php file include
- [ ] SERVER-WEBAPP Cyboards default_header.php access
- [ ] SERVER-WEBAPP newsPHP Language file include attempt
- [ ] SERVER-WEBAPP PhpGedView PGV functions.php base directory manipulation attempt
- [ ] SERVER-WEBAPP ISAPISkeleton.dll access
- [ ] SERVER-WEBAPP Sample_showcode.html access
- [ ] PROTOCOL-FTP XMKD overflow attempt
- [ ] MALWARE-CNC DoomJuice/mydoom.a backdoor upload/execute
- [ ] SERVER-OTHER ISAKMP second payload certificate request length overflow attempt
- [ ] SERVER-OTHER ISAKMP forth payload certificate request length overflow attempt
- [ ] SERVER-WEBAPP Checkpoint Firewall-1 HTTP parsing format string vulnerability attempt
- [ ] SERVER-WEBAPP Apple QuickTime streaming server view_broadcast.cgi access
- [ ] PROTOCOL-FTP STOU overflow attempt
- [ ] PROTOCOL-FTP RETR overflow attempt
- [ ] SERVER-WEBAPP Compaq web-based management agent denial of service attempt
- [ ] SERVER-WEBAPP CCBill whereami.cgi arbitrary command execution attempt
- [ ] SERVER-WEBAPP WAnewsletter newsletter.php file include attempt
- [ ] SERVER-WEBAPP edittag.pl access
- [ ] NETBIOS SMB-DS Session Setup andx username overflow attempt
- [ ] NETBIOS SMB-DS Session Setup unicode andx username overflow attempt
- [ ] PROTOCOL-TELNET APC SmartSlot default admin account attempt
- [ ] SERVER-WEBAPP Invision Power Board search.pl access
- [ ] SERVER-WEBAPP IGeneric Free Shopping Cart page.php access
- [ ] INDICATOR-COMPROMISE successful cross site scripting forced download attempt
- [ ] SERVER-OTHER ISAKMP initial contact notification without SPI attempt
- [ ] PROTOCOL-FTP invalid MDTM command attempt
- [ ] POLICY-OTHER Microsoft Windows Terminal Server no encryption session initiation attempt
- [x] FILE-IDENTIFY RealNetworks Realplayer .rmp playlist file download request
- [x] FILE-IDENTIFY RealNetworks Realplayer .rp playlist file download request
- [ ] PROTOCOL-NNTP senduuname overflow attempt
- [ ] PROTOCOL-NNTP checkgroups overflow attempt
- [ ] PROTOCOL-NNTP sendme overflow attempt
- [ ] PROTOCOL-NNTP rmgroup overflow attempt
- [ ] SERVER-WEBAPP MDaemon form2raw.cgi overflow attempt
- [ ] FILE-IDENTIFY Microsoft emf file download request
- [ ] FILE-MULTIMEDIA RealNetworks RealPlayer arbitrary javascript command attempt
- [ ] FILE-MULTIMEDIA RealNetworks RealPlayer playlist http URL overflow attempt
- [ ] SERVER-WEBAPP NetObserve authentication bypass attempt
- [ ] SERVER-WEBAPP ServletManager access
- [ ] PROTOCOL-FTP ALLO overflow attempt
- [ ] POLICY-SOCIAL Yahoo IM voicechat
- [ ] POLICY-SOCIAL Yahoo IM conference invitation
- [ ] POLICY-SOCIAL Yahoo IM conference message

- POLICY-SOCIAL Yahoo Messenger File Transfer Receive Request
- POLICY-SOCIAL Yahoo IM message
- POLICY-SOCIAL Yahoo IM successful chat join
- POLICY-SOCIAL Yahoo IM conference offer invitation
- POLICY-SOCIAL Yahoo IM conference request
- POLICY-SOCIAL Yahoo IM conference watch
- SERVER-OTHER Ethereal IGMP IGAP account overflow attempt
- SERVER-OTHER Ethereal IGMP IGAP message overflow attempt
- SERVER-OTHER Ethereal EIGRP prefix length overflow attempt
- NETBIOS SMB-DS ADMIN$ share access
- SERVER-WEBAPP source.jsp access
- BROWSER-PLUGINS Symantec Norton Internet Security 2004 ActiveX clsid access
- SERVER-OTHER ISAKMP invalid identification payload attempt
- SERVER-MAIL WinZip MIME content-type buffer overflow
- SERVER-MAIL WinZip MIME content-disposition buffer overflow
- SERVER-OTHER esignal STREAMQUOTE buffer overflow attempt
- SERVER-OTHER esignal SNAPQUOTE buffer overflow attempt
- OS-WINDOWS DCERPC NCACN-IP-TCP lsass DsRolerUpgradeDownlevelServer overflow attempt
- OS-WINDOWS DCERPC NCADG-IP-UDP lsass DsRolerUpgradeDownlevelServer overflow attempt
- SERVER-OTHER BGP spoofed connection reset attempt
- SERVER-OTHER AFP FPLoginExt username buffer overflow attempt
- PROTOCOL-FTP MDTM overflow attempt
- SERVER-OTHER HP Web JetAdmin remote file upload attempt
- SERVER-OTHER HP Web JetAdmin setinfo access attempt
- SERVER-OTHER HP Web JetAdmin file write attempt
- FILE-OTHER Nullsoft Winamp XM file buffer overflow attempt
- SERVER-OTHER Oracle Web Cache GET overflow attempt
- SERVER-OTHER Oracle Web Cache HEAD overflow attempt
- SERVER-OTHER Oracle Web Cache PUT overflow attempt
- SERVER-OTHER Oracle Web Cache POST overflow attempt
- SERVER-OTHER Oracle Web Cache TRACE overflow attempt
- SERVER-OTHER Oracle Web Cache DELETE overflow attempt
- SERVER-OTHER Oracle Web Cache LOCK overflow attempt
- SERVER-OTHER Oracle Web Cache MKCOL overflow attempt
- SERVER-OTHER Oracle Web Cache COPY overflow attempt
- SERVER-OTHER Oracle Web Cache MOVE overflow attempt
- SERVER-OTHER rsync backup-dir directory traversal attempt
- SERVER-WEBAPP McAfee ePO file upload attempt
- NETBIOS NS lookup response name overflow attempt
- NETBIOS NS lookup short response attempt
- SERVER-WEBAPP modules.php access
- SERVER-WEBAPP PHPBB viewforum.php access
- SERVER-WEBAPP Emumail init.emu access
- SERVER-WEBAPP Emumail emumail.fcgi access
- SERVER-WEBAPP cPanel resetpass access
- SERVER-WEBAPP invalid HTTP version string
- SERVER-IIS SmarterTools SmarterMail frmGetAttachment.aspx access
- SERVER-IIS SmarterTools SmarterMail login.aspx buffer overflow attempt
- SERVER-IIS SmarterTools SmarterMail frmCompose.asp access
- PROTOCOL-FTP RETR format string attempt
- SERVER-WEBAPP Opt-X header.php remote file include attempt
- SERVER-ORACLE dbms_repcat.generate_replication_support buffer overflow attempt
- FILE-OTHER local resource redirection attempt
- SERVER-WEBAPP server negative Content-Length attempt
- SERVER-WEBAPP SAP Crystal Reports crystalimagehandler.aspx access
- OS-WINDOWS SAP Crystal Reports crystalImageHandler.asp directory traversal attempt
- SERVER-OTHER CVS Max-dotdot integer overflow attempt
- SERVER-OTHER eMule buffer overflow attempt
- SERVER-WEBAPP nessus 2.x 404 probe
- PUA-P2P eDonkey server response
- SERVER-WEBAPP TUTOS path disclosure attempt
- OS-WINDOWS Microsoft Windows Content-Disposition CLSID command attempt
- SERVER-WEBAPP Samba SWAT Authorization overflow attempt
- SERVER-WEBAPP Samba SWAT Authorization port 901 overflow attempt
- SERVER-ORACLE dbms_repcat.add_grouped_column buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_master_repgroup buffer overflow attempt
- SERVER-ORACLE dbms_repcat.create_mview_repgroup buffer overflow attempt
- SERVER-ORACLE dbms_repcat.compare_old_values buffer overflow attempt
- SERVER-ORACLE dbms_repcat.comment_on_repobject buffer overflow attempt
- SERVER-ORACLE sysdbms_repcat_rgt.check_ddl_text buffer overflow attempt
- SERVER-ORACLE dbms_repcat.cancel_statistics buffer overflow attempt
- SERVER-ORACLE LINK metadata buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_auth.revoke_surrogate_repcat buffer overflow attempt
- SERVER-ORACLE time_zone buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_auth.grant_surrogate_repcat buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat.alter_mview_propagation buffer overflow attempt
- SERVER-ORACLE dbms_repcat.alter_master_repobject buffer overflow attempt
- SERVER-ORACLE dbms_repcat_sna_utl.register_flavor_change buffer overflow attempt
- SERVER-ORACLE dbms_repcat_admin.unregister_user_repgroup buffer overflow attempt
- SERVER-ORACLE dbms_repcat.send_old_values buffer overflow attempt
- SERVER-ORACLE dbms_repcat.repcat_import_check buffer overflow attempt
- SERVER-ORACLE dbms_repcat_admin.register_user_repgroup buffer overflow attempt
- SERVER-ORACLE sys.dbms_rectifier_diff.rectify buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_master_repobject buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_mview_repgroup buffer overflow attempt
- SERVER-ORACLE dbms_repcat_instantiate.drop_site_instantiation buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_fla.ensure_not_published buffer overflow attempt
- SERVER-ORACLE from_tz buffer overflow attempt
- SERVER-ORACLE dbms_repcat_instantiate.instantiate_offline buffer overflow attempt
- SERVER-ORACLE Oracle 9i TNS Listener SERVICE_NAME Remote Buffer Overflow attempt

- SERVER-ORACLE user name buffer overflow attempt
- SERVER-ORACLE dbms_offline_og.begin_load buffer overflow attempt
- SERVER-OTHER HP Web JetAdmin ExecuteFile admin access
- SERVER-WEBAPP SSLv2 Client_Hello with pad Challenge Length overflow attempt
- PROTOCOL-IMAP login format string attempt
- PROTOCOL-POP PASS format string attempt
- SERVER-WEBAPP processit access
- SERVER-WEBAPP pgpmail.pl access
- SERVER-WEBAPP sresult.exe access
- SERVER-ORACLE dbms_repcat.add_delete_resolution buffer overflow attempt
- SERVER-ORACLE dbms_repcat_rgt.instantiate_online buffer overflow attempt
- SERVER-ORACLE sys.dbms_system.ksdwrt buffer overflow attempt
- SERVER-ORACLE mdsys.sdo_admin.sdo_code_size buffer overflow attempt
- SERVER-ORACLE mdsys.md2.sdo_code_size buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_rq.add_column buffer overflow attempt
- SERVER-ORACLE sys.dbms_internal_repcat.validate buffer overflow attempt
- SERVER-ORACLE sys.dbms_internal_repcat.disable_receiver_trace buffer overflow attempt
- SERVER-ORACLE sys.dbms_defer_internal_sys.parallel_push_recovery buffer overflow attempt
- SERVER-ORACLE sys.dbms_aqadm.verify_queue_types_no_queue buffer overflow attempt
- SERVER-ORACLE sys.dbms_aq_import_internal.aq_table_defn_update buffer overflow attempt
- SERVER-ORACLE alter file buffer overflow attempt
- SERVER-ORACLE TO_CHAR buffer overflow attempt
- SERVER-WEBAPP Oracle iSQLPlus username overflow attempt
- SERVER-WEBAPP Oracle 10g iSQLPlus login.unix connectID overflow attempt
- FILE-IMAGE JPEG parser multipacket heap overflow attempt
- SERVER-ORACLE dbms_offline_og.begin_instantiation buffer overflow attempt
- SERVER-ORACLE dbms_offline_og.end_instantiation buffer overflow attempt
- SERVER-ORACLE dbms_offline_og.resume_subset_of_masters buffer overflow attempt
- SERVER-ORACLE dbms_offline_snapshot.end_load buffer overflow attempt
- SERVER-ORACLE dbms_rectifier_diff.rectify buffer overflow attempt
- SERVER-ORACLE dbms_repcat.add_column_group_to_flavor buffer overflow attempt
- SERVER-ORACLE dbms_repcat.add_object_to_flavor buffer overflow attempt
- SERVER-ORACLE dbms_repcat.add_priority_date buffer overflow attempt
- SERVER-ORACLE dbms_repcat.add_priority_number buffer overflow attempt
- SERVER-ORACLE dbms_repcat.add_priority_raw buffer overflow attempt
- SERVER-ORACLE dbms_repcat.add_site_priority_site buffer overflow attempt
- SERVER-ORACLE dbms_repcat.add_update_resolution buffer overflow attempt
- SERVER-ORACLE NUMTODSINTERVAL/NUMTOYMINTERVAL buffer overflow attempt
- SERVER-WEBAPP PHPNuke Forum viewtopic SQL insertion attempt
- SERVER-WEBAPP SSLv2 Client_Hello Challenge Length overflow attempt
- SERVER-WEBAPP Ipswitch WhatsUpGold instancename overflow attempt
- PROTOCOL-IMAP login literal format string attempt
- SERVER-IIS ping.asp access
- SERVER-WEBAPP ibillpm.pl access
- BROWSER-IE Microsoft Internet Explorer bitmap BitmapOffset integer overflow attempt
- FILE-IMAGE libpng tRNS overflow attempt
- SERVER-ORACLE dbms_repcat_rgt.instantiate_offline buffer overflow attempt
- SERVER-ORACLE ctx_output.start_log buffer overflow attempt
- SERVER-ORACLE ctxsys.driddlr.subindexpopulate buffer overflow attempt
- SERVER-ORACLE mdsys.md2.validate_geom buffer overflow attempt
- SERVER-ORACLE sys.ltutil.pushdeferredtxns buffer overflow attempt
- SERVER-ORACLE sys.dbms_rectifier_diff.differences buffer overflow attempt
- SERVER-ORACLE sys.dbms_internal_repcat.enable_receiver_trace buffer overflow attempt
- SERVER-ORACLE sys.dbms_defer_repcat.enable_propagation_to_dblink buffer overflow attempt
- SERVER-ORACLE sys.dbms_aqadm_sys.verify_queue_types buffer overflow attempt
- SERVER-ORACLE sys.dbms_aqadm.verify_queue_types_get_nrp buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_utl.is_master buffer overflow attempt
- SERVER-ORACLE create file buffer overflow attempt
- SERVER-WEBAPP Oracle iSQLPlus sid overflow attempt
- SERVER-WEBAPP Oracle iSQLPlus login.uix username overflow attempt
- FILE-IMAGE Microsoft Multiple Products JPEG parser heap overflow attempt
- SERVER-ORACLE dbms_offline_og.begin_flavor_change buffer overflow attempt
- SERVER-ORACLE dbms_offline_og.end_flavor_change buffer overflow attempt
- SERVER-ORACLE dbms_offline_og.end_load buffer overflow attempt
- SERVER-ORACLE dbms_offline_snapshot.begin_load buffer overflow attempt
- SERVER-ORACLE dbms_rectifier_diff.differences buffer overflow attempt
- SERVER-ORACLE dbms_repcat.abort_flavor_definition buffer overflow attempt
- SERVER-ORACLE dbms_repcat.add_columns_to_flavor buffer overflow attempt
- SERVER-ORACLE dbms_repcat.add_priority_char buffer overflow attempt
- SERVER-ORACLE dbms_repcat.add_priority_nchar buffer overflow attempt
- SERVER-ORACLE dbms_repcat.add_priority_nvarchar2 buffer overflow attempt
- SERVER-ORACLE dbms_repcat.add_priority_varchar2 buffer overflow attempt
- SERVER-ORACLE dbms_repcat.add_unique_resolution buffer overflow attempt
- SERVER-ORACLE dbms_repcat.alter_master_propagation buffer overflow attempt

- SERVER-ORACLE dbms_repcat.alter_mview_propagation buffer overflow attempt
- SERVER-ORACLE dbms_repcat.alter_priority_char buffer overflow attempt
- SERVER-ORACLE dbms_repcat.alter_priority_date buffer overflow attempt
- SERVER-ORACLE dbms_repcat.alter_priority_nchar buffer overflow attempt
- SERVER-ORACLE dbms_repcat.alter_priority_number buffer overflow attempt
- SERVER-ORACLE dbms_repcat.alter_priority_nvarchar2 buffer overflow attempt
- SERVER-ORACLE dbms_repcat.alter_priority_raw buffer overflow attempt
- SERVER-ORACLE dbms_repcat.alter_priority buffer overflow attempt
- SERVER-ORACLE dbms_repcat.alter_priority_varchar2 buffer overflow attempt
- SERVER-ORACLE dbms_repcat.alter_site_priority_site buffer overflow attempt
- SERVER-ORACLE dbms_repcat.alter_site_priority buffer overflow attempt
- SERVER-ORACLE dbms_repcat.alter_snapshot_propagation buffer overflow attempt
- SERVER-ORACLE dbms_repcat_auth.revoke_surrogate_repcat buffer overflow attempt
- SERVER-ORACLE dbms_repcat.begin_flavor_definition buffer overflow attempt
- SERVER-ORACLE dbms_repcat.comment_on_column_group buffer overflow attempt
- SERVER-ORACLE dbms_repcat.comment_on_delete_resolution buffer overflow attempt
- SERVER-ORACLE dbms_repcat.comment_on_mview_repsites buffer overflow attempt
- SERVER-ORACLE dbms_repcat.comment_on_priority_group buffer overflow attempt
- SERVER-ORACLE dbms_repcat.comment_on_repgroup buffer overflow attempt
- SERVER-ORACLE dbms_repcat.comment_on_repsites buffer overflow attempt
- SERVER-ORACLE dbms_repcat.comment_on_site_priority buffer overflow attempt
- SERVER-ORACLE dbms_repcat.comment_on_unique_resolution buffer overflow attempt
- SERVER-ORACLE dbms_repcat.comment_on_update_resolution buffer overflow attempt
- SERVER-ORACLE dbms_repcat.create_master_repgroup buffer overflow attempt
- SERVER-ORACLE dbms_repcat.create_master_repobject buffer overflow attempt
- SERVER-ORACLE dbms_repcat.create_snapshot_repgroup buffer overflow attempt
- SERVER-ORACLE dbms_repcat.define_column_group buffer overflow attempt
- SERVER-ORACLE dbms_repcat.define_priority_group buffer overflow attempt
- SERVER-ORACLE dbms_repcat.define_site_priority buffer overflow attempt
- SERVER-ORACLE dbms_repcat.do_deferred_repcat_admin buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_column_group_from_flavor buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_column_group buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_columns_from_flavor buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_delete_resolution buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_grouped_column buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_mview_repobject buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_object_from_flavor buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_priority_char buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_priority_date buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_priority_nchar buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_priority_number buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_priority_nvarchar2 buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_priority_raw buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_priority buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_priority_varchar2 buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_site_priority_site buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_site_priority buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_snapshot_repgroup buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_snapshot_repobject buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_unique_resolution buffer overflow attempt
- SERVER-ORACLE dbms_repcat.drop_update_resolution buffer overflow attempt
- SERVER-ORACLE dbms_repcat.execute_ddl buffer overflow attempt
- SERVER-ORACLE dbms_repcat.generate_replication_package buffer overflow attempt
- SERVER-ORACLE dbms_repcat_instantiate.instantiate_online buffer overflow attempt
- SERVER-ORACLE dbms_repcat.make_column_group buffer overflow attempt
- SERVER-ORACLE dbms_repcat.obsolete_flavor_definition buffer overflow attempt
- SERVER-ORACLE dbms_repcat.publish_flavor_definition buffer overflow attempt
- SERVER-ORACLE dbms_repcat.purge_flavor_definition buffer overflow attempt
- SERVER-ORACLE dbms_repcat.purge_master_log buffer overflow attempt
- SERVER-ORACLE dbms_repcat.purge_statistics buffer overflow attempt
- SERVER-ORACLE dbms_repcat.refresh_mview_repgroup buffer overflow attempt
- SERVER-ORACLE dbms_repcat.refresh_snapshot_repgroup buffer overflow attempt
- SERVER-ORACLE dbms_repcat.register_mview_repgroup buffer overflow attempt
- SERVER-ORACLE dbms_repcat.register_snapshot_repgroup buffer overflow attempt
- SERVER-ORACLE dbms_repcat.register_statistics buffer overflow attempt
- SERVER-ORACLE dbms_repcat.relocate_masterdef buffer overflow attempt
- SERVER-ORACLE dbms_repcat.rename_shadow_column_group buffer overflow attempt
- SERVER-ORACLE dbms_repcat.resume_master_activity buffer overflow attempt

- SERVER-ORACLE dbms_repcat_rgt.check_ddl_text buffer overflow attempt
- SERVER-ORACLE dbms_repcat_rgt.drop_site_instantiation buffer overflow attempt
- SERVER-ORACLE dbms_repcat.send_and_compare_old_values buffer overflow attempt
- SERVER-ORACLE dbms_repcat.set_columns buffer overflow attempt
- SERVER-ORACLE dbms_repcat.set_local_flavor buffer overflow attempt
- SERVER-ORACLE dbms_repcat.specify_new_masters buffer overflow attempt
- SERVER-ORACLE dbms_repcat.suspend_master_activity buffer overflow attempt
- SERVER-ORACLE dbms_repcat.unregister_mview_repgroup buffer overflow attempt
- SERVER-ORACLE dbms_repcat.unregister_snapshot_repgroup buffer overflow attempt
- SERVER-ORACLE dbms_repcat.validate_flavor_definition buffer overflow attempt
- SERVER-ORACLE dbms_repcat.validate_for_local_flavor buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_fla.abort_flavor_definition buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_fla.add_object_to_flavor buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_fla.begin_flavor_definition buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_fla.drop_object_from_flavor buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_fla_mas.add_column_group_to_flavor buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_fla_mas.add_columns_to_flavor buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_fla_mas.drop_column_group_from_flavor buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_fla_mas.drop_columns_from_flavor buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_fla_mas.obsolete_flavor_definition buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_fla_mas.publish_flavor_definition buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_fla_mas.purge_flavor_definition buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_fla.set_local_flavor buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_fla.validate_flavor_definition buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_fla.validate_for_local_flavor buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_mas.alter_master_repobject buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_mas.comment_on_repgroup buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_mas.comment_on_repobject buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_mas.create_master_repgroup buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_mas.create_master_repobject buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_mas.do_deferred_repcat_admin buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_mas.drop_master_repgroup buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_mas.generate_replication_package buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_mas.purge_master_log buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_mas.relocate_masterdef buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_mas.rename_shadow_column_group buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_mas.resume_master_activity buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_mas.suspend_master_activity buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna_utl.alter_snapshot_propagation buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna_utl.create_snapshot_repgroup buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna_utl.drop_snapshot_repgroup buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna_utl.drop_snapshot_repobject buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna_utl.refresh_snapshot_repgroup buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna_utl.register_snapshot_repgroup buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna_utl.repcat_import_check buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna_utl.unregister_snapshot_repgroup buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_utl4.drop_master_repobject buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_utl.drop_an_object buffer overflow attempt
- SERVER-ORACLE dbms_repcat.create_mview_repobject buffer overflow attempt
- SERVER-ORACLE dbms_repcat.create_snapshot_repobject buffer overflow attempt
- SERVER-ORACLE dbms_repcat.generate_mview_support buffer overflow attempt
- SERVER-ORACLE dbms_repcat.generate_replication_trigger buffer overflow attempt
- SERVER-ORACLE dbms_repcat.generate_snapshot_support buffer overflow attempt
- SERVER-ORACLE dbms_repcat.remove_master_databases buffer overflow attempt
- SERVER-ORACLE dbms_repcat.switch_mview_master buffer overflow attempt
- SERVER-ORACLE dbms_repcat.switch_snapshot_master buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.add_delete_resolution buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.add_priority_char buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.add_priority_date buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.add_priority_nchar buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.add_priority_number buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.add_priority_nvarchar2 buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.add_priority_raw buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.add_priority_varchar2 buffer overflow attempt

- SERVER-ORACLE sys.dbms_repcat_conf.add_site_priority_site buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.add_unique_resolution buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.add_update_resolution buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.alter_priority_char buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.alter_priority_date buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.alter_priority_nchar buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.alter_priority_number buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.alter_priority_nvarchar2 buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.alter_priority_raw buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.alter_priority buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.alter_priority_varchar2 buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.alter_site_priority_site buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.alter_site_priority buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.cancel_statistics buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.comment_on_delete_resolution buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.comment_on_priority_group buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.comment_on_site_priority buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.comment_on_unique_resolution buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.comment_on_update_resolution buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.define_priority_group buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.define_site_priority buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.drop_delete_resolution buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.drop_priority_char buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.drop_priority_date buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.drop_priority_nchar buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.drop_priority_number buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.drop_priority_nvarchar2 buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.drop_priority_raw buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.drop_priority buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.drop_priority_varchar2 buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.drop_site_priority_site buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.drop_site_priority buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.drop_unique_resolution buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.drop_update_resolution buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.purge_statistics buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_conf.register_statistics buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna.alter_snapshot_propagation buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna.create_snapshot_repgroup buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna.create_snapshot_repobject buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna.create_snapshot_repschema buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna.drop_snapshot_repgroup buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna.drop_snapshot_repobject buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna.drop_snapshot_repschema buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna.generate_snapshot_support buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna.refresh_snapshot_repgroup buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna.refresh_snapshot_repschema buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna.register_snapshot_repgroup buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna.repcat_import_check buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna.set_local_flavor buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna.switch_snapshot_master buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna.unregister_snapshot_repgroup buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna_utl.switch_snapshot_master buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_sna.validate_for_local_flavor buffer overflow attempt
- SERVER-ORACLE sys.dbms_repcat_untrusted.register_snapshot_repgroup buffer overflow attempt
- PROTOCOL-DNS UDP inverse query
- PROTOCOL-DNS TCP inverse query
- NETBIOS SMB repeated logon failure
- NETBIOS SMB-DS repeated logon failure
- SERVER-WEBAPP PhpGedView PGV base directory manipulation
- OS-WINDOWS Microsoft Windows XPAT pattern overflow attempt
- OS-WINDOWS DCERPC NCACN-IP-TCP nddeapi NDdeSetTrustedShareW overflow attempt
- NETBIOS DCERPC NCACN-IP-TCP winreg InitiateSystemShutdown attempt
- SERVER-OTHER Volition Freespace 2 buffer overflow attempt
- PROTOCOL-IMAP command overflow attempt
- PROTOCOL-IMAP delete literal overflow attempt
- MALWARE-BACKDOOR NetBus Pro 2.0 connection request
- MALWARE-CNC RUX the Tick get windows directory
- MALWARE-CNC RUX the Tick get system directory
- MALWARE-CNC RUX the Tick upload/execute arbitrary file
- MALWARE-CNC Asylum 0.1 connection request
- MALWARE-CNC Asylum 0.1 connection
- MALWARE-CNC Insane Network 4.0 connection

- [ ] MALWARE-CNC Insane Network 4.0 connection port 63536
- [ ] NETBIOS SMB NT Trans NT CREATE oversized Security Descriptor attempt
- [ ] NETBIOS SMB NT Trans NT CREATE unicode oversized Security Descriptor attempt
- [ ] NETBIOS SMB-DS NT Trans NT CREATE oversized Security Descriptor attempt
- [ ] NETBIOS SMB-DS NT Trans NT CREATE unicode oversized Security Descriptor attempt
- [ ] NETBIOS SMB NT Trans NT CREATE SACL overflow attempt
- [ ] NETBIOS SMB NT Trans NT CREATE unicode SACL overflow attempt
- [ ] NETBIOS SMB-DS NT Trans NT CREATE SACL overflow attempt
- [ ] NETBIOS SMB-DS NT Trans NT CREATE unicode SACL overflow attempt
- [ ] NETBIOS SMB NT Trans NT CREATE DACL overflow attempt
- [ ] NETBIOS SMB NT Trans NT CREATE unicode DACL overflow attempt
- [ ] NETBIOS SMB-DS NT Trans NT CREATE DACL overflow attempt
- [ ] NETBIOS SMB-DS NT Trans NT CREATE unicode DACL overflow attempt
- [ ] NETBIOS SMB NT Trans NT CREATE invalid SACL ace size dos attempt
- [ ] NETBIOS SMB NT Trans NT CREATE unicode invalid SACL ace size dos attempt
- [ ] NETBIOS SMB-DS NT Trans NT CREATE invalid SACL ace size dos attempt
- [ ] NETBIOS SMB-DS NT Trans NT CREATE unicode invalid SACL ace size dos attempt
- [ ] NETBIOS SMB NT Trans NT CREATE invalid SACL ace size dos attempt
- [ ] NETBIOS SMB NT Trans NT CREATE unicode invalid SACL ace size dos attempt
- [ ] NETBIOS SMB-DS NT Trans NT CREATE invalid SACL ace size dos attempt
- [ ] NETBIOS SMB-DS NT Trans NT CREATE unicode invalid SACL ace size dos attempt
- [ ] PROTOCOL-IMAP copy literal overflow attempt
- [ ] SERVER-WEBAPP NetScreen SA 5000 delhomepage.cgi access
- [ ] MALWARE-BACKDOOR Vampire 1.2 connection confirmation
- [ ] PROTOCOL-IMAP APPEND overflow attempt
- [ ] PROTOCOL-IMAP fetch literal overflow attempt
- [ ] PROTOCOL-IMAP status literal overflow attempt
- [ ] PROTOCOL-IMAP SUBSCRIBE literal overflow attempt
- [ ] PROTOCOL-IMAP unsubscribe literal overflow attempt
- [ ] PROTOCOL-FTP RNFR overflow attempt
- [ ] BROWSER-IE Microsoft Internet Explorer ANI file parsing buffer overflow attempt
- [x] MALWARE-BACKDOOR Y3KRAT 1.5 Connect
- [ ] MALWARE-BACKDOOR Y3KRAT 1.5 Connection confirmation
- [ ] SERVER-OTHER AOL Instant Messenger goaway message buffer overflow attempt
- [ ] SERVER-IIS w3who.dll buffer overflow attempt
- [ ] SERVER-OTHER squid WCCP I_SEE_YOU message overflow attempt
- [ ] PUA-OTHER Microsoft MSN Messenger png overflow
- [ ] FILE-IMAGE Microsoft and libpng multiple products PNG large image width overflow attempt
- [ ] FILE-IMAGE Microsoft PNG large colour depth download attempt
- [x] NETBIOS SMB Trans2 QUERY_FILE_INFO andx attempt
- [x] NETBIOS SMB-DS Trans2 QUERY_FILE_INFO andx attempt
- [x] NETBIOS SMB Trans2 FIND_FIRST2 andx attempt
- [x] NETBIOS SMB-DS Trans2 FIND_FIRST2 andx attempt
- [ ] OS-WINDOWS Microsoft Windows SMB Trans2 FIND_FIRST2 response andx overflow attempt
- [ ] OS-WINDOWS Microsoft Windows WINS overflow attempt
- [ ] NETBIOS SMB NT Trans NT CREATE andx oversized Security Descriptor attempt
- [ ] NETBIOS SMB NT Trans NT CREATE unicode andx oversized Security Descriptor attempt
- [ ] NETBIOS SMB-DS NT Trans NT CREATE andx oversized Security Descriptor attempt
- [ ] NETBIOS SMB-DS NT Trans NT CREATE unicode andx oversized Security Descriptor attempt
- [ ] NETBIOS SMB NT Trans NT CREATE andx SACL overflow attempt
- [ ] NETBIOS SMB NT Trans NT CREATE unicode andx SACL overflow attempt
- [ ] NETBIOS SMB-DS NT Trans NT CREATE andx SACL overflow attempt
- [ ] NETBIOS SMB-DS NT Trans NT CREATE unicode andx SACL overflow attempt
- [ ] NETBIOS SMB NT Trans NT CREATE andx DACL overflow attempt
- [ ] NETBIOS SMB NT Trans NT CREATE unicode andx DACL overflow attempt
- [ ] NETBIOS SMB-DS NT Trans NT CREATE andx DACL overflow attempt
- [ ] NETBIOS SMB-DS NT Trans NT CREATE unicode andx DACL overflow attempt
- [ ] NETBIOS SMB NT Trans NT CREATE andx invalid SACL ace size dos attempt
- [ ] NETBIOS SMB NT Trans NT CREATE unicode andx invalid SACL ace size dos attempt
- [ ] NETBIOS SMB-DS NT Trans NT CREATE andx invalid SACL ace size dos attempt
- [ ] NETBIOS SMB-DS NT Trans NT CREATE unicode andx invalid SACL ace size dos attempt
- [ ] NETBIOS SMB NT Trans NT CREATE andx invalid SACL ace size dos attempt
- [ ] NETBIOS SMB NT Trans NT CREATE unicode andx invalid SACL ace size dos attempt
- [ ] NETBIOS SMB-DS NT Trans NT CREATE andx invalid SACL ace size dos attempt
- [ ] NETBIOS SMB-DS NT Trans NT CREATE unicode andx invalid SACL ace size dos attempt
- [ ] APP-DETECT distccd remote command execution attempt
- [ ] MALWARE-BACKDOOR Vampire 1.2 connection request
- [ ] PROTOCOL-IMAP append literal overflow attempt
- [ ] PROTOCOL-IMAP examine literal overflow attempt
- [ ] PROTOCOL-IMAP fetch overflow attempt
- [ ] PROTOCOL-IMAP STATUS overflow attempt
- [ ] PROTOCOL-IMAP SUBSCRIBE overflow attempt
- [ ] PROTOCOL-IMAP UNSUBSCRIBE overflow attempt
- [ ] PROTOCOL-NNTP Microsoft Windows SEARCH pattern overflow attempt
- [ ] SERVER-OTHER Unreal Tournament secure overflow attempt
- [x] MALWARE-BACKDOOR Y3KRAT 1.5 Connect Client Response
- [ ] SERVER-OTHER Veritas backup overflow attempt
- [ ] SERVER-WEBAPP 3Com 3CRADSL72 ADSL 11g Wireless Router app_sta.stm access attempt
- [ ] FILE-MULTIMEDIA Nullsoft Winamp cda file name overflow attempt
- [ ] OS-WINDOWS DCERPC NCACN-IP-TCP llsrpc LlsrConnect overflow attempt
- [ ] SERVER-WEBAPP mailman directory traversal attempt
- [ ] FILE-IMAGE Microsoft Multiple Products PNG large image height download attempt
- [x] NETBIOS SMB Trans2 QUERY_FILE_INFO attempt
- [x] NETBIOS SMB-DS Trans2 QUERY_FILE_INFO attempt
- [x] NETBIOS SMB Trans2 FIND_FIRST2 attempt
- [x] NETBIOS SMB-DS Trans2 FIND_FIRST2 attempt
- [ ] OS-WINDOWS Microsoft Windows SMB Trans2 FIND_FIRST2 command response overflow attempt
- [ ] OS-WINDOWS Microsoft Windows SMB-DS Trans2 FIND_FIRST2 response overflow attempt

- [ ] OS-WINDOWS Microsoft Windows SMB-DS Trans2 FIND_FIRST2 response andx overflow attempt
- [ ] OS-WINDOWS Microsoft Windows HTML Help hhctrl.ocx clsid access attempt
- [ ] SERVER-IIS SQLXML content type overflow
- [ ] SQL sa brute force failed login attempt
- [ ] PROTOCOL-DNS UDP inverse query overflow
- [ ] OS-WINDOWS DCERPC NCACN-IP-TCP ISystemActivator CoGetInstanceFromFile attempt
- [ ] OS-WINDOWS DCERPC NCADG-IP-UDP msqueue function 4 overflow attempt
- [ ] SERVER-IIS .cmd executable file parsing attack
- [ ] OS-WINDOWS name query overflow attempt TCP
- [ ] OS-WINDOWS Microsoft Windows WINS name query overflow attempt TCP
- [ ] SERVER-IIS httpodbc.dll access - nimda
- [ ] OS-WINDOWS Messenger message little endian overflow attempt
- [ ] OS-WINDOWS DCERPC NCACN-IP-TCP irot IrotIsRunning/Revoke overflow attempt
- [ ] SQL sa brute force failed login unicode attempt
- [ ] OS-WINDOWS DCERPC NCACN-IP-TCP ISystemActivator RemoteCreateInstance attempt
- [ ] OS-WINDOWS DCERPC NCACN-IP-TCP IActivation remoteactivation overflow attempt
- [ ] OS-WINDOWS Microsoft Windows TCP print service overflow attempt
- [ ] SERVER-OTHER Arkeia client backup generic info probe
- [ ] SERVER-MYSQL 4.0 root login attempt
- [ ] SERVER-OTHER Arkeia backup client type 84 overflow attempt
- [ ] PROTOCOL-FTP REST with numeric argument
- [ ] BROWSER-IE Microsoft Internet Explorer Content-Encoding overflow attempt
- [ ] SERVER-WEBAPP awstats.pl command execution attempt
- [ ] PROTOCOL-VOIP inbound INVITE message
- [x] FILE-IDENTIFY PDF file download request
- [x] FILE-IDENTIFY BMP file download request
- [x] FILE-IDENTIFY JPEG file download request
- [x] FILE-IDENTIFY Portable Executable binary file download request
- [x] FILE-IDENTIFY Microsoft Compound File Binary v4 file magic detected
- [x] FILE-IDENTIFY OLE document file magic detected
- [x] FILE-IDENTIFY XML file download request
- [x] NETBIOS SMB-DS Trans2 Distributed File System GET_DFS_REFERRAL request
- [ ] SERVER-OTHER multiple products blacknurse ICMP denial of service attempt
- [ ] MALWARE-CNC Win.Trojan.Injector variant outbound connection
- [x] FILE-IDENTIFY Microsoft Client Agent Helper JAR file download request
- [x] FILE-IDENTIFY JAR/ZIP file magic detected
- [x] FILE-IDENTIFY JAR/ZIP file magic detected
- [x] FILE-IDENTIFY JAR/ZIP file magic detected
- [x] FILE-IDENTIFY PNG file magic detected
- [x] FILE-IDENTIFY JPEG file magic detected
- [x] FILE-IDENTIFY PDF file magic detected
- [x] FILE-IDENTIFY Microsoft Windows EMF metafile file attachment detected
- [x] FILE-IDENTIFY DIB file download request
- [x] FILE-IDENTIFY JPEG file download request
- [x] FILE-IDENTIFY JPEG file download request
- [x] FILE-IDENTIFY PDF file attachment detected
- [ ] MALWARE-CNC User-Agent known malicious user-agent string DataCha0s
- [x] MALWARE-OTHER known malicious FTP quit banner - Goodbye happy r00ting
- [ ] MALWARE-CNC User-Agent known malicious user-agent string Morfeus Scanner
- [x] PROTOCOL-TELNET login buffer overflow attempt
- [ ] BROWSER-IE Microsoft Internet Explorer malformed object type overflow attempt
- [ ] PROTOCOL-FINGER / execution attempt
- [ ] PROTOCOL-DNS TCP inverse query overflow
- [ ] MALWARE-BACKDOOR BackOrifice 2000 Inbound Traffic
- [ ] OS-WINDOWS DCERPC NCADG-IP-UDP ISystemActivator CoGetInstanceFromFile attempt
- [ ] OS-WINDOWS Microsoft Windows Media Player directory traversal via Content-Disposition attempt
- [ ] SERVER-IIS .bat executable file parsing attack
- [ ] OS-WINDOWS name query overflow attempt UDP
- [ ] OS-WINDOWS Microsoft Windows WINS name query overflow attempt UDP
- [ ] OS-WINDOWS DCERPC NCACN-IP-TCP winreg OpenKey overflow attempt
- [ ] OS-WINDOWS Messenger message overflow attempt
- [ ] OS-WINDOWS DCERPC NCADG-IP-UDP irot IrotIsRunning/Revoke overflow attempt
- [x] PROTOCOL-TELNET login buffer non-evasive overflow attempt
- [ ] OS-WINDOWS DCERPC NCADG-IP-UDP ISystemActivator RemoteCreateInstance attempt
- [ ] PROTOCOL-FTP PORT bounce attempt
- [ ] SERVER-OTHER Arkeia client backup system info probe
- [ ] SERVER-OTHER Bontago Game Server Nickname buffer overflow
- [ ] SERVER-OTHER Arkeia backup client type 77 overflow attempt
- [ ] PUA-P2P Manolito Search Query
- [ ] SERVER-MAIL Content-Type overflow attempt
- [ ] SERVER-WEBAPP awstats access
- [x] FILE-OFFICE Microsoft Windows RTF file with embedded object package download attempt
- [x] FILE-IDENTIFY RTF file download request
- [x] FILE-IDENTIFY Microsoft Office Word file download request
- [ ] MALWARE-CNC Win.Trojan.Hydraq variant outbound connection
- [x] FILE-IDENTIFY JPEG file download request
- [x] FILE-IDENTIFY Microsoft Compound File Binary v3 file magic detected
- [x] FILE-IDENTIFY JPEG file download request
- [x] FILE-IDENTIFY PNG file download request
- [x] NETBIOS SMB TRANS2 Find_First2 request attempt
- [x] FILE-IDENTIFY ZIP archive file download request
- [ ] MALWARE-CNC Win.Trojan.Derusbi.A variant outbound connection
- [x] FILE-IDENTIFY SMI file download request
- [x] FILE-IDENTIFY JAR/ZIP file magic detected
- [x] FILE-IDENTIFY JAR/ZIP file magic detected
- [x] FILE-IDENTIFY JAR/ZIP file magic detected
- [x] FILE-IDENTIFY JAR/ZIP file magic detected
- [x] FILE-IDENTIFY JPEG file magic detection
- [x] FILE-IDENTIFY RTF file magic detected
- [x] FILE-IDENTIFY JAR file download request
- [x] FILE-IDENTIFY Microsoft Windows EMF metafile file attachment detected
- [x] FILE-IDENTIFY SAMI file download request
- [x] FILE-IDENTIFY JPEG file download request
- [x] FILE-IDENTIFY PDF file attachment detected
- [ ] MALWARE-CNC Win.Trojan.Betad variant outbound connection
- [x] MALWARE-OTHER known malicious FTP login banner - 0wns j0
- [ ] MALWARE-CNC URI - known scanner tool muieblackcat
- [ ] POLICY-OTHER TRENDnet IP Camera anonymous access attempt

- [x] FILE-IDENTIFY XSL file download request
- [x] FILE-IDENTIFY XSL file attachment detected
- [x] FILE-IDENTIFY XSLT file attachment detected
- [x] FILE-IDENTIFY XML download detected
- [ ] SERVER-WEBAPP Remote Execution Backdoor Attempt Against Horde
- [x] FILE-IDENTIFY paq8o file attachment detected
- [ ] FILE-PDF hostile PDF associated with Laik exploit kit
- [ ] MALWARE-CNC URI request for known malicious URI - base64 encoded
- [ ] MALWARE-CNC User-Agent known malicious user-agent string core-project
- [ ] EXPLOIT-KIT Blackhole exploit kit landing page with specific structure - prototype catch
- [x] FILE-IDENTIFY XML file attachment detected
- [ ] MALWARE-CNC Win.Trojan.Bredolab variant outbound connection
- [x] FILE-IDENTIFY PNG file attachment detected
- [x] FILE-IDENTIFY SMI file attachment detected
- [x] FILE-IDENTIFY SAMI file attachment detected
- [x] FILE-IDENTIFY ANI file download request
- [x] FILE-IDENTIFY ANI file attachment detected
- [x] FILE-IDENTIFY JPG file attachment detected
- [x] FILE-IDENTIFY JPG file attachment detected
- [x] FILE-IDENTIFY JPG file attachment detected
- [x] FILE-IDENTIFY JPG file attachment detected
- [x] FILE-IDENTIFY JPG file attachment detected
- [x] FILE-IDENTIFY JPG file attachment detected
- [x] FILE-IDENTIFY RTF file attachment detected
- [ ] SERVER-WEBAPP System variable directory traversal attempt - %ALLUSERSPROFILE%
- [ ] SERVER-WEBAPP System variable directory traversal attempt - %APPDATA%
- [ ] SERVER-WEBAPP System variable directory traversal attempt - %COMMONPROGRAMFILES - x86%
- [ ] SERVER-WEBAPP System variable directory traversal attempt - %HOMEDRIVE%
- [ ] SERVER-WEBAPP System variable directory traversal attempt - %LOCALAPPDATA%
- [ ] SERVER-WEBAPP System variable directory traversal attempt - %PROGRAMFILES - X86%
- [ ] SERVER-WEBAPP System variable directory traversal attempt - %SystemRoot%
- [ ] SERVER-WEBAPP System variable directory traversal attempt - %TMP%
- [ ] SERVER-WEBAPP System variable directory traversal attempt - %USERNAME%
- [ ] SERVER-WEBAPP System variable directory traversal attempt - %WINDIR%
- [ ] SERVER-WEBAPP System variable directory traversal attempt - %PSModulePath%
- [ ] SERVER-WEBAPP System variable in URI attempt - %LOGONSERVER%
- [ ] SERVER-WEBAPP System variable in URI attempt - %PATHEXT%
- [ ] SERVER-WEBAPP System variable in URI attempt - %USERDOMAIN%
- [ ] MALWARE-CNC TDS Sutra - request in.cgi
- [ ] MALWARE-OTHER TDS Sutra - HTTP header redirecting to a SutraTDS
- [ ] MALWARE-OTHER TDS Sutra - redirect received
- [x] FILE-IDENTIFY ZIP file attachment detected
- [x] FILE-IDENTIFY Portable Executable file attachment detected
- [x] FILE-IDENTIFY XM file download request
- [x] FILE-IDENTIFY XM file attachment detected
- [x] MALWARE-OTHER Alureon - Malicious IFRAME load attempt
- [ ] PROTOCOL-FTP Multiple Products FTP MKD buffer overflow attempt
- [ ] INDICATOR-OBFUSCATION hex escaped characters in setTimeout call
- [x] FILE-IDENTIFY XSL file attachment detected
- [x] FILE-IDENTIFY XSLT file download request
- [x] FILE-IDENTIFY XSLT file attachment detected
- [ ] MALWARE-CNC User-Agent ASafaWeb Scan
- [x] FILE-IDENTIFY paq8o file download request
- [x] FILE-IDENTIFY paq8o file attachment detected
- [ ] EXPLOIT-KIT Blackhole exploit kit JavaScript carat string splitting with hostile applet
- [ ] MALWARE-CNC Win.Trojan.TDSS variant outbound connection
- [x] FILE-IDENTIFY XML file magic detected
- [x] FILE-IDENTIFY XML file magic detected
- [x] FILE-IDENTIFY XML file attachment detected
- [x] FILE-IDENTIFY PNG file attachment detected
- [ ] EXPLOIT-KIT Blackhole exploit kit landing page with specific structure - prototype catch
- [x] FILE-IDENTIFY SMI file attachment detected
- [x] FILE-IDENTIFY SAMI file attachment detected
- [x] FILE-IDENTIFY ANI file attachment detected
- [x] FILE-IDENTIFY ANI file magic detection
- [x] FILE-IDENTIFY JPG file attachment detected
- [x] FILE-IDENTIFY JPG file attachment detected
- [x] FILE-IDENTIFY JPG file attachment detected
- [x] FILE-IDENTIFY JPG file attachment detected
- [x] FILE-IDENTIFY JPG file attachment detected
- [x] FILE-IDENTIFY JPG file attachment detected
- [x] FILE-IDENTIFY JPG file attachment detected
- [x] FILE-IDENTIFY RTF file attachment detected
- [ ] SERVER-WEBAPP System variable directory traversal attempt - %PROGRAMDATA%
- [ ] SERVER-WEBAPP System variable directory traversal attempt - %COMMONPROGRAMFILES%
- [ ] SERVER-WEBAPP System variable directory traversal attempt - %COMSPEC%
- [ ] SERVER-WEBAPP System variable directory traversal attempt - %HOMEPATH%
- [ ] SERVER-WEBAPP System variable directory traversal attempt - %PROGRAMFILES%
- [ ] SERVER-WEBAPP System variable directory traversal attempt - %SystemDrive%
- [ ] SERVER-WEBAPP System variable directory traversal attempt - %TEMP%
- [ ] SERVER-WEBAPP System variable directory traversal attempt - %USERDATA%
- [ ] SERVER-WEBAPP System variable directory traversal attempt - %USERPROFILE%
- [ ] SERVER-WEBAPP System variable directory traversal attempt - %PUBLIC%
- [ ] SERVER-WEBAPP System variable in URI attempt - %COMPUTERNAME%
- [ ] SERVER-WEBAPP System variable in URI attempt - %PATH%
- [ ] SERVER-WEBAPP System variable in URI attempt - %PROMPT%
- [ ] MALWARE-OTHER TDS Sutra - redirect received
- [ ] MALWARE-OTHER TDS Sutra - page redirecting to a SutraTDS
- [ ] MALWARE-OTHER TDS Sutra - request hi.cgi
- [x] FILE-IDENTIFY ZIP file attachment detected
- [x] FILE-IDENTIFY Portable Executable file attachment detected
- [x] FILE-IDENTIFY EMF file magic detected
- [x] FILE-IDENTIFY XM file attachment detected
- [x] FILE-IDENTIFY XM file magic detected
- [ ] SERVER-WEBAPP PHP-CGI remote file include attempt
- [ ] INDICATOR-COMPROMISE script before DOCTYPE possible malicious redirect attempt
- [ ] INDICATOR-OBFUSCATION hex escaped characters in addEventListener call

- [ ] MALWARE-CNC Win.Trojan.ZeroAccess outbound connection
- [ ] INDICATOR-OBFUSCATION known packer routine with secondary obfuscation
- [ ] INDICATOR-OBFUSCATION JavaScript built-in function parseInt appears obfuscated - likely packer or encoder
- [x] FILE-IDENTIFY JAR/ZIP file magic detected
- [x] FILE-IDENTIFY JAR/ZIP file magic detected
- [x] FILE-IDENTIFY JAR/ZIP file magic detected
- [x] FILE-IDENTIFY JAR/ZIP file magic detected
- [x] FILE-IDENTIFY JAR/ZIP file magic detected
- [x] FILE-IDENTIFY JAR/ZIP file magic detected
- [x] FILE-IDENTIFY PNG file magic detected
- [x] FILE-IDENTIFY JPEG file magic detected
- [x] FILE-IDENTIFY RTF file magic detected
- [x] FILE-IDENTIFY PDF file magic detected
- [x] FILE-IDENTIFY Microsoft Compound File Binary v3 file magic detected
- [x] FILE-IDENTIFY Microsoft Compound File Binary v4 file magic detected
- [x] FILE-IDENTIFY OLE Document file magic detected
- [x] FILE-IDENTIFY Portable Executable binary file magic detected
- [x] FILE-IDENTIFY XML file magic detected
- [x] FILE-IDENTIFY XML file magic detected
- [x] FILE-IDENTIFY EMF file magic detected
- [x] FILE-IDENTIFY XM file magic detected
- [x] MALWARE-CNC Win.Trojan.Magania variant outbound connection
- [x] MALWARE-OTHER Possible malicious redirect - rebots.php
- [x] MALWARE-OTHER malicious redirection attempt
- [ ] OS-MOBILE Android/Fakelash.A!tr.spy trojan command and control channel traffic
- [ ] INDICATOR-COMPROMISE IP only webpage redirect attempt
- [ ] INDICATOR-COMPROMISE IP only webpage redirect attempt
- [x] MALWARE-OTHER Malicious UA detected on non-standard port
- [x] OS-WINDOWS Microsoft Windows SMB NTLM NULL session attempt
- [x] FILE-IDENTIFY JPEG file magic detected
- [x] FILE-IDENTIFY JPEG file magic detected
- [x] FILE-IDENTIFY JPEG file magic detected
- [x] FILE-IDENTIFY JPEG file magic detected
- [ ] POLICY-SPAM 1.usa.gov URL in email, possible spam redirect
- [ ] MALWARE-CNC Potential Banking Trojan Config File Download
- [ ] MALWARE-CNC Win.Trojan.Dorkbot variant outbound connection
- [x] NETBIOS SMB Trans2 FIND_FIRST2 find file and directory info request
- [ ] MALWARE-CNC Win.Trojan.Zeus variant outbound connection
- [ ] MALWARE-CNC ZeroAccess Clickserver callback
- [ ] MALWARE-CNC User-Agent known malicious user agent - NewBrandTest
- [ ] MALWARE-CNC Win.Trojan.ZeroAccess URI and Referer
- [ ] MALWARE-CNC Win.Worm.Gamarue variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Skintrim variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Rombrast variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.BancosBanload variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Buterat variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Buzus variant outbound connection
- [x] MALWARE-OTHER Request for a non-legit postal receipt
- [x] APP-DETECT Acunetix web vulnerability scan attempt
- [ ] APP-DETECT Acunetix web vulnerability scanner probe attempt
- [ ] APP-DETECT Acunetix web vulnerability scanner authentication attempt
- [ ] APP-DETECT Acunetix web vulnerability scanner RFI attempt
- [ ] APP-DETECT Acunetix web vulnerability scanner base64 XSS attempt
- [ ] APP-DETECT Acunetix web vulnerability scanner URI injection attempt
- [ ] APP-DETECT Acunetix web vulnerability scanner prompt XSS attempt
- [ ] APP-DETECT Acunetix web vulnerability scanner XSS attempt
- [ ] MALWARE-CNC Pushdo Spiral Traffic
- [ ] MALWARE-CNC Necurs Rootkit sba.cgi
- [ ] MALWARE-CNC Necurs Rootkit op.cgi
- [ ] MALWARE-CNC Win.Trojan.Symmi variant outbound connection
- [x] FILE-IDENTIFY Portable Executable download detected
- [x] FILE-IDENTIFY Portable Executable download detected
- [x] FILE-IDENTIFY Portable Executable binary file magic detected
- [ ] OS-MOBILE Apple iPod User-Agent detected
- [ ] OS-MOBILE Apple iPad User-Agent detected
- [ ] OS-MOBILE Apple iPhone User-Agent detected
- [ ] OS-MOBILE Android User-Agent detected
- [ ] OS-MOBILE Nokia User-Agent detected
- [ ] OS-MOBILE Samsung User-Agent detected
- [ ] OS-MOBILE Kindle User-Agent detected
- [ ] OS-OTHER Nintendo User-Agent detected
- [ ] MALWARE-CNC Win.Rootkit.Necurs possible URI with encrypted POST
- [x] MALWARE-OTHER Fake postal receipt HTTP Response phishing attack
- [x] MALWARE-OTHER Fake bookinginfo HTTP Response phishing attack
- [x] MALWARE-OTHER Fake bookingdetails HTTP Response phishing attack
- [ ] SERVER-OTHER libupnp command buffer overflow attempt
- [ ] MALWARE-CNC Win.Trojan.Reventon variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Kryptic variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Medfos variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Fakeavlock variant outbound connection
- [ ] MALWARE-CNC Trojan Agent YEH variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Bancos variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Urausy Botnet variant outbound connection
- [ ] MALWARE-CNC Trojan Banker FTC variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Zeus variant outbound connection - MSIE7 No Referer No Cookie
- [ ] APP-DETECT Ammyy remote access tool
- [x] EXPLOIT-KIT redirection to driveby download
- [x] MALWARE-CNC Win.Trojan.Zebrocy outbound data connection
- [x] EXPLOIT-KIT Sibhost exploit kit
- [ ] MALWARE-CNC Win.Trojan.Zbot variant in.php outbound connection
- [ ] MALWARE-CNC Win.Trojan.Wecod variant outbound connection
- [x] FILE-IDENTIFY ZIP file download detected
- [x] FILE-IDENTIFY ZIP file attachment detected
- [ ] MALWARE-CNC Bancos variant outbound connection SQL query POST data
- [ ] MALWARE-CNC Win.Trojan.Zeus variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Gupd variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Eldorado variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Proxyier variant outbound connection
- [x] FILE-IDENTIFY JPEG file magic detected
- [x] MALWARE-OTHER Fake postal receipt HTTP Response phishing attack
- [x] MALWARE-CNC Dapato banking Trojan variant outbound connection
- [x] SERVER-WEBAPP DD-WRT httpd cgi-bin remote command execution attempt
- [ ] SERVER-WEBAPP Linksys E1500/E2500 apply.cgi submit_button page redirection attempt
- [ ] SERVER-WEBAPP Linksys E1500/E2500 apply.cgi submit_button page redirection attempt
- [ ] SERVER-WEBAPP Linksys E1500/E2500 apply.cgi unauthenticated password reset attempt

- [ ] SERVER-WEBAPP Linksys E1500/E2500 apply.cgi unauthenticated password reset attempt
- [ ] APP-DETECT Absolute Software Computrace outbound connection - search.namequery.com
- [ ] MALWARE-CNC Daws Trojan Outbound Plaintext over SSL Port
- [ ] MALWARE-CNC Win.Trojan.Scar variant outbound connection
- [ ] MALWARE-CNC FBI Ransom Trojan variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Bancos variant outbound connection - ksa.txt
- [ ] MALWARE-OTHER UTF-8 BOM in zip file attachment detected
- [ ] MALWARE-OTHER UTF-8 BOM in zip file attachment detected
- [ ] MALWARE-CNC Win.Trojan.Gamarue variant outbound connection
- [ ] MALWARE-OTHER Win.Worm.Dorkbot folder snkb0ptz creation attempt SMB
- [ ] MALWARE-OTHER Win.Worm.Dorkbot Desktop.ini snkb0ptz.exe creation attempt SMB
- [ ] SERVER-ORACLE Oracle WebCenter FatWire Satellite Server header injection on blobheadername2 attempt
- [x] MALWARE-OTHER Win.Trojan.Zeus Spam 2013 dated zip/exe HTTP Response - potential malware download
- [ ] MALWARE-CNC Unknown Thinner Encrypted POST botnet C&C
- [ ] MALWARE-CNC User-Agent known malicious user agent NOKIAN95/ WEB
- [ ] INDICATOR-COMPROMISE Unix.Backdoor.Cdorked redirect attempt
- [x] EXPLOIT-KIT Stamp exploit kit portable executable download
- [ ] MALWARE-CNC User-Agent known Malicious user agent Brutus AET
- [ ] MALWARE-CNC Win.Trojan.Zeus variant outbound connection
- [ ] MALWARE-CNC Harakit botnet traffic
- [ ] MALWARE-CNC User-Agent known malicious user agent Opera 10
- [ ] MALWARE-CNC Win.Trojan.Kazy/FakeAV Checkin with IE6 User-Agent
- [ ] MALWARE-CNC Medfos Trojan variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Travnet Botnet data upload
- [ ] BROWSER-WEBKIT Possible Google Chrome Plugin install from non-trusted source
- [x] MALWARE-OTHER Fake delivery information phishing attack
- [ ] MALWARE-CNC Cbeplay Ransomware variant outbound connection - Abnormal HTTP Headers
- [x] MALWARE-OTHER Compromised Website response - leads to Exploit Kit
- [ ] MALWARE-CNC Win.Trojan.BlackRev rev 1 outbound traffic
- [ ] MALWARE-CNC Win.Trojan.BlackRev rev 3 outbound traffic
- [ ] MALWARE-CNC Win.Trojan.Kbot variant outbound connection
- [ ] MALWARE-CNC Trojan Downloader7
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc stop command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc sleep command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc loginpost command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc syn command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc udpdata command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc icmp command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc dataget command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc dns command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc resolve command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc range command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc download command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc slowhttp command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc full command
- [ ] MALWARE-CNC Win.Trojan.Blocker variant outbound connection HTTP Header Structure
- [ ] MALWARE-CNC Win.Trojan.Cridex encrypted POST check-in
- [ ] MALWARE-CNC XP Fake Antivirus Payment Page Request
- [ ] APP-DETECT Absolute Software Computrace outbound connection - search.dnssearch.org
- [ ] MALWARE-CNC Brontok Worm variant outbound connection
- [ ] MALWARE-CNC file path used as User-Agent - potential Trojan
- [ ] MALWARE-CNC OSX.Trojan.Flashfake variant outbound connection
- [ ] INDICATOR-COMPROMISE IP address check to dyndns.org detected
- [ ] MALWARE-CNC Win.Trojan.Bancos variant outbound connection - op POST
- [ ] MALWARE-OTHER UTF-8 BOM in zip file attachment detected
- [ ] APP-DETECT Ufasoft bitcoin miner possible data upload
- [ ] INDICATOR-COMPROMISE IP address check to j.maxmind.com detected
- [ ] MALWARE-OTHER Win.Worm.Dorkbot executable snkb0ptz.exe creation attempt SMB
- [ ] MALWARE-CNC Win.Trojan.Magic variant inbound connection
- [ ] SERVER-ORACLE Oracle WebCenter FatWire Satellite Server header injection on blobheadername2 attempt
- [ ] MALWARE-CNC Win.Trojan.Zbot fake PNG config file download without User-Agent
- [ ] SERVER-WEBAPP JavaScript tag in User-Agent field possible XSS attempt
- [x] EXPLOIT-KIT Portable Executable downloaded with bad DOS stub
- [ ] MALWARE-CNC Unknown malware - Incorrect headers - Referer HTTP/1.0
- [ ] PUA-ADWARE Win.Adware.BProtector browser hijacker dll list download attempt
- [ ] MALWARE-CNC Win.Trojan.Bancos variant outbound connection - getcomando POST data
- [ ] EXPLOIT-KIT Nuclear exploit kit Spoofed Host Header .com- requests
- [ ] MALWARE-CNC Potential hostile executable served from compromised or malicious WordPress site attempt
- [ ] MALWARE-CNC Win.Trojan.Kazy/FakeAV Checkin with IE6 User-Agent
- [ ] INDICATOR-COMPROMISE config.inc.php in iframe
- [x] MALWARE-BACKDOOR Win.Backdoor.PCRat data upload
- [ ] MALWARE-CNC Win.Trojan.Shiz variant outbound connection
- [ ] BROWSER-FIREFOX Possible Mozilla Firefox Plugin install from non-Mozilla source
- [ ] MALWARE-CNC Win.Trojan.Namihno variant outbound request
- [ ] MALWARE-CNC Cbeplay Ransomware variant outbound connection - POST Body
- [ ] MALWARE-CNC Kazy Trojan check-in
- [ ] MALWARE-CNC Win.Trojan.BlackRev rev 2 outbound traffic
- [ ] MALWARE-CNC Win.Trojan.Kbot variant outbound connection
- [ ] MALWARE-CNC Bancos fake JPG encrypted config file download
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc http command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc die command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc simple command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc datapost command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc udp command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc data command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc tcpdata command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc connect command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc exec command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc antiddos command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc ftp command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc fastddos command
- [ ] MALWARE-CNC Win.Trojan.BlackRev cnc allhttp command
- [ ] MALWARE-CNC Win.Worm.Luder variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Blocker variant outbound connection POST
- [ ] MALWARE-CNC cridex HTTP Response - default0.js
- [ ] MALWARE-CNC XP Fake Antivirus Check-in

- [ ] EXPLOIT-KIT Blackholev2 exploit kit Initial Gate from Linked-In Mailing Campaign
- [ ] MALWARE-CNC RDN Banker POST variant outbound connection
- [ ] MALWARE-CNC BitBot Idle C2 response
- [x] MALWARE-BACKDOOR Win.Backdoor.Boda Malware Checkin
- [ ] MALWARE-CNC Win.Trojan.Rombrast Trojan outbound connection
- [ ] MALWARE-CNC Win.Trojan.Zeus variant outbound connection
- [ ] SQL generic convert injection attempt - GET parameter
- [ ] EXPLOIT-KIT DotkaChef/Rmayana/DotCache exploit kit inbound java exploit download
- [x] EXPLOIT-KIT DotkaChef/Rmayana/DotCache exploit kit Malvertising Campaign URI request
- [ ] MALWARE-CNC Win32/Autorun.JN variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Gozi Trojan Data Theft POST URL
- [ ] MALWARE-CNC Win.Trojan.Injector Info Stealer Trojan variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Dapato variant inbound response connection
- [x] EXPLOIT-KIT Styx exploit kit plugin detection connection jorg
- [x] EXPLOIT-KIT Styx exploit kit plugin detection connection jovf
- [ ] MALWARE-CNC Win.Trojan.Blocker Download
- [x] EXPLOIT-KIT Unknown Malvertising exploit kit Hostile Jar pipe.class
- [x] EXPLOIT-KIT Blackholev2/Cool exploit kit outbound portable executable request
- [x] EXPLOIT-KIT Private exploit kit outbound traffic
- [ ] MALWARE-CNC Win.Trojan.Meredrop variant outbound connection POST Request
- [ ] INDICATOR-COMPROMISE Apache auto_prepend_file a.control.bin C2 traffic
- [x] MALWARE-OTHER Mac OSX FBI ransomware
- [ ] MALWARE-CNC Win.Trojan.ZeroAccess 111-byte URL variant outbound connection
- [ ] MALWARE-CNC Yakes Trojan HTTP Header Structure
- [ ] MALWARE-CNC Win.Trojan.Kryptik Drive-by Download Malware
- [ ] MALWARE-CNC Potential Win.Trojan.Kraziomel Download - 000.jpg
- [x] MALWARE-OTHER HideMeBetter spam injection variant
- [ ] MALWARE-CNC Win.Trojan.Redyms variant outbound connection
- [ ] MALWARE-CNC Win.Backdoor.Aumlib variant outbound connection
- [ ] MALWARE-CNC Win.Backdoor.Aumlib variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.SpyBanker.ZSL variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.ZeroAccess variant outbound connection
- [ ] MALWARE-CNC Orbit Downloader denial of service update
- [ ] MALWARE-CNC Orbit Downloader denial of service update
- [ ] MALWARE-CNC Win.Trojan.Fareit variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.PRISM variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Bisonha variant outbound connection
- [x] EXPLOIT-KIT Blackholev2/Darkleech exploit kit landing page
- [ ] PROTOCOL-VOIP Excessive number of SIP 4xx responses potential user or password guessing attempt
- [ ] PROTOCOL-VOIP Possible SIP OPTIONS service information gathering attempt
- [ ] PROTOCOL-VOIP Excessive number of SIP 4xx responses potential user or password guessing attempt
- [ ] PUA-ADWARE Vittalia adware - get ads
- [ ] PUA-ADWARE Vittalia adware outbound connection - pre install
- [ ] PUA-TOOLBARS Vittalia adware outbound connection - offers
- [x] EXPLOIT-KIT Sweet Orange exploit kit landing page in.php base64 uri
- [ ] MALWARE-CNC RDN Banker Strange Google Traffic
- [ ] EXPLOIT-KIT Blackholev2 exploit kit Initial Gate from NatPay Mailing Campaign
- [ ] MALWARE-CNC ZeroAccess Encrypted 128-byte POST No Accept Headers
- [ ] MALWARE-CNC Win.Trojan.Rombrast Trojan outbound connection
- [ ] MALWARE-CNC Potential Gozi Trojan HTTP Header Structure
- [ ] EXPLOIT-KIT DotkaChef/Rmayana/DotCache exploit kit inbound java exploit download
- [x] EXPLOIT-KIT DotkaChef/Rmayana/DotCache exploit kit landing page
- [ ] MALWARE-CNC Win.Trojan.Win32 Facebook Secure Cryptor C2
- [ ] MALWARE-CNC Win.Trojan.Gozi Data Theft POST Data
- [ ] MALWARE-CNC Win.Trojan.Pirminay variant outbound connection
- [x] EXPLOIT-KIT Rawin exploit kit outbound java retrieval
- [ ] MALWARE-CNC Win.Trojan.OnlineGameHack variant outbound connection
- [x] EXPLOIT-KIT Styx exploit kit plugin detection connection jlnp
- [ ] MALWARE-CNC User-Agent known malicious user-agent string pb - Htbot
- [ ] INDICATOR-COMPROMISE Unknown ?1 redirect
- [x] EXPLOIT-KIT Unknown Malvertising exploit kit stage-1 redirect
- [x] EXPLOIT-KIT DotkaChef/Rmayana/DotCache exploit kit Zeroaccess download attempt
- [ ] MALWARE-CNC Win.Trojan.Meredrop variant outbound connection GET Request
- [ ] MALWARE-CNC Win.Trojan.Neurevt variant outbound connection
- [ ] MALWARE-CNC Potential Bancos Brazilian Banking Trojan Browser Proxy Autoconfig File
- [ ] MALWARE-CNC Win.Trojan.Gamarue - Mozi1la User-Agent
- [ ] MALWARE-CNC Win.Trojan.Cridex Encrypted POST w/ URL Pattern
- [ ] INDICATOR-COMPROMISE All Numbers .EXE file name from abnormally ordered HTTP headers - Potential Yakes Trojan Download
- [ ] MALWARE-CNC Win.Trojan.Kryptic 7-byte URI Invalid Firefox Headers - no Accept-Language
- [ ] MALWARE-OTHER self-signed SSL certificate with default MyCompany Ltd organization name
- [ ] MALWARE-CNC Win.Trojan.Rovnix malicious download request
- [ ] MALWARE-CNC Fort Disco Registration variant outbound connection
- [ ] MALWARE-CNC Win.Backdoor.Aumlib variant outbound connection
- [ ] MALWARE-CNC Worm.Silly variant outbound connection
- [ ] MALWARE-CNC Brazilian Banking Trojan data theft
- [ ] MALWARE-CNC Win.Ransomware.Urausy outbound connection
- [ ] MALWARE-CNC Orbit Downloader denial of service update
- [ ] MALWARE-CNC RDN Banker Data Exfiltration
- [ ] MALWARE-CNC Win.Trojan.PRISM variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.PRISM variant outbound connection
- [x] EXPLOIT-KIT Blackholev2/Darkleech exploit kit landing page request
- [ ] PROTOCOL-VOIP Possible SIP OPTIONS service information gathering attempt
- [ ] PROTOCOL-VOIP Ghost call attack attempt
- [ ] PROTOCOL-VOIP Ghost call attack attempt
- [ ] EXPLOIT-KIT Blackholev2/Cool exploit kit payload download attempt
- [ ] PUA-ADWARE Vittalia adware - post install
- [ ] PUA-TOOLBARS Vittalia adware outbound connection - Eazel toolbar install
- [ ] MALWARE-CNC Win.Trojan.Zeus variant outbound connection

- [ ] MALWARE-CNC Win.Trojan.Zeus encrypted POST Data exfiltration
- [ ] MALWARE-CNC Win.Trojan.Eupuds variant connection
- [x] MALWARE-CNC Win.Backdoor.Chopper web shell connection
- [ ] MALWARE-CNC Win.Trojan.Kuluoz outbound command
- [ ] MALWARE-CNC BLYPT installer startupkey outbound traffic
- [ ] MALWARE-CNC BLYPT installer configkey outbound traffic
- [ ] MALWARE-CNC BLYPT installer createproc outbound traffic
- [ ] EXPLOIT-KIT Blackholev2 exploit kit landing page
- [ ] MALWARE-CNC Win.Ransomware.Urausy variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.CryptoLocker variant connection
- [ ] MALWARE-CNC Win.Trojan.Napolar data theft
- [ ] MALWARE-CNC Win.Trojan.Banload information upload
- [ ] MALWARE-CNC Win.Trojan.Fareit variant outbound connection - /default.htm GET Encrypted Payload
- [ ] MALWARE-CNC Win.Trojan.Fareit variant outbound connection - /home.htm GET Encrypted Payload
- [ ] MALWARE-CNC Win.Trojan.Fareit variant outbound connection - /login.htm GET Encrypted Payload
- [ ] MALWARE-CNC Win.Trojan.Fareit variant outbound connection - /start.htm GET Encrypted Payload
- [ ] MALWARE-CNC Win.Trojan.Fareit variant outbound connection - /index.htm GET Encrypted Payload
- [ ] MALWARE-CNC Win.Trojan.Conficker variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Foreign variant outbound connection - /html2/
- [ ] MALWARE-CNC Win.Trojan.Foreign variant outbound connection - MSIE 7.2
- [ ] MALWARE-CNC Win.Trojan.Kuluoz Potential Phishing URL
- [ ] EXPLOIT-KIT Blackholev2/Cool exploit kit payload download attempt
- [ ] MALWARE-CNC Win.Trojan.Kuluoz Potential phishing URL
- [ ] EXPLOIT-KIT Blackholev2/Cool exploit kit exploit download attempt
- [x] MALWARE-CNC Win.Backdoor.Chopper web shell connection
- [ ] INDICATOR-OBFUSCATION large number of calls to chr function - possible sql injection obfuscation
- [x] INDICATOR-OBFUSCATION Javascript obfuscation - seen in IFRAMEr Tool attack
- [ ] MALWARE-CNC Win.Trojan.Kazy variant outbound connection
- [x] INDICATOR-OBFUSCATION Javascript obfuscation - fromCharCode - seen in IFRAMEr Tool attack
- [x] EXPLOIT-KIT Glazunov exploit kit outbound jnlp download attempt
- [ ] MALWARE-CNC Win.Trojan.Symmi variant SQL check-in
- [x] MALWARE-CNC DeputyDog diskless method outbound connection
- [ ] MALWARE-CNC Win.Trojan.ZeroAccess Download Headers
- [ ] MALWARE-CNC Win.Trojan.Conficker variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Fareit variant outbound connection - /main.htm GET Encrypted Payload
- [ ] MALWARE-OTHER SQL Slammer worm propagation attempt inbound
- [ ] PROTOCOL-DNS Malformed DNS query with HTTP content
- [x] EXPLOIT-KIT Goon/Infinity exploit kit payload download attempt
- [ ] MALWARE-CNC Win.Trojan.Bancos outbound connection
- [ ] MALWARE-CNC Win.Trojan.Injector outbound connection
- [ ] INDICATOR-COMPROMISE potential malware download - single digit .exe file download
- [ ] MALWARE-CNC Win.Trojan.Dofoil inbound connection
- [ ] MALWARE-CNC Win.Trojan.Gozi/Neverquest variant outbound connection
- [x] MALWARE-CNC Win.Backdoor.Iniduoh variant outbound connection
- [ ] MALWARE-CNC User-Agent known malicious user-agent z00sAgent - Win.Trojan.Zbot
- [ ] MALWARE-CNC Win.Trojan.Symmi variant network connectivity check
- [ ] MALWARE-CNC Win.Trojan.Fakeav variant outbound data connection
- [ ] INDICATOR-COMPROMISE exe.exe download
- [x] EXPLOIT-KIT HiMan exploit kit outbound payload retreival - specific string
- [ ] MALWARE-CNC Win.Trojan.Gh0st variant outbound connection
- [x] MALWARE-CNC Win.Backdoor.Chopper web shell connection
- [x] MALWARE-CNC Win.Backdoor.Chopper web shell connection
- [ ] MALWARE-OTHER Win.Trojan.Kuluoz outbound download request
- [ ] MALWARE-CNC BLYPT installer reuse outbound traffic
- [ ] MALWARE-CNC BLYPT installer tserror outbound traffic
- [ ] MALWARE-CNC Win.Trojan.Bancos variant outbound connection
- [ ] EXPLOIT-KIT Blackholev2/Cool exploit kit exploit download attempt
- [ ] MALWARE-CNC Win.Trojan.Caphaw variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Napolar variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Banload variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Banload download
- [ ] MALWARE-CNC Win.Trojan.Fareit variant outbound connection - /file.htm GET Encrypted Payload
- [ ] MALWARE-CNC Win.Trojan.Fareit variant outbound connection - /install.htm GET Encrypted Payload
- [ ] MALWARE-CNC Win.Trojan.Fareit variant outbound connection - /search.htm GET Encrypted Payload
- [ ] MALWARE-CNC Win.Trojan.Fareit variant outbound connection - /welcome.htm GET Encrypted Payload
- [ ] MALWARE-CNC Win.Trojan.Fareit variant outbound connection - /setup.htm GET Encrypted Payload
- [ ] MALWARE-CNC Win.Trojan.Mevade variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Foreign variant outbound connection - MSIE 7.1
- [ ] PUA-ADWARE Linkury outbound time check
- [ ] SERVER-WEBAPP vBulletin upgrade.php exploit attempt
- [ ] MALWARE-CNC Win.Trojan.KanKan variant connection
- [ ] MALWARE-CNC Win.Trojan.hdog connectivity check-in version 2
- [ ] MALWARE-CNC Win.Trojan.Agent variant connection
- [x] PUA-ADWARE FakeAV runtime detection
- [x] INDICATOR-OBFUSCATION Javascript obfuscation - split - seen in IFRAMEr Tool attack
- [ ] MALWARE-CNC Win.Trojan.Kazy variant outbound connection
- [x] INDICATOR-OBFUSCATION Javascript obfuscation - createElement - seen in IFRAMEr Tool attack
- [x] EXPLOIT-KIT Glazunov exploit kit landing page
- [x] EXPLOIT-KIT Glazunov exploit kit zip file download
- [x] EXPLOIT-KIT Sakura exploit kit exploit payload retrieve attempt
- [ ] MALWARE-CNC Win.Trojan.Asprox/Kuluoz variant connection
- [ ] MALWARE-CNC Win.Trojan.Conficker variant outbound connection
- [ ] INDICATOR-SCAN inbound probing for IPTUX messenger port
- [ ] MALWARE-CNC Win.Trojan.Fareit variant outbound connection - /online.htm GET Encrypted Payload
- [ ] PROTOCOL-DNS DNS query amplification attempt
- [x] EXPLOIT-KIT Nuclear exploit kit payload request
- [ ] MALWARE-CNC Win.Trojan.Zeus outbound connection
- [ ] MALWARE-CNC Win.Trojan.Injector inbound connection
- [ ] MALWARE-CNC Win.Trojan.Palevo outbound connection
- [ ] MALWARE-CNC Win.Trojan.Injector variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Zeus variant outbound connection - MSIE7 No Referer No Cookie
- [ ] MALWARE-CNC Win.Trojan.Gozi/Neverquest variant outbound connection
- [ ] MALWARE-CNC User-Agent known malicious user-agent string - Linux.Trojan.Zollard
- [ ] MALWARE-BACKDOOR Zollard variant outbound connection attempt
- [ ] MALWARE-CNC Win.Trojan.Symmi variant network connectivity check
- [ ] MALWARE-CNC Win.Trojan.Rovnix malicious download
- [ ] MALWARE-CNC Win.Trojan.Alurewo outbound connection
- [ ] MALWARE-CNC Win.Trojan.Agent.DF - Data Exfiltration

- [ ] MALWARE-CNC Win.Trojan.Agent.DF - User-Agent Missing Bracket
- [ ] MALWARE-CNC Win.Trojan.Steckt IRCbot executable download
- [ ] MALWARE-CNC Win.Worm.Steckt IRCbot executable download
- [ ] MALWARE-CNC Win.Worm.Steckt IRCbot variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Banload variant inbound connection
- [x] EXPLOIT-KIT CritX exploit kit payload download attempt
- [ ] MALWARE-CNC User-Agent known malicious user-agent string fortis
- [ ] MALWARE-CNC Win.Trojan.Androm variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Graftor variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Dropper variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Zusy variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Dropper outbound encrypted traffic - potential exfiltration
- [x] FILE-IDENTIFY Adobe AIR file download request
- [x] FILE-IDENTIFY Adobe AIR file attachment detected
- [ ] POLICY-SPAM Potential phishing attack - .zip receipt filename download with .exe name within .zip the same
- [ ] POLICY-SPAM Potential phishing attack - .zip voicemail filename download with .exe name within .zip the same
- [ ] PROTOCOL-ICMP Unusual L3retriever Ping detected
- [ ] PROTOCOL-ICMP Unusual PING detected
- [ ] MALWARE-CNC Win.Trojan.Fexel variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.DomaIQ variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Linkup outbound connection
- [ ] MALWARE-CNC Win.Trojan.Careto outbound connection
- [ ] MALWARE-CNC Win.Trojan.Careto plugin download
- [ ] MALWARE-CNC Win.Trojan.Jackpos outbound connection
- [ ] MALWARE-CNC User-Agent known malicious user agent - TixDll - Win.Trojan.Adload.dyhq
- [x] SERVER-WEBAPP HNAP remote code execution attempt
- [x] SERVER-WEBAPP Linksys E-series HNAP TheMoon remote code execution attempt
- [ ] MALWARE-CNC Win.Trojan.Pirminay variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Kuluoz outbound connection
- [ ] MALWARE-CNC Win.Trojan.Pony HTTP response connection
- [ ] MALWARE-CNC Win.Trojan.Zeus variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Pushdo variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.ExplorerHijack variant outbound connection
- [x] EXPLOIT-KIT Hello/LightsOut exploit kit payload download attempt
- [x] MALWARE-OTHER ANDR.Trojan.iBanking outbound connection attempt
- [x] MALWARE-OTHER ANDR.Trojan.iBanking outbound connection attempt
- [ ] MALWARE-CNC Win.Trojan.Necurs variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Androm variant outbound connection
- [x] EXPLOIT-KIT Nuclear exploit kit outbound payload request
- [ ] MALWARE-CNC Win.Trojan.Strictor HTTP Response - Brazil Geolocated Infected User
- [ ] MALWARE-CNC Win.Trojan.ExplorerHijack variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Strictor variant outbound connection
- [x] PUA-ADWARE Lucky Leap Adware outbound connection
- [ ] MALWARE-CNC Win.Trojan.Glupteba.M initial outbound connection
- [ ] MALWARE-CNC Linux.Trojan.Calfbot outbound connection
- [ ] MALWARE-CNC Win.Trojan.Zbot/Bublik outbound connection
- [x] SERVER-OTHER OpenSSL SSLv3 heartbeat read overrun attempt
- [x] SERVER-OTHER OpenSSL TLSv1.1 heartbeat read overrun attempt
- [x] SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt
- [x] SERVER-OTHER OpenSSL TLSv1.1 large heartbeat response - possible ssl heartbleed attempt
- [ ] MALWARE-CNC Win.Worm.Steckt IRCbot requesting URL through IRC
- [ ] MALWARE-CNC Win.Worm.Steckt IRCbot executable download
- [ ] MALWARE-CNC Win.Worm.Neeris IRCbot variant outbound connection
- [ ] MALWARE-CNC Win.Worm.Steckt IRCbot variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Zeus variant outbound connection
- [x] EXPLOIT-KIT CritX exploit kit payload download attempt
- [x] EXPLOIT-KIT Magnitude exploit kit Microsoft Internet Explorer Payload request
- [ ] MALWARE-CNC Win.Trojan.Strictor variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Graftor variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Graftor variant inbound connection
- [ ] MALWARE-CNC Win.Trojan.Dropper inbound encrypted traffic
- [ ] MALWARE-CNC Win.Trojan.Dropper outbound encrypted traffic
- [x] FILE-IDENTIFY Adobe AIR file attachment detected
- [ ] MALWARE-CNC Win.Trojan.Zeus variant outbound connection
- [ ] POLICY-SPAM Potential phishing attack - .zip shipping filename download with .exe name within .zip the same
- [ ] POLICY-SPAM Potential phishing attack - .zip statement filename download with .exe name within .zip the same
- [ ] PROTOCOL-ICMP Unusual Microsoft Windows Ping detected
- [ ] PROTOCOL-ICMP Unusual Microsoft Windows 7 Ping detected
- [ ] MALWARE-CNC Linux.Backdoor.Shellbot outbound connection
- [ ] MALWARE-CNC Win.Trojan.Graftor variant outbound connection
- [ ] MALWARE-CNC User-Agent known malicious user-agent string MSIE 4.01 - Win.Trojan.Careto
- [ ] MALWARE-CNC Win.Trojan.Careto plugin download
- [ ] MALWARE-CNC Win.Trojan.Careto plugin download
- [ ] MALWARE-CNC Win.Trojan.Jackpos outbound connection
- [ ] MALWARE-CNC Win.Trojan.Adload.dyhq variant outbound connection
- [ ] SERVER-WEBAPP Linksys E-series HNAP TheMoon remote code execution attempt
- [ ] MALWARE-CNC Win.Trojan.Pirminay variant outbout connection
- [x] EXPLOIT-KIT Redkit exploit kit payload request
- [ ] MALWARE-CNC Win.Trojan.Napolar phishing attack
- [ ] MALWARE-CNC Win.Trojan.WEC variant outbound connection
- [ ] MALWARE-CNC User-Agent known malicious user-agent string Updates downloader - Win.Trojan.Upatre
- [ ] MALWARE-CNC Win.Trojan.Bancos variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Tiny variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Androm variant outbound connection
- [x] MALWARE-OTHER ANDR.Trojan.iBanking outbound connection attempt
- [ ] MALWARE-CNC Win.Trojan.Gamut configuration download
- [ ] MALWARE-CNC Win.Trojan.Uroburos usermode-centric client request
- [ ] MALWARE-CNC Win.Trojan.Symmi variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Graftor variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Strictor HTTP Response - Non-Brazil Geolocated Infected User
- [ ] MALWARE-CNC Win.Trojan.Zeus variant outbound connection
- [x] PUA-ADWARE Lucky Leap Adware outbound connection
- [ ] MALWARE-CNC Win.Trojan.Symmi variant outbound connection
- [x] EXPLOIT-KIT Goon/Infinity exploit kit malicious portable executable file request
- [ ] MALWARE-CNC Win.Trojan.Zbot/Bublik inbound connection
- [ ] MALWARE-CNC Win.Trojan.Zbot/Bublik outbound connection
- [x] SERVER-OTHER OpenSSL TLSv1 heartbeat read overrun attempt
- [x] SERVER-OTHER OpenSSL TLSv1.2 heartbeat read overrun attempt
- [x] SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt
- [x] SERVER-OTHER OpenSSL TLSv1.2 large heartbeat response - possible ssl heartbleed attempt

- [x] SERVER-OTHER OpenSSL SSLv3 heartbeat read overrun attempt - vulnerable client response
- [x] SERVER-OTHER OpenSSL TLSv1 heartbeat read overrun attempt - vulnerable client response
- [x] SERVER-OTHER OpenSSL TLSv1.1 heartbeat read overrun attempt - vulnerable client response
- [x] SERVER-OTHER OpenSSL TLSv1.2 heartbeat read overrun attempt - vulnerable client response
- [x] SERVER-OTHER OpenSSL TLSv1.1 heartbeat read overrun attempt
- [x] SERVER-OTHER OpenSSL TLSv1.2 heartbeat read overrun attempt
- [ ] MALWARE-CNC Win.Trojan.Ramdo variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Zeus variant outbound connection
- [x] SERVER-OTHER OpenSSL Heartbleed masscan access exploitation attempt
- [ ] MALWARE-CNC Malicious BitCoiner Miner download - Win.Trojan.Minerd
- [ ] MALWARE-CNC Malicious BitCoiner Miner download - Win.Trojan.Systema
- [ ] MALWARE-CNC Linux.Trojan.Elknot outbound connection
- [x] MALWARE-OTHER Win.Trojan.Agent E-FAX phishing attempt
- [x] MALWARE-OTHER Win.Trojan.Agent E-FAX phishing attempt
- [x] MALWARE-OTHER Win.Trojan.Agent Funeral ceremony phishing attempt
- [ ] MALWARE-CNC Win.Trojan.Zeus variant outbound connection
- [x] SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt
- [x] SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt
- [x] SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt
- [x] SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt
- [ ] SERVER-OTHER OpenSSL TLSv1.1 large heartbeat response - possible ssl heartbleed attempt
- [x] SERVER-OTHER OpenSSL TLSv1.1 large heartbeat response - possible ssl heartbleed attempt
- [x] SERVER-OTHER OpenSSL TLSv1.2 large heartbeat response - possible ssl heartbleed attempt
- [x] SERVER-OTHER OpenSSL TLSv1.2 large heartbeat response - possible ssl heartbleed attempt
- [x] SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt
- [x] SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt
- [ ] SERVER-OTHER OpenSSL TLSv1.1 large heartbeat response - possible ssl heartbleed attempt
- [ ] SERVER-OTHER OpenSSL TLSv1.2 large heartbeat response - possible ssl heartbleed attempt
- [x] FILE-OTHER RARLAB WinRAR ZIP format filename spoof attempt
- [x] FILE-OTHER RARLAB WinRAR ZIP format filename spoof attempt
- [ ] MALWARE-CNC Win.Trojan.SpySmall variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.SpySmall variant outbound connection
- [ ] MALWARE-CNC User-Agent known malicious user agent - User-Agent User-Agent Mozilla
- [ ] MALWARE-CNC Win.Trojan.Bancos variant outbound connection
- [x] EXPLOIT-KIT Multiple exploit kit redirection gate
- [x] MALWARE-BACKDOOR Win.Backdoor.Hikit outbound banner response
- [x] EXPLOIT-KIT CritX exploit kit payload request
- [ ] INDICATOR-COMPROMISE Potential malware download - .doc.exe within .zip file
- [ ] INDICATOR-COMPROMISE Potential malware download - .gif.exe within .zip file
- [ ] INDICATOR-COMPROMISE Potential malware download - .jpeg.exe within .zip file
- [ ] INDICATOR-COMPROMISE Potential malware download - .jpg.exe within .zip file
- [ ] INDICATOR-COMPROMISE Potential malware download - .pdf.exe within .zip file
- [ ] MALWARE-CNC Win.Trojan.Bancos variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.SpyBanker variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.MadnessPro outbound connection
- [ ] MALWARE-CNC Win.Rootkit.Necurs outbound connection
- [ ] MALWARE-CNC Win.Trojan.Zbot variant outbound connection
- [ ] MALWARE-CNC User-Agent known malicious user agent - User-Agent hello crazyk
- [ ] MALWARE-CNC Win.Trojan.Bancos password stealing attempt
- [ ] MALWARE-CNC Win.Trojan.Bancos variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.ZeroAccess inbound connection
- [ ] MALWARE-CNC Win.Trojan.Banker variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Banker variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Necurs variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Kuluoz outbound connection
- [ ] MALWARE-CNC Win.Trojan.Andromeda HTTP proxy response attempt
- [ ] MALWARE-CNC Win.Trojan.Symmi outbound connection
- [ ] MALWARE-CNC Win.Worm.VBNA variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Dyre publickey outbound connection
- [ ] MALWARE-CNC Win.Trojan.Zusy variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.MSIL variant outbound connection
- [ ] SERVER-APACHE Apache Chunked-Encoding worm attempt
- [ ] MALWARE-CNC Win.Trojan.Injector variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.CryptoWall downloader attempt
- [ ] MALWARE-CNC Win.Trojan.CryptoWall outbound connection
- [ ] MALWARE-CNC Win.Trojan.Symmi variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.ChoHeap variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.ChoHeap variant outbound connection
- [ ] EXPLOIT-KIT Rig Exploit Kit Outbound DGA Request
- [ ] MALWARE-CNC Win.Trojan.SDBot variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Androm Click Fraud Request
- [ ] MALWARE-CNC Win.Trojan.Androm Click Fraud Request
- [ ] MALWARE-CNC Win.Trojan.Androm variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Papras variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.HW32 variant spam attempt
- [ ] MALWARE-CNC Win.Trojan.Symmi variant outbound connection
- [x] INDICATOR-COMPROMISE MinerDeploy monitor request attempt
- [ ] MALWARE-CNC Andr.Trojan.SMSSend outbound connection
- [ ] MALWARE-CNC Win.Trojan.Glupteba C&C server HELLO request to client
- [ ] MALWARE-CNC Win.Trojan.Glupteba C&C server READD command to client
- [ ] MALWARE-CNC Win.Trojan.Glupteba C&C server READY command to client
- [ ] MALWARE-CNC Win.Trojan.Glupteba payload download request
- [ ] MALWARE-CNC Win.Trojan.Glupteba client response/authenticate to C&C server
- [ ] MALWARE-CNC Win.Tinybanker variant outbound connection
- [ ] MALWARE-CNC Win.Tinybanker variant outbound connection
- [ ] MALWARE-CNC Andr.Trojan.Scarelocker outbound connection
- [ ] MALWARE-CNC Win.Trojan.Bancos variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Tirabot variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Badur download attempt
- [ ] MALWARE-CNC Win.Trojan.Badur download attempt
- [ ] MALWARE-CNC Win.Trojan.Badur variant outbound connection
- [ ] FILE-IMAGE Microsoft Multiple Products JPEG parser heap overflow attempt
- [ ] MALWARE-CNC Win.Banker.Delf variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Graftor variant outbound connection

- [ ] MALWARE-CNC Win.Trojan.Delf variant HTTP Response
- [x] POLICY-OTHER QLogic Switch 5600/5800 default ftp login attempt
- [x] FILE-IDENTIFY JPEG file magic detection
- [ ] MALWARE-CNC Win.Trojan.Symmi variant HTTP response attempt
- [ ] MALWARE-CNC Win.Trojan.Banker variant outbound connection
- [ ] EXPLOIT-KIT Astrum exploit kit payload delivery
- [x] EXPLOIT-KIT Astrum exploit kit redirection attempt
- [ ] EXPLOIT-KIT Astrum exploit kit payload delivery
- [ ] OS-OTHER Bash CGI environment variable injection attempt
- [x] OS-OTHER Bash CGI environment variable injection attempt
- [x] OS-OTHER Malicious DHCP server bash environment variable injection attempt
- [ ] MALWARE-CNC User-Agent known malicious user-agent string - Treck - Win.Backdoor.Upatre
- [ ] MALWARE-CNC Linux.Backdoor.Flooder inbound connection attempt - command
- [ ] MALWARE-CNC Linux.Backdoor.Flooder outbound connection
- [x] OS-OTHER Bash environment variable injection attempt
- [ ] OS-OTHER Bash environment variable injection attempt
- [ ] MALWARE-CNC Win.Trojan.Asprox inbound connection
- [ ] MALWARE-CNC Win.Trojan.Asprox outbound connection
- [ ] MALWARE-CNC Win.Trojan.Zemot configuration download attempt
- [ ] MALWARE-CNC Win.Trojan.Zemot payload download attempt
- [ ] MALWARE-CNC WIN.Trojan.Plugx variant outbound connection
- [ ] MALWARE-CNC Win.Backdoor.ZxShell connection outgoing attempt
- [ ] MALWARE-CNC Win.Trojan.Graftor variant outbound connection
- [ ] BROWSER-FIREFOX Mozilla 1.0 Javascript arbitrary cookie access attempt
- [x] MALWARE-OTHER Sinkhole reply - irc-sinkhole.cert.pl
- [ ] OS-OTHER Bash CGI environment variable injection attempt
- [ ] MALWARE-CNC Win.Trojan.GameOverZeus variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Androm variant outbound connection
- [x] FILE-IDENTIFY dib file attachment detected
- [ ] MALWARE-CNC Win.Trojan.Symmi variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Geodo variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Sodebral variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Sodebral HTTP Response attempt
- [ ] INDICATOR-COMPROMISE Potential malware download - _pdf.exe within .zip file
- [ ] MALWARE-CNC Win.Trojan.Chopstick variant outbound request
- [ ] MALWARE-CNC Win.Trojan.Wiper variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Darkhotel outbound connection
- [ ] MALWARE-CNC Win.Trojan.Darkhotel outbound connection
- [ ] MALWARE-CNC Win.Trojan.Darkhotel response connection attempt
- [ ] APP-DETECT Absolute Software Computrace outbound connection - absolute.com
- [ ] APP-DETECT Absolute Software Computrace outbound connection - namequery.nettrace.co.za
- [ ] APP-DETECT Absolute Software Computrace outbound connection - search2.namequery.com
- [ ] MALWARE-CNC Win.Trojan.Poolfiend variant outbound connection
- [x] INDICATOR-COMPROMISE Potential Redirect from Compromised WordPress site to Fedex - Spammed Malware Download attempt
- [ ] MALWARE-BACKDOOR Win.Trojan.Wiper inbound communication attempt
- [ ] MALWARE-BACKDOOR Win.Trojan.Wiper download attempt
- [ ] MALWARE-BACKDOOR Win.Trojan.Wiper inbound communication attempt
- [ ] MALWARE-BACKDOOR Win.Trojan.Wiper inbound communication attempt
- [ ] MALWARE-OTHER Win.Trojan.Wiper download attempt
- [ ] MALWARE-OTHER Win.Trojan.Wiper download attempt
- [ ] MALWARE-OTHER Win.Trojan.Wiper listener download attempt
- [ ] MALWARE-OTHER Win.Trojan.Wiper listener download attempt

- [ ] MALWARE-CNC Win.Trojan.Delf variant outbound connection
- [x] POLICY-OTHER QLogic Switch 5600/5800 default ftp login attempt
- [ ] MALWARE-CNC Win.Trojan.Bancos variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Symmi variant outbound connection
- [x] EXPLOIT-KIT Astrum exploit kit landing page
- [ ] EXPLOIT-KIT Astrum exploit kit payload delivery
- [x] EXPLOIT-KIT Astrum exploit kit multiple exploit download request
- [ ] MALWARE-CNC Win.Trojan.Chebri variant outbound connection
- [x] OS-OTHER Bash CGI environment variable injection attempt
- [x] OS-OTHER Bash CGI environment variable injection attempt
- [ ] MALWARE-CNC User-Agent known malicious user-agent string - Install - Win.Backdoor.Upatre
- [x] MALWARE-OTHER Fake Delta Ticket HTTP Response phishing attack
- [ ] MALWARE-CNC Linux.Backdoor.Flooder outbound telnet connection attempt
- [x] OS-OTHER Bash environment variable injection attempt
- [ ] OS-OTHER Bash environment variable injection attempt
- [x] OS-OTHER Bash environment variable injection attempt
- [ ] MALWARE-CNC Win.Trojan.Asprox outbound connection
- [x] OS-OTHER Bash environment variable injection attempt
- [ ] MALWARE-CNC Win.Trojan.Zemot outbound connection
- [ ] MALWARE-CNC Win.Trojan.Bancos variant outbound connection
- [ ] MALWARE-CNC Win.Backdoor.ZxShell connection incoming attempt
- [ ] MALWARE-CNC Win.Trojan.Zxshell variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Cryptowall variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Hydraq.variant outbound detected
- [ ] OS-OTHER Bash CGI environment variable injection attempt
- [ ] OS-OTHER Bash environment variable injection attempt
- [ ] SERVER-OTHER AOL Instant Messenger goaway message buffer overflow attempt
- [x] FILE-IDENTIFY bmp file attachment detected
- [x] EXPLOIT-KIT Nuclear exploit kit outbound structure
- [ ] MALWARE-CNC Win.Trojan.Symmi variant outbound connection
- [ ] MALWARE-CNC Win.Worm.Jenxcus variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Sodebral HTTP Response attempt
- [ ] MALWARE-CNC User-Agent known malicious user-agent string RUpdate
- [ ] MALWARE-CNC Win.Trojan.Chopstick variant outbound request
- [x] MALWARE-CNC Win.Dropper.Ch variant outbound connection
- [ ] MALWARE-CNC FIN4 VBA Macro credentials upload attempt
- [ ] MALWARE-CNC Win.Trojan.Darkhotel variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Darkhotel data upload attempt
- [ ] APP-DETECT Absolute Software Computrace outbound connection - 209.53.113.223
- [ ] APP-DETECT Absolute Software Computrace outbound connection - bh.namequery.com
- [ ] APP-DETECT Absolute Software Computrace outbound connection - search.us.namequery.com
- [ ] APP-DETECT Absolute Software Computrace outbound connection - search64.namequery.com
- [ ] MALWARE-CNC Win.Trojan.Poolfiend variant outbound connection
- [ ] FILE-IMAGE Microsoft and libpng multiple products PNG large image width overflow attempt
- [ ] MALWARE-BACKDOOR Win.Trojan.Wiper outbound communication attempt
- [ ] MALWARE-BACKDOOR Win.Trojan.Wiper download attempt
- [ ] MALWARE-BACKDOOR Win.Trojan.Wiper outbound communication attempt
- [ ] MALWARE-BACKDOOR Win.Trojan.Wiper download attempt
- [ ] MALWARE-OTHER Win.Trojan.Wiper download attempt
- [ ] MALWARE-OTHER Win.Trojan.Wiper listener download attempt
- [ ] MALWARE-OTHER Win.Trojan.Wiper listener download attempt
- [ ] MALWARE-OTHER Win.Trojan.Wiper listener download attempt

- [ ] MALWARE-OTHER Win.Trojan.Wiper listener download attempt
- [ ] MALWARE-OTHER Win.Trojan.Wiper listener download attempt
- [ ] MALWARE-OTHER Win.Trojan.Wiper listener download attempt
- [ ] MALWARE-OTHER Win.Trojan.Wiper listener download attempt
- [ ] MALWARE-OTHER Win.Trojan.Wiper download attempt
- [ ] MALWARE-TOOLS Win.Trojan.Wiper proxy communication attempt
- [ ] MALWARE-CNC Android.CoolReaper.Trojan outbound connection
- [ ] MALWARE-CNC Win.Trojan.TinyZBot response connection attempt
- [ ] MALWARE-CNC Win.Trojan.Kuluos variant outbound connection
- [ ] MALWARE-CNC Win.Backdoor.Medusa variant inbound connection
- [ ] MALWARE-CNC Win.Backdoor.Medusa variant outbound connection
- [ ] MALWARE-CNC User-Agent known malicious user-agent string - Mazilla/5.0 - Win.Backdoor.Upatre
- [ ] MALWARE-CNC Win.Trojan.Gamarue variant outbound connection
- [x] MALWARE-CNC Win.Trojan.HawkEye Keylogger exfiltration attempt - clipboard and screenshot
- [ ] MALWARE-CNC Win.Trojan.HawkEye Keylogger exfiltration attempt - clipboard and screenshot
- [ ] MALWARE-CNC Win.Agent.BHHK variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Upatre variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.SpyBanker variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.FileEncoder variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Kovter variant outbound connection
- [ ] MALWARE-CNC User-Agent known malicious user agent - ALIZER
- [ ] MALWARE-CNC Win.Trojan.Zusy variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.DNSChanger variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Turla outbound connection
- [ ] MALWARE-CNC Linux.Trojan.XORDDoS outbound connection
- [ ] MALWARE-CNC User-Agent known malicious user agent - Google Omaha - Win.Trojan.ExtenBro
- [ ] MALWARE-CNC Win.Trojan.Babar outbound connection
- [ ] FILE-IMAGE Microsoft emf file download request
- [ ] PUA-ADWARE Adware Goobzo/CrossRider variant outbound connection
- [x] OS-WINDOWS Microsoft Windows SMB NTLM NULL session attempt
- [ ] PUA-ADWARE User-Agent adware OutBrowse/Amonitize
- [ ] MALWARE-CNC Win.Trojan.Poseidon outbound connection
- [ ] MALWARE-CNC Win.Trojan.Gh0st variant outbound connection
- [ ] PUA-ADWARE InstallMetrix precheck stage outbound connection
- [ ] PUA-ADWARE InstallMetrix reporting binary installation stage status
- [ ] PUA-ADWARE User-Agent Vitruvian
- [ ] PUA-ADWARE Vitruvian outbound connection
- [ ] PUA-ADWARE SearchProtect user-agent detection
- [ ] PUA-ADWARE SuperOptimizer installation status
- [ ] PUA-ADWARE SuperOptimizer geolocation request
- [ ] PUA-ADWARE Eorezo get advertisement
- [ ] MALWARE-CNC Linux.Trojan.XORDDoS outbound connection
- [ ] SERVER-WEBAPP vBulletin XSS redirect attempt
- [ ] MALWARE-CNC Win.Trojan.DesertFalcon variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.DesertFalcon variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.DesertFalcon variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.DesertFalcon variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.DesertFalcon variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.DesertFalcon variant outbound connection
- [ ] SERVER-WEBAPP Magento remote code execution attempt
- [ ] MALWARE-CNC Win.Trojan.Banload variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Bancos variant outbound connection
- [ ] MALWARE-CNC Linux.Trojan.Mumblehard variant outbound connection
- [x] MALWARE-BACKDOOR Win.Backdoor.Wekby Torn variant outbound connection
- [ ] MALWARE-OTHER Win.Trojan.Wiper listener download attempt
- [ ] MALWARE-OTHER Win.Trojan.Wiper listener download attempt
- [ ] MALWARE-OTHER Win.Trojan.Wiper listener download attempt
- [ ] MALWARE-OTHER Win.Trojan.Wiper download attempt
- [ ] MALWARE-TOOLS Win.Trojan.Wiper proxy tools download attempt
- [ ] MALWARE-TOOLS Win.Trojan.Wiper proxy tool download attempt
- [ ] MALWARE-CNC Win.Trojan.TinyZBot outbound SOAP connection attempt
- [ ] MALWARE-CNC Win.Trojan.Kuluos variant outbound connection
- [ ] MALWARE-CNC User-Agent known malicious user-agent string - realupdate - Win.Backdoor.Upatre
- [ ] MALWARE-CNC Win.Backdoor.Medusa variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Heur variant outbound connection
- [x] PUA-ADWARE SoftPulse variant HTTP response attempt
- [ ] MALWARE-CNC Win.Trojan.HawkEye keylogger exfiltration attempt
- [ ] MALWARE-CNC Win.Trojan.HawkEye Keylogger exfiltration attempt - clipboard and screenshot
- [ ] INDICATOR-COMPROMISE Win.Trojan.Blocker variant outbound connection attempt
- [ ] MALWARE-CNC Win.Trojan.Kovter variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Symmi variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.FileEncoder IP geolocation checkin attempt
- [x] PUA-TOOLBARS Win.Toolbar.Crossrider variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Symmi variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Zusy inbound CNC response
- [ ] MALWARE-CNC User-Agent known malicious user-agent - DNS Changer
- [ ] MALWARE-CNC Win.Trojan.DNSChanger variant outbound connection
- [ ] MALWARE-CNC Linux.Trojan.XORDDoS outbound connection
- [ ] MALWARE-CNC Linux.Trojan.XORDDoS outbound connection
- [ ] MALWARE-CNC Win.Trojan.Tinba outbound connection
- [ ] MALWARE-CNC Win.Trojan.FannyWorm outbound connection
- [ ] PUA-ADWARE Adware Goobzo/CrossRider variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Egamipload variant outbound connection
- [ ] PUA-ADWARE User-Agent adware OutBrowse/Amonitize
- [ ] PUA-ADWARE User-Agent adware OutBrowse/Amonitize
- [ ] MALWARE-CNC Win.Trojan.Poseidon outbound connection
- [ ] MALWARE-CNC Win.Trojan.VBPasswordStealer variant outbound connection
- [ ] PUA-ADWARE InstallMetrix fetch offers stage outbound connection
- [ ] PUA-ADWARE InstallMetrix reporting fetch offers stage status
- [ ] PUA-ADWARE Vitruvian outbound connection
- [ ] MALWARE-CNC Win.Trojan.Banload variant MSSQL response
- [ ] MALWARE-CNC Win.Trojan.Dyre publickey outbound connection
- [ ] PUA-ADWARE SuperOptimizer encrypted data transmission
- [ ] PUA-ADWARE Eorezo outbound connection
- [ ] MALWARE-CNC Linux.Trojan.XORDDoS outbound connection
- [ ] MALWARE-CNC Linux.Trojan.XORDDoS outbound connection
- [ ] MALWARE-CNC Win.Trojan.Kraken outbound connection
- [ ] MALWARE-CNC Win.Trojan.DesertFalcon variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.DesertFalcon variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.DesertFalcon variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.DesertFalcon variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.DesertFalcon variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.CryptoWall variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Beebone outbound connection
- [ ] MALWARE-CNC Win.Trojan.Banload variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Bancos variant outbound connection
- [ ] MALWARE-CNC Linux.Downloader.Mumblehard variant outbound connection
- [ ] MALWARE-CNC Win.Backdoor.Wekby Torn variant outbound connection

- [ ] MALWARE-CNC Win.Trojan.Bancos variant outbound connection
- [ ] INDICATOR-COMPROMISE Metasploit Meterpreter reverse HTTPS certificate
- [ ] MALWARE-CNC Win.Trojan.Critroni certificate exchange
- [ ] MALWARE-CNC Win.Trojan.Prok variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.SpyBanker variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Banbra variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Agent-ALPW variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Zeus variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Ursnif outbound connection
- [ ] MALWARE-CNC Win.Trojan.Elise.B variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Andromeda initial outbound connection
- [ ] MALWARE-CNC Win.Trojan.TorrentLocker/Teerac self-signed certificate
- [ ] MALWARE-CNC Win.Trojan.Zeus variant outbound connection
- [ ] SERVER-WEBAPP Netgear WNDR4700 and R6200 admin interface authentication bypass attempt
- [ ] MALWARE-CNC Win.Trojan.Zeus variant outbound connection
- [ ] MALWARE-CNC Win.Backdoor.IsSpace initial outbound connection
- [x] FILE-IDENTIFY OLE Document upload detected
- [ ] MALWARE-CNC Win.Trojan.Bagsu variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.FakeAV variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Yakes variant dropper
- [ ] INDICATOR-COMPROMISE Metasploit Meterpreter reverse HTTPS certificate
- [ ] MALWARE-CNC Win.Trojan.Kovter outbound connection
- [ ] MALWARE-CNC Win.Trojan.Vawtrak variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.iSpySoft variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Engr variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Symmi variant outbound connection
- [ ] PROTOCOL-DNS glibc getaddrinfo AAAA record stack buffer overflow attempt
- [ ] POLICY-OTHER Polycom Botnet inbound connection attempt
- [ ] MALWARE-CNC Win.Trojan.Kazy variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Locky variant outbound connection
- [ ] MALWARE-CNC Win-Linux.Trojan.Derusbi variant outbound connection
- [ ] MALWARE-CNC Win-Linux.Trojan.Derusbi variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Locky variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.NetWiredRC variant connection setup
- [ ] MALWARE-CNC Win.Trojan.NetWiredRC variant keepalive
- [ ] MALWARE-CNC Win.Trojan.NetWiredRC variant send mail credentials
- [ ] MALWARE-CNC Win.Trojan.Dridex file download attempt
- [ ] MALWARE-CNC Win.Trojan.FTPKeyLogger outbound connection
- [ ] MALWARE-CNC Win.Trojan.FTPKeyLogger outbound connection
- [ ] MALWARE-CNC Win.Trojan.Boaxxe variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Sweeper outbound connection
- [ ] MALWARE-CNC Win.Trojan.Sweeper outbound connection
- [ ] MALWARE-CNC Win.Trojan.GateKeylogger outbound connection
- [ ] MALWARE-CNC Win.Trojan.GateKeylogger outbound connection - keystorkes
- [ ] MALWARE-CNC Win.Trojan.GateKeylogger plugins download attempt
- [ ] MALWARE-CNC Win.Trojan.GateKeylogger fake 404 response
- [ ] MALWARE-CNC Win.Trojan.Sweeper variant dropper initial download attempt
- [x] FILE-OFFICE RFT document malformed header
- [ ] MALWARE-CNC Win.Backdoor.DFSCook variant JS dropper outbound connection
- [ ] MALWARE-CNC Win.Backdoor.DFSCook variant outbound connection
- [ ] MALWARE-CNC Win.Backdoor.DFSCook variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.UP007 variant outbound connection
- [ ] MALWARE-CNC User-Agent known malicious user agent - EMERY - Win.Trojan.W97M
- [ ] MALWARE-CNC Win.Trojan.Rovnix variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Bancos variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Androm variant outbound connection
- [ ] PUA-ADWARE Win.Adware.Sendori user-agent detection
- [ ] MALWARE-CNC Win.Trojan.Banbra HTTP Header Structure
- [ ] MALWARE-CNC Win.Trojan.Graftor variant HTTP Response
- [ ] MALWARE-CNC Win.Zusy variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Cryptowall click fraud response
- [ ] MALWARE-CNC Win.Trojan.Bedep initial outbound connection
- [ ] MALWARE-CNC Win.Trojan.Andromeda download request
- [ ] MALWARE-CNC Win.Trojan.TorrentLocker/Teerac payment page request
- [ ] MALWARE-CNC Win.Trojan.Potao outbound connection
- [x] INDICATOR-COMPROMISE Wild Neutron potential exploit attempt
- [ ] MALWARE-CNC Win.Backdoor.IsSpace outbound connection
- [x] FILE-IDENTIFY JPEG file upload detected
- [ ] MALWARE-CNC Win.Trojan.Bagsu variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Bagsu variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Nimisi variant outbound connection
- [ ] INDICATOR-COMPROMISE Metasploit Meterpreter reverse HTTPS certificate
- [ ] MALWARE-CNC Potential hostile executable served from compromised or malicious WordPress site
- [x] MALWARE-CNC Win.Backdoor.Chopper web shell connection
- [ ] MALWARE-CNC Win.Trojan.iSpySoft variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.iSpySoft variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Symmi variant dropper download connection
- [ ] PROTOCOL-DNS glibc getaddrinfo A record stack buffer overflow attempt
- [ ] MALWARE-CNC Win.Trojan.Dridex dropper variant outbound connection
- [ ] POLICY-OTHER Polycom Botnet inbound connection attempt
- [ ] MALWARE-CNC Win.Trojan.Locky variant outbound connection
- [ ] INDICATOR-COMPROMISE malicious file download attempt
- [ ] MALWARE-CNC Win-Linux.Trojan.Derusbi variant outbound connection
- [ ] MALWARE-CNC Win/Linux.Trojan.Derusbi variant outbound connection
- [ ] MALWARE-CNC Linux.Trojan.Bifrose outbound connection
- [ ] MALWARE-CNC Win.Trojan.NetWiredRC variant failed read logs
- [ ] MALWARE-CNC Win.Trojan.NetWiredRC variant send credentials
- [ ] MALWARE-CNC Win.Trojan.Dridex certificate exchange
- [ ] MALWARE-CNC Win.Trojan.Dridex file download attempt
- [ ] MALWARE-CNC Win.Trojan.FTPKeyLogger outbound connection
- [ ] MALWARE-CNC Win.Trojan.FTPKeyLogger geolocation check
- [ ] MALWARE-CNC Win.Trojan.iSpySoft variant exfiltration attempt
- [ ] MALWARE-CNC Win.Trojan.Sweeper outbound connection
- [ ] MALWARE-CNC binary download while video expected
- [ ] MALWARE-CNC Win.Trojan.GateKeylogger outbound connection
- [ ] MALWARE-CNC Win.Trojan.GateKeylogger outbound connection - screenshot
- [ ] MALWARE-CNC Win.Trojan.GateKeylogger initial exfiltration attempt
- [ ] MALWARE-CNC Win.Trojan.GateKeylogger keylog exfiltration attempt
- [ ] MALWARE-CNC Win.Trojan.Sweeper variant dropper download attempt
- [x] FILE-OFFICE RFT document malformed header
- [ ] MALWARE-CNC Win.Backdoor.DFSCook variant outbound connection
- [ ] MALWARE-CNC Win.Backdoor.DFSCook variant temporary redirect attempt
- [ ] APP-DETECT Bloomberg web crawler outbound connection
- [ ] MALWARE-CNC Win.Trojan.Qakbot variant network speed test

- [ ] MALWARE-CNC Win.Trojan.Qakbot variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Godzilla downloader successful base64 binary download
- [ ] MALWARE-CNC Win.Trojan.Dridex certificate exchange
- [ ] MALWARE-CNC Win.Trojan.Bayrob variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Locky variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Kirts initial registration
- [x] PUA-ADWARE Win.Adware.OpenSoftwareUpdater variant outbound connection attempt
- [x] PUA-ADWARE Win.Adware.OpenSoftwareUpdater variant outbound connection attempt
- [ ] MALWARE-CNC Win.Trojan.Sinrin initial JS dropper outbound connection
- [ ] MALWARE-CNC Win.Trojan.LuminosityLink RAT variant outbound connection
- [ ] MALWARE-CNC Win.Backdoor.JRat inbound self-signed SSL certificate
- [ ] MALWARE-CNC Win.Trojan.Dridex self-signed certificate exchange
- [ ] MALWARE-CNC Win.Trojan.iSpy variant initial outbound connection
- [ ] MALWARE-CNC Win.Trojan.Qbot variant outbound connection
- [x] FILE-OFFICE RTF document incorrect file magic attempt
- [x] FILE-OFFICE Microsoft Office RTF WRAssembly ASLR bypass download attempt
- [ ] MALWARE-CNC Win.Backdoor.NanoBot variant outbound connection
- [ ] MALWARE-CNC Win.Backdoor.NanoBot variant outbound connection
- [ ] MALWARE-CNC Win.Backdoor.NanoBot variant inbound connection
- [ ] MALWARE-CNC Win.Backdoor.NanoBot variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.NanoBot/Perseus server heartbeat request attempt
- [ ] MALWARE-CNC Win.Trojan.Zeus variant inbound connection
- [ ] SERVER-WEBAPP HttpOxy CGI application vulnerability potential man-in-the-middle attempt
- [ ] MALWARE-CNC Win.Trojan.Hancitor variant outbound connection
- [x] FILE-OFFICE Microsoft Windows RTF file with embedded object package SMTP upload attempt
- [ ] MALWARE-CNC Win.Trojan.Locky variant outbound connection
- [x] FILE-IDENTIFY XLSB file magic detected
- [ ] OS-LINUX Linux Kernel Challenge ACK provocation attempt
- [x] SERVER-OTHER Cisco IOS Group-Prime memory disclosure exfiltration attempt
- [x] SERVER-OTHER Cisco IOS Group-Prime SHA memory disclosure attempt
- [ ] MALWARE-CNC Win.Perseus variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Satana ransomware outbound connection
- [ ] MALWARE-CNC Win.Trojan.Dexter Banker variant second stage download attempt
- [ ] MALWARE-CNC Win.Trojan.iSpy variant outbound connection
- [ ] MALWARE-CNC Android.Trojan.SpyNote RAT variant getSMS command response
- [ ] MALWARE-CNC Win.Trojan.Locky variant outbound connection
- [ ] MALWARE-CNC Win.Backdoor.Houdini variant initial outbound connection
- [ ] MALWARE-CNC Win.Backdoor.Houdini variant screenshot inbound init command attempt
- [ ] MALWARE-CNC Win.Backdoor.Houdini variant screen_thumb inbound init command attempt
- [ ] PUA-ADWARE Sokuxuan outbound connection attempt
- [ ] PUA-OTHER Bitcoin Mining authorize Stratum protocol client request attempt
- [ ] MALWARE-CNC Win.Trojan.RockLoader variant outbound connection
- [ ] INDICATOR-COMPROMISE Content-Type text/plain containing Portable Executable data
- [ ] MALWARE-CNC Win.Trojan.Dridex certificate exchange
- [ ] MALWARE-CNC Win.Trojan.Locky JS dropper outbound connection
- [ ] MALWARE-CNC Win.Trojan.Kirts exfiltration attempt
- [ ] MALWARE-CNC Win.Trojan.PassStealer passwords exfiltration attempt
- [x] PUA-ADWARE Win.Adware.OpenSoftwareUpdater variant outbound connection attempt
- [x] SQL use of sleep function in HTTP header - likely SQL injection attempt
- [ ] MALWARE-CNC Win.Trojan.NetWiredRC variant connection setup
- [ ] MALWARE-CNC Win.Trojan.LuminosityLink RAT variant inbound connection
- [ ] MALWARE-CNC Win.Backdoor.JRat inbound self-signed SSL certificate
- [ ] MALWARE-CNC Win.Trojan.Dridex self-signed certificate exchange
- [ ] MALWARE-CNC Win.Trojan.iSpy variant exfiltration outbound connection
- [x] FILE-OFFICE RTF document incorrect file magic attempt
- [x] FILE-OFFICE Microsoft Office RTF WRAssembly ASLR bypass download attempt
- [ ] MALWARE-CNC Win.Backdoor.NanoBot variant outbound connection
- [ ] MALWARE-CNC Win.Backdoor.NanoBot variant outbound connection
- [ ] MALWARE-CNC Win.Backdoor.NanoBot variant outbound connection
- [ ] MALWARE-CNC Win.Backdoor.NanoBot variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.NanoBot/Perseus initial outbound connection
- [ ] MALWARE-CNC Win.Trojan.NanoBot/Perseus client heartbeat response attempt
- [ ] INDICATOR-COMPROMISE Content-Type image containing Portable Executable data
- [ ] MALWARE-CNC Win.Trojan.Trans variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Spyrat variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.HawkEye keylogger exfiltration attempt
- [ ] BROWSER-FIREFOX Mozilla Firefox about field spoofing attempt
- [x] FILE-IDENTIFY XLSB file magic detected
- [ ] EXPLOIT-KIT Phoenix Exploit Kit inbound geoip.php bdr exploit attempt
- [x] SERVER-OTHER Cisco IOS Group-Prime MD5 memory disclosure attempt
- [ ] MALWARE-CNC User-Agent known malicious user-agent string - Win.Trojan.Perseus
- [ ] MALWARE-CNC Osx.Trojan.Keydnap variant initial backdoor download attempt
- [ ] MALWARE-CNC Win.Trojan.CryPy ransomware variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Dexter Banker variant successful installation report attempt
- [ ] MALWARE-CNC Android.Trojan.SpyNote RAT variant inbound connection
- [ ] MALWARE-CNC Android.Trojan.SpyNote RAT variant getContacts command response
- [ ] PUA-ADWARE MindSpark framework installer attempt
- [ ] MALWARE-CNC Win.Backdoor.Houdini variant keylogger inbound init command attempt
- [ ] MALWARE-CNC Win.Backdoor.Houdini variant screenshot inbound silence command attempt
- [ ] MALWARE-CNC Win.Backdoor.Houdini variant file enumeration inbound init/root/faf command attempt
- [ ] PUA-OTHER Bitcoin Mining subscribe Stratum protocol client request attempt
- [ ] PUA-OTHER Bitcoin Mining extranonce Stratum protocol subscribe client request attempt

- [ ] PROTOCOL-OTHER TP-Link TDDP SET_CONFIG type buffer overflow attempt
- [x] BROWSER-FIREFOX Mozilla Firefox ESR NotifyTimeChange use after free attempt
- [ ] MALWARE-CNC Win.Rootkit.Sednit variant outbound connection
- [ ] SERVER-WEBAPP Netgear WNR2000 authentication bypass attempt
- [ ] MALWARE-CNC Win.Trojan.Locky variant outbound connection
- [ ] MALWARE-CNC Andr.Trojan.Sysch variant outbound connection
- [ ] SERVER-WEBAPP Western Digital MyCloud command injection attempt
- [ ] SERVER-WEBAPP Western Digital MyCloud command injection attempt
- [ ] MALWARE-CNC Win.Trojan.NetWiredRC variant registration message
- [ ] MALWARE-CNC Win.Trojan.NetWiredRC variant keepalive
- [ ] MALWARE-CNC User-Agent known malicious user-agent string - X-Mas
- [ ] MALWARE-CNC Win.Ransomware.X-Mas variant keylogger outbound connection
- [ ] SERVER-OTHER QNAP remote buffer overflow attempt
- [x] SERVER-WEBAPP WordPress get_post authentication bypass attempt
- [ ] MALWARE-CNC Win.Ransomware.CryptoLocker binary download response attempt
- [ ] SERVER-WEBAPP Netgear passwordrecovered.cgi insecure admin password disclosure attempt
- [ ] SERVER-WEBAPP Netgear DGN2200 ping.cgi command injection attempt
- [ ] SERVER-WEBAPP Netgear DGN2200 ping.cgi command injection attempt
- [ ] MALWARE-CNC Win.Trojan.Houdini variant initial outbound connection
- [ ] SERVER-WEBAPP DotNetNuke installation attempt detected
- [x] SERVER-OTHER Cisco IOS Smart Install protocol download config command attempt
- [x] SERVER-OTHER Cisco IOS Smart Install protocol version command attempt
- [ ] SERVER-WEBAPP Netgear DGN2200 dnslookup.cgi command injection attempt
- [ ] SERVER-WEBAPP Netgear DGN2200 dnslookup.cgi command injection attempt
- [ ] MALWARE-CNC User-Agent known malicious user-agent string - Andr.Trojan.Agent
- [ ] MALWARE-CNC Win.Ransomware.Sage variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Ismdoor variant outbound connection
- [ ] OS-WINDOWS Microsoft Windows empty RDP cookie negotiation attempt
- [x] MALWARE-CNC Win.Trojan.Doublepulsar variant process injection command
- [x] OS-WINDOWS Microsoft Windows SMB large NT RENAME transaction request memory leak attempt
- [ ] OS-WINDOWS Microsoft Windows SMB anonymous session IPC share access attempt
- [x] OS-WINDOWS Microsoft Malware Protection Engine type confusion attempt
- [x] MALWARE-CNC Win.Backdoor.Chopper web shell connection
- [x] MALWARE-CNC Win.Backdoor.Chopper web shell connection
- [ ] MALWARE-CNC Deputy Dog implant outbound connection
- [ ] MALWARE-CNC ZoxPNG initial outbound connection
- [ ] MALWARE-CNC Win.Trojan.MadMax implant outbound connection
- [ ] MALWARE-CNC HttpBrowser User-Agent outbound communication attmept
- [x] PROTOCOL-OTHER NETBIOS SMB IPC share access attempt
- [x] SERVER-SAMBA Samba is_known_pipe arbitrary module load code execution attempt
- [ ] MALWARE-CNC Win.Trojan.HiddenCobra variant outbound connection

- [x] BROWSER-FIREFOX Mozilla Firefox ESR NotifyTimeChange use after free attempt
- [ ] PROTOCOL-OTHER TP-Link TDDP Get_config configuration leak attempt
- [ ] MALWARE-CNC Linux.DDoS.D93 outbound connection
- [ ] SERVER-WEBAPP Netgear WNR2000 hidden_lang_avi stack buffer overflow attempt
- [x] MALWARE-CNC Win.Trojan.Locky variant outbound connection
- [ ] MALWARE-CNC Andr.Trojan.Sysch variant outbound connection
- [ ] SERVER-WEBAPP Western Digital MyCloud command injection attempt
- [ ] SERVER-WEBAPP Western Digital MyCloud command injection attempt
- [ ] MALWARE-CNC Win.Trojan.NetWiredRC variant check logs
- [ ] POLICY-OTHER Cisco Webex explicit use of web plugin detected
- [ ] MALWARE-CNC Win.Ransomware.X-Mas outbound connection
- [ ] MALWARE-CNC Win.Ransomware.X-Mas variant keylogger outbound connection
- [x] SERVER-WEBAPP WordPress get_post authentication bypass attempt
- [x] SERVER-WEBAPP WordPress get_post authentication bypass attempt
- [x] SERVER-SAMBA Microsoft Windows SMBv2/SMBv3 Buffer Overflow attempt
- [ ] MALWARE-CNC Osx.Downloader.MacDownloader variant outbound connection
- [ ] SERVER-WEBAPP Netgear DGN2200 ping.cgi command injection attempt
- [ ] INDICATOR-COMPROMISE Binary file download request from internationalized domain name using Microsoft BITS
- [ ] MALWARE-CNC Win.Trojan.Houdini backdoor file download request
- [x] SERVER-OTHER Cisco IOS Smart Install protocol backup config command attempt
- [x] SERVER-OTHER Cisco IOS Smart Install protocol download image command attempt
- [ ] SERVER-WEBAPP Netgear DGN2200 dnslookup.cgi command injection attempt
- [ ] SERVER-WEBAPP Netgear DGN2200 dnslookup.cgi command injection attempt
- [x] OS-WINDOWS Microsoft Windows SMB remote code execution attempt
- [ ] MALWARE-CNC Andr.Trojan.Agent variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Ismdoor variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.RedLeaves outbound connection
- [x] OS-WINDOWS Microsoft Windows SMB anonymous user session setup request detected
- [x] MALWARE-CNC Win.Trojan.Doublepulsar variant ping command
- [x] OS-WINDOWS Microsoft Windows SMB possible leak of kernel heap memory
- [ ] MALWARE-CNC Win.Trojan.RedLeaves outbound connection
- [x] OS-WINDOWS Microsoft Malware Protection Engine type confusion attempt
- [x] MALWARE-CNC Win.Backdoor.Chopper web shell connection
- [ ] SERVER-WEBAPP MVPower DVR Shell arbitrary command execution attempt
- [ ] MALWARE-CNC Deputy Dog implant outbound connection
- [ ] MALWARE-CNC Win.Trojan.MadMax implant outbound connection attempt
- [ ] MALWARE-CNC WashingTon ssl certificate negotiation attempt
- [x] OS-WINDOWS Microsoft Windows SMB remote code execution attempt
- [x] PROTOCOL-OTHER NETBIOS SMB IPC share access attempt
- [ ] MALWARE-CNC Win.Trojan.Kabob outbound connection
- [ ] MALWARE-CNC Win.Trojan.HiddenCobra variant outbound connection

- [ ] SERVER-WEBAPP /.svn/entries file access attempt
- [ ] SERVER-WEBAPP /etc/inetd.conf file access attempt
- [ ] SERVER-WEBAPP /etc/shadow file access attempt
- [ ] SERVER-WEBAPP Oracle Application Server 9i unauthenticated application deployment attempt
- [ ] POLICY-OTHER Teleopti WFM administrative user credentials request detected
- [ ] SERVER-OTHER WSFTP IpSwitch custom SITE command execution attempt
- [ ] SERVER-WEBAPP Kaspersky Linux File Server WMC directory traversal attempt
- [ ] SERVER-WEBAPP Kaspersky Linux File Server WMC directory traversal attempt
- [ ] MALWARE-CNC Osx.Trojan.XAgent outbound connection
- [ ] MALWARE-CNC Win.Trojan.Fareit variant outbound connection
- [ ] MALWARE-CNC Andr.Trojan.Femas variant outbound connection
- [ ] SERVER-WEBAPP Cisco DDR2200 ADSL gateway command injection attempt
- [ ] SERVER-WEBAPP Cisco DDR2200 ADSL gateway command injection attempt
- [ ] MALWARE-CNC Win.Trojan.Trickbot self-signed certificate exchange
- [ ] MALWARE-CNC Win.Trojan.Trickbot self-signed certificate exchange
- [ ] MALWARE-CNC Potential hostile executable served from compromised or malicious WordPress site attempt
- [ ] MALWARE-CNC Win.Trojan.PandaZeus malicious certificate exchange
- [ ] SERVER-OTHER Mikrotik RouterOS denial of service attempt
- [ ] POLICY-OTHER NetSupport Manager RAT outbound connection detected
- [ ] SERVER-WEBAPP Netgear DGN1000 series routers arbitrary command execution attempt
- [ ] SERVER-WEBAPP Internal field separator use in HTTP URI attempt
- [ ] SERVER-OTHER libupnp command buffer overflow attempt
- [ ] MALWARE-CNC Win.Trojan.KopiLuwak variant outbound request detected
- [ ] SERVER-OTHER QNAP transcode server command injection attempt
- [ ] MALWARE-CNC Win.Trojan.Neuron variant inbound service request detected
- [ ] MALWARE-CNC Win.Trojan.Neuron variant inbound service request detected
- [ ] MALWARE-CNC Win.Backdoor.StoneDrill server selection outbound connection
- [ ] MALWARE-CNC Win.Backdoor.StoneDrill get commands outbound connection
- [ ] PUA-ADWARE Osx.Adware.SurfBuyer adware outbound connection detected
- [ ] MALWARE-CNC Osx.Trojan.OceanLotus outbound connection attempt
- [ ] SERVER-WEBAPP Asus RT-AC88U deleteOfflineClients memory corruption attempt
- [ ] SERVER-WEBAPP MikroTik RouterOS jsproxy readPostData memory corruption attempt
- [ ] MALWARE-CNC Unix.Trojan.Vpnfilter variant outbound connection attempt
- [ ] MALWARE-CNC Vbs.Trojan.Agent outbound connection
- [x] MALWARE-CNC Vbs.Trojan.Agent inbound payload download
- [ ] MALWARE-CNC Vbs.Trojan.Agent outbound system information disclosure
- [x] MALWARE-CNC Win.Trojan.Revenge RAT initial outbound connection
- [x] MALWARE-CNC Win.Trojan.UDPOS outbound command and control IP address check
- [x] MALWARE-CNC Win.Trojan.UDPOS outbound heartbeat
- [x] MALWARE-CNC Win.Trojan.UDPOS outbound data exfiltration
- [ ] SERVER-WEBAPP /cgi-bin/sh file access attempt
- [ ] SERVER-WEBAPP /etc/motd file access attempt
- [ ] SERVER-WEBAPP /ws_ftp.log file access attempt
- [ ] POLICY-OTHER Teleopti WFM database information request detected
- [ ] POLICY-OTHER Teleopti WFM administrative user creation detected
- [ ] SERVER-WEBAPP Kaspersky Linux File Server WMC cross site request forgery attempt
- [ ] SERVER-WEBAPP Kaspersky Linux File Server WMC directory traversal attempt
- [ ] SERVER-WEBAPP Kaspersky Linux File Server WMC cross site scripting attempt
- [ ] SERVER-WEBAPP Ubiquiti Networks UniFi Cloud Key Firm v0.6.1 Host Remote Command Execution attempt
- [ ] MALWARE-CNC Andr.Trojan.Femas variant outbound connection
- [ ] POLICY-OTHER Cisco DDR2200 ASDL gateway file download detected
- [ ] SERVER-WEBAPP Cisco DDR2200 ADSL gateway command injection attempt
- [ ] SERVER-WEBAPP Cisco DDR2200 ADSL gateway command injection attempt
- [ ] MALWARE-CNC Win.Trojan.Trickbot self-signed certificate exchange
- [ ] MALWARE-CNC Win.Trojan.Trickbot self-signed certificate exchange
- [ ] MALWARE-CNC Potential hostile executable served from compromised or malicious WordPress site attempt
- [ ] MALWARE-CNC Win.Trojan.PandaZeus self-signed certificate exchange
- [ ] MALWARE-CNC Win.Zusy variant outbound connection
- [x] SERVER-WEBAPP Netgear DGN1000 series routers authentication bypass attempt
- [ ] MALWARE-CNC Win.Trojan.Gen variant outbound connection
- [ ] SERVER-WEBAPP Internal field separator use in HTTP URI attempt
- [ ] MALWARE-CNC Win.Trojan.KopiLuwak variant outbound request detected
- [ ] SERVER-WEBAPP MikroTik RouterOS cross site request forgery attempt
- [ ] SERVER-WEBAPP Netgear WNR2000 information leak attempt
- [ ] MALWARE-CNC Win.Trojan.Neuron variant inbound service request detected
- [ ] MALWARE-CNC Win.Trojan.Neuron variant inbound service request detected
- [ ] MALWARE-CNC Win.Backdoor.StoneDrill login outbound connection
- [ ] SERVER-OTHER SSDP M-SEARCH ssdp-all potential amplified distributed denial-of-service attempt
- [ ] PUA-ADWARE Osx.Adware.SurfBuyer adware outbound connection detected
- [ ] POLICY-OTHER TrendMicro ServerProtect server configuration file download detected
- [x] MALWARE-CNC Osx.Trojan.SHLayer variant outbound connection
- [x] MALWARE-CNC Unix.Trojan.Vpnfilter variant outbound connection attempt
- [ ] MALWARE-CNC Win.Trojan.Rokrat variant outbound connection detected
- [ ] MALWARE-CNC Vbs.Trojan.Agent inbound payload download
- [x] MALWARE-CNC Vbs.Trojan.Agent inbound payload download
- [x] MALWARE-CNC Win.Trojan.Silverstar outbound connection
- [x] MALWARE-CNC Win.Trojan.Revenge RAT inbound heartbeat check
- [x] MALWARE-CNC Win.Trojan.UDPOS outbound system information disclousre
- [x] MALWARE-CNC Win.Trojan.UDPOS outbound data exfiltration
- [ ] OS-WINDOWS Microsoft Windows SMB kernel heap memory leak attempt

- [ ] OS-WINDOWS Microsoft Windows SMB kernel heap memory leak attempt
- [x] MALWARE-CNC MultiOS.Trojan.OSCelestial variant inbound connection
- [x] MALWARE-CNC Win.Trojan.Gen variant outbound communication
- [x] MALWARE-CNC Win.Trojan.Bandook/Anbacas outbound connection attempt
- [x] MALWARE-CNC Win.Trojan.yty second stage downloader initial outbound connection
- [x] MALWARE-CNC Win.Trojan.yty module download request
- [x] MALWARE-CNC Win.Trojan.yty file exfiltration outbound request
- [ ] SERVER-WEBAPP Linksys E-Series apply.cgi cross site scripting attempt
- [ ] SERVER-WEBAPP Linksys E-Series apply.cgi ping function command injection attempt
- [ ] SERVER-WEBAPP Linksys E-Series apply.cgi directory traversal attempt
- [ ] SERVER-WEBAPP Linksys E-Series apply.cgi ping function command injection attempt
- [ ] PROTOCOL-OTHER use of undocumented ScMM test interface in Cisco small business devices detected
- [ ] PROTOCOL-OTHER use of undocumented ScMM test interface in Cisco small business devices detected
- [ ] MALWARE-CNC Win.Trojan.Banbra variant outbound connection
- [ ] SERVER-WEBAPP Linksys E series denial of service attempt
- [ ] SERVER-WEBAPP QNAP VioStor NVR and QNAP NAS command injection attempt
- [ ] SERVER-WEBAPP QNAP VioStor NVR and QNAP NAS command injection attempt
- [ ] SERVER-WEBAPP QNAP WTS 4.2.1 command injection attempt
- [ ] SERVER-WEBAPP QNAP WTS 4.2.1 command injection attempt
- [ ] SERVER-OTHER QNAP NVR/NAS Heap/Stack Overflow attempt
- [ ] SERVER-WEBAPP Netgear WNR2000 information disclosure attempt
- [ ] SERVER-WEBAPP Netgear WNR2000 information disclosure attempt
- [x] SERVER-WEBAPP Drupal 8 remote code execution attempt
- [ ] SERVER-OTHER NETGEAR TelnetEnable attempt
- [ ] SERVER-WEBAPP Netgear DGN2200B stored cross-site scripting attempt
- [ ] MALWARE-CNC Win.Ransomware.Matrix outbound connection
- [ ] SERVER-WEBAPP Akeeba Kickstart cross site request forgery attempt
- [ ] SERVER-OTHER libgd heap-overflow attempt
- [x] MALWARE-CNC Win.Trojan.Dropper variant outbound connection
- [x] MALWARE-CNC Win.Trojan.Kraens delivery attempt
- [ ] MALWARE-CNC Win.Trojan.Kraens initial outbound request
- [ ] MALWARE-CNC Win.Adware.Doyo client outbound connection
- [x] MALWARE-CNC Vbs.Downloader.Agent inbound connection
- [x] MALWARE-CNC Vbs.Downloader.Agent inbound connection
- [x] MALWARE-CNC Installation Keylogger Osx.Trojan.Mokes data exfiltration
- [x] MALWARE-CNC Win.Trojan.Ammy heartbeat
- [x] MALWARE-CNC Win.Trojan.Agent outbound request
- [ ] SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt
- [ ] SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt
- [ ] SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt
- [ ] SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt
- [ ] SERVER-WEBAPP Belkin N750 F9K1103 wireless router remote telnet enable attempt
- [ ] MALWARE-CNC Win.Trojan.Banload second stage download request
- [ ] SERVER-WEBAPP Digital Guardian Management Console arbitrary file upload attempt
- [x] MALWARE-CNC MultiOS.Trojan.OSCelestial variant outbound connection
- [ ] POLICY-OTHER Sandvine PacketLogic http redirection attempt
- [x] MALWARE-CNC Win.Trojan.CrossRAT outbound connection attempt
- [x] MALWARE-CNC User-Agent known malicious user-agent string Uploador - Win.Trojan.CrossRAT
- [x] MALWARE-CNC Win.Trojan.yty plugin downloader initial outbound connection
- [x] MALWARE-CNC Win.Trojan.yty module request
- [ ] NETBIOS MikroTik RouterOS buffer overflow attempt
- [ ] SERVER-WEBAPP Linksys E-Series apply.cgi cross site scripting attempt
- [ ] SERVER-WEBAPP Linksys E-Series apply.cgi directory traversal attempt
- [ ] SERVER-WEBAPP Linksys E-Series apply.cgi ping function command injection attempt
- [ ] PROTOCOL-OTHER use of undocumented ScMM test interface in Cisco small business devices detected
- [ ] PROTOCOL-OTHER use of undocumented ScMM test interface in Cisco small business devices detected
- [ ] MALWARE-CNC Win.Trojan.HW32 variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Cidox variant outbound connection attempt
- [ ] SERVER-WEBAPP QNAP VioStor NVR and QNAP NAS command injection attempt
- [ ] SERVER-WEBAPP QNAP VioStor NVR and QNAP NAS command injection attempt
- [ ] SERVER-OTHER QNAP QTS X-Forwarded-For buffer overflow
- [ ] SERVER-WEBAPP QNAP WTS 4.2.1 command injection attempt
- [ ] SERVER-WEBAPP QNAP WTS 4.2.1 command injection attempt
- [ ] SERVER-OTHER QNAP NVR/NAS Heap/Stack Overflow attempt
- [ ] SERVER-WEBAPP Netgear WNR2000 information disclosure attempt
- [ ] SERVER-WEBAPP Joomla restore.php PHP object injection attempt
- [ ] SERVER-OTHER NETGEAR TelnetEnable attempt
- [ ] SERVER-WEBAPP Netgear DGN2200B stored cross-site scripting attempt
- [ ] SERVER-OTHER QNAP QTS hard coded credential access attempt
- [ ] SERVER-WEBAPP Akeeba Kickstart restoration.php reconnaissance attempt
- [ ] SERVER-OTHER QNAP QTS cross site request forgery attempt
- [ ] SERVER-OTHER libgd heap-overflow attempt
- [ ] MALWARE-CNC Win.Spyware.Autoit outbound connection
- [x] MALWARE-CNC Win.Trojan.Kraens delivery attempt
- [ ] MALWARE-CNC Win.Adware.Doyo initial connection
- [x] MALWARE-CNC Vbs.Downloader.Kryptik known malicious user-agent string
- [x] MALWARE-CNC Vbs.Downloader.Agent inbound connection
- [x] MALWARE-CNC Vbs.Downloader.Agent inbound delivery attempt
- [ ] SERVER-WEBAPP TwonkyMedia server directory listing attempt
- [x] MALWARE-CNC Win.Trojan.Ammy download attempt
- [x] MALWARE-CNC Win.Trojan.Agent outbound request
- [ ] SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt
- [ ] SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt
- [ ] SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt
- [ ] SERVER-WEBAPP Belkin N750 F9K1103 wireless router command injection attempt
- [ ] SERVER-WEBAPP Belkin N750 F9K1103 wireless router remote telnet enable attempt
- [x] MALWARE-CNC Win.Trojan.Unruy outbound callout
- [ ] SERVER-WEBAPP Digital Guardian Management Console arbitrary file upload attempt

- [x] MALWARE-CNC Win.Trojan.Dropper malicious script download attempt
- [x] MALWARE-CNC Win.Trojan.Dropper initial outbound connection attempt
- [ ] MALWARE-CNC Win.Trojan.Dropper malicious executable download attempt
- [x] MALWARE-CNC Win.Trojan.Qarallax outbound connection attempt
- [x] MALWARE-CNC Win.Trojan.Qarallax outbound connection
- [ ] SERVER-WEBAPP Nagios XI SQL injection attempt
- [ ] SERVER-WEBAPP NagiosXI SQL injection attempt
- [ ] SERVER-WEBAPP Nagios XI command injection attempt
- [ ] SERVER-WEBAPP Nagios XI command injection attempt
- [ ] SERVER-WEBAPP Nagios XI command injection attempt
- [ ] SERVER-WEBAPP Nagios XI command injection attempt
- [ ] SERVER-WEBAPP Nagios XI database settings modification attempt
- [ ] MALWARE-CNC Unix.Trojan.Vpnfilter variant SSL connection attempt
- [x] MALWARE-CNC Win.Downloader.Zebrocy known malicious user-agent string
- [x] MALWARE-CNC Win.Downloader.Zebrocy initial outbound request
- [x] MALWARE-CNC Andr.Trojan.ZooPark outbound connection attempt
- [x] MALWARE-CNC Andr.Trojan.ZooPark outbound connection attempt
- [x] MALWARE-CNC Andr.Trojan.ZooPark outbound connection attempt
- [x] MALWARE-CNC Andr.Trojan.ZooPark outbound connection attempt
- [ ] SERVER-WEBAPP Anti-Web directory traversal attempt
- [ ] SERVER-WEBAPP Anti-Web directory traversal attempt
- [x] SERVER-WEBAPP BA Systems BAS Web information disclosure attempt
- [x] SERVER-WEBAPP BA Systems BAS Web information disclosure attempt
- [ ] SERVER-WEBAPP FLIR Breakstream 2300 unauthenticated information disclosure attempt
- [x] MALWARE-CNC Win.Ransomware.Satan outbound connection
- [x] MALWARE-OTHER Win.Ransomware.Satan payload download
- [ ] SERVER-WEBAPP DotNetNuke DreamSlider arbitrary file download attempt
- [x] MALWARE-CNC Win.Trojan.Dunihi outbound connection
- [ ] MALWARE-CNC Win.Trojan.RedLeaves variant outbound connection
- [ ] OS-LINUX Red Hat NetworkManager DHCP client command injection attempt
- [x] MALWARE-CNC Win.Trojan.CowerSnail command and control response detected
- [x] MALWARE-CNC Win.Trojan.CowerSnail initial outbound connection attempt
- [x] MALWARE-CNC Win.Trojan.Joanap variant outbound connection
- [x] MALWARE-CNC Win.Trojan.Nocturnal outbound connection
- [x] MALWARE-CNC Win.Trojan.Fareit variant outbound connection
- [x] MALWARE-CNC Win.Trojan.Dropper outbound connection
- [x] MALWARE-CNC Win.Trojan.Danabot outbound connection
- [x] MALWARE-CNC Win.Trojan.Danabot outbound connection
- [x] MALWARE-CNC Win.Trojan.Danabot outbound connection
- [ ] MALWARE-CNC Win.Trojan.Autophyte dropper variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.Autophyte RAT variant outbound connection
- [ ] INDICATOR-COMPROMISE Microsoft Office Discovery User-Agent to a potential URL shortener service
- [ ] INDICATOR-COMPROMISE Microsoft Office Discovery User-Agent to a potential URL shortener service
- [x] MALWARE-CNC Win.Trojan.Orcus RAT inbound SSL certificate
- [ ] INDICATOR-COMPROMISE Microsoft cmd.exe banner
- [x] MALWARE-CNC Win.Trojan.SocketPlayer outbound connection
- [ ] MALWARE-CNC Win.Trojan.SocketPlayer outbound connection
- [x] MALWARE-CNC Win.Spyware.Invisimole CnC outbound connection
- [x] MALWARE-CNC Win.Trojan.TechSupportScam installed binary outbound connection
- [x] MALWARE-CNC Win.Trojan.TechSupportScam installed binary outbound connection
- [x] MALWARE-CNC Win.Trojan.TechSupportScam installed binary outbound connection
- [ ] PUA-ADWARE Win.Adware.Pbot variant outbound connection
- [ ] PUA-ADWARE Win.Adware.Pbot variant outbound connection
- [ ] PUA-ADWARE Win.Adware.Pbot variant outbound connection
- [ ] MALWARE-CNC Win.Trojan.NukeSped RAT variant outbound communication
- [ ] MALWARE-CNC Win.Trojan.NukeSped RAT variant outbound connection
- [x] MALWARE-CNC Js.Trojan.Agent JS Sniffer beacon connection
- [x] MALWARE-CNC Win.Trojan.ARS VBS loader outbound connection
- [x] MALWARE-CNC Unix.Trojan.Vpnfilter plugin variant connection attempt
- [ ] SERVER-WEBAPP Oracle WebLogic Server unauthenticated modified JSP access attempt
- [ ] SERVER-WEBAPP Oracle WebLogic Server potential unauthenticated reconnaissance attempt
- [ ] SERVER-WEBAPP Oracle WebLogic Server potential precursor to keystore attack attempt
- [x] MALWARE-CNC Osx.Trojan.Calisto outbound connection
- [x] MALWARE-CNC Osx.Trojan.Calisto outbound connection
- [x] MALWARE-CNC Win.Trojan.Mapoyun variant outbound connection attempt
- [ ] MALWARE-CNC Win.Trojan.PLEAD downloader outbound connection
- [ ] MALWARE-CNC Win.Trojan.PLEAD downloader outbound connection
- [x] MALWARE-CNC Win.Trojan.Zegost variant outbound connection
- [x] SERVER-WEBAPP Joomla Proclaim biblestudy backup access attempt
- [x] MALWARE-CNC Win.Trojan.KeyPass variant inbound connection attempt
- [ ] INDICATOR-OBFUSCATION DNS TXT response record tunneling
- [ ] SERVER-WEBAPP SSL certificate with null issuer rdnSequence fields detected
- [x] MALWARE-CNC Win.Trojan.Marap outbound beacon detected
- [x] MALWARE-CNC Andr.Trojan.MysteryBot outbound connection
- [x] MALWARE-CNC Andr.Trojan.AnubisCrypt variant outbound post detected
- [x] MALWARE-CNC Andr.Trojan.AnubisCrypt variant outbound post detected
- [x] MALWARE-CNC Win.Trojan.OilRig variant outbound connection
- [x] MALWARE-CNC Win.Trojan.OilRig variant outbound connection
- [x] MALWARE-CNC Win.Trojan.OilRig variant outbound connection
- [x] MALWARE-CNC Win.Trojan.MSDownloader variant outbound connection
- [x] MALWARE-CNC Win.Trojan.MSDownloader variant download
- [x] MALWARE-CNC Win.Trojan.MSDownloader variant download
- [x] MALWARE-CNC Win.Trojan.AcridRain outbound connection
- [x] MALWARE-CNC Win.Trojan.AcridRain outbound connection
- [x] MALWARE-CNC Win.Trojan.MirageFox variant outbound connection
- [x] MALWARE-CNC Win.Trojan.MirageFox variant outbound connection
- [x] MALWARE-CNC Win.Trojan.ITranslator variant outbound connection
- [x] MALWARE-CNC Win.Trojan.ITranslator variant outbound connection
- [x] MALWARE-CNC Win.Trojan.ITranslator variant outbound connection
- [x] MALWARE-CNC Win.Trojan.ITranslator variant outbound connection

- [x] MALWARE-CNC Win.Trojan.ITranslator variant outbound connection
- [x] MALWARE-CNC Win.Downloader.XAgent variant outbound connection
- [x] MALWARE-CNC Win.Trojan.Zebrocy variant outbound connection
- [x] MALWARE-CNC Win.Trojan.Zebrocy variant payload download attempt
- [x] MALWARE-CNC Js.Trojan.Agent variant inbound payload download
- [x] MALWARE-CNC Osx.Trojan.WindTail outbound connection
- [x] MALWARE-CNC Osx.Trojan.WindTail outbound connection
- [x] MALWARE-CNC Win.Trojan.BitterRAT variant outbound connection
- [x] MALWARE-CNC Win.Trojan.BitterRAT variant outbound connection
- [x] MALWARE-CNC Win.Trojan.BitterRAT variant outbound connection
- [x] MALWARE-CNC Win.Trojan.Zebrocy variant outbound connection
- [ ] PROTOCOL-SCADA PCOM Init Device ASCII request
- [ ] PROTOCOL-SCADA PCOM Get UnitID ASCII request
- [ ] PROTOCOL-SCADA PCOM Set RTC ASCII request
- [ ] PROTOCOL-SCADA PCOM Read System Bits ASCII request
- [ ] PROTOCOL-SCADA PCOM Read Memory Longs ASCII request
- [ ] PROTOCOL-SCADA PCOM Write System Bits ASCII request
- [ ] PROTOCOL-SCADA PCOM Read System Integers ASCII request
- [ ] PROTOCOL-SCADA PCOM Write Ouputs ASCII request
- [ ] PROTOCOL-SCADA PCOM Start Device ASCII request
- [ ] PROTOCOL-SCADA PCOM Get RTC ASCII request
- [ ] PROTOCOL-SCADA PCOM Reset Device ASCII request
- [ ] PROTOCOL-SCADA PCOM Write Memory Integers ASCII request
- [ ] PROTOCOL-SCADA PCOM Set UnitID ASCII reply
- [ ] PROTOCOL-SCADA PCOM Identification ASCII reply
- [ ] PROTOCOL-SCADA PCOM Get UnitID ASCII reply
- [ ] PROTOCOL-SCADA PCOM Get PLC Name binary request
- [ ] PROTOCOL-SCADA PCOM Read Inputs ASCII reply
- [ ] PROTOCOL-SCADA PCOM Read Longs ASCII reply
- [ ] PROTOCOL-SCADA PCOM Read Ouputs ASCII reply
- [ ] PROTOCOL-SCADA PCOM Read Memory Integers ASCII reply
- [ ] PROTOCOL-SCADA PCOM Write System Integers ASCII reply
- [ ] PROTOCOL-SCADA PCOM Write Ouputs ASCII reply
- [ ] PROTOCOL-SCADA PCOM Write Longs ASCII reply
- [ ] PROTOCOL-SCADA PCOM Get PLC Name binary reply
- [ ] PROTOCOL-SCADA PCOM Read Data Table binary reply
- [ ] PUA-ADWARE Osx.Adware.Genieo variant outbound connection detected
- [x] SERVER-SAMBA Samba is_known_pipe arbitrary module load code execution attempt
- [x] MALWARE-CNC Win.Trojan.Zebrocy variant outbound connection
- [x] MALWARE-CNC Win.Trojan.Zebrocy variant outbound connection
- [x] MALWARE-CNC Win.Trojan.Fakewmi variant outbound connection attempt
- [x] MALWARE-CNC Win.Trojan.SectorA05 outbound connection attempt
- [x] MALWARE-CNC Win.Trojan.SectorA05 outbound connection attempt
- [x] MALWARE-CNC Win.Trojan.TSCookie variant outbound connection
- [x] MALWARE-CNC Win.Ransomware.Lockergoga binary download attempt
- [x] MALWARE-CNC Win.Ransomware.Lockergoga binary download attempt
- [x] MALWARE-CNC Win.Trojan.Zacinlo outbound connection
- [x] MALWARE-CNC Win.Trojan.Zacinlo outbound connection
- [ ] SERVER-WEBAPP Tpshop remote file include attempt
- [ ] SERVER-WEBAPP LG-Ericsson iPECS NMS 30M directory traversal attempt
- [ ] SERVER-WEBAPP LG-Ericsson iPECS NMS 30M directory traversal attempt
- [x] MALWARE-CNC Win.Downloader.TeamBot outbound cnc connection
- [x] MALWARE-CNC Win.Downloader.TeamBot additional payload download attempt
- [x] MALWARE-CNC Win.Downloader.TeamBot additional payload download attempt
- [x] MALWARE-CNC Win.Trojan.ITranslator variant outbound connection
- [x] MALWARE-CNC Win.Trojan.Zebrocy variant outbound connection
- [x] MALWARE-CNC Win.Trojan.Zebrocy variant outbound connection
- [x] MALWARE-CNC Js.Trojan.Agent variant outbound connection
- [x] MALWARE-CNC Win.Trojan.Zebrocy variant outbound connection
- [x] MALWARE-CNC Osx.Trojan.WindTail outbound connection
- [x] MALWARE-CNC Win.Trojan.Agent variant outbound connection
- [x] MALWARE-CNC Win.Trojan.BitterRAT variant outbound connection
- [x] MALWARE-CNC Win.Trojan.BitterRAT variant outbound connection
- [x] MALWARE-CNC Win.Trojan.BitterRAT variant outbound connection
- [ ] PROTOCOL-SCADA PCOM Identification ASCII request
- [ ] PROTOCOL-SCADA PCOM Set UnitID ASCII request
- [ ] PROTOCOL-SCADA PCOM Read Inputs ASCII request
- [ ] PROTOCOL-SCADA PCOM Read Ouputs ASCII request
- [ ] PROTOCOL-SCADA PCOM Read Memory Integers ASCII request
- [ ] PROTOCOL-SCADA PCOM Write System Integers ASCII request
- [ ] PROTOCOL-SCADA PCOM Read System Longs ASCII request
- [ ] PROTOCOL-SCADA PCOM Read Memory Bits ASCII request
- [ ] PROTOCOL-SCADA PCOM Stop Device ASCII request
- [ ] PROTOCOL-SCADA PCOM Write System Longs ASCII request
- [ ] PROTOCOL-SCADA PCOM Write Memory Bits ASCII request
- [ ] PROTOCOL-SCADA PCOM Write Memory Longs ASCII request
- [ ] PROTOCOL-SCADA PCOM Read Operands binary request
- [ ] PROTOCOL-SCADA PCOM Get RTC ASCII reply
- [ ] PROTOCOL-SCADA PCOM Write Data Table binary request
- [ ] PROTOCOL-SCADA PCOM Read Data Table binary request
- [ ] PROTOCOL-SCADA PCOM Set RTC ASCII reply
- [ ] PROTOCOL-SCADA PCOM Read System Bits ASCII reply
- [ ] PROTOCOL-SCADA PCOM Read System Integers ASCII reply
- [ ] PROTOCOL-SCADA PCOM Read Memory Bits ASCII reply
- [ ] PROTOCOL-SCADA PCOM Write Memory Bits ASCII reply
- [ ] PROTOCOL-SCADA PCOM Write System Bits ASCII reply
- [ ] PROTOCOL-SCADA PCOM Write Memory Integers ASCII reply
- [ ] PROTOCOL-SCADA PCOM Read Operands binary reply
- [ ] PROTOCOL-SCADA PCOM Write Data Table binary reply
- [ ] PUA-ADWARE Osx.Adware.FairyTail variant outbound connection detected
- [ ] PUA-ADWARE Osx.Adware.MacSearch variant outbound connection detected
- [ ] SERVER-WEBAPP Magecart inbound scan for vulnerable plugin attempt
- [x] MALWARE-CNC Win.Trojan.Zebrocy variant outbound connection
- [ ] SERVER-WEBAPP Orange LiveBox unauthorized credentials access attempt
- [x] MALWARE-CNC Win.Trojan.Fakewmi variant outbound connection attempt
- [x] MALWARE-CNC Win.Trojan.SectorA05 outbound connection attempt
- [x] MALWARE-CNC Win.Trojan.SectorA05 outbound connection attempt
- [x] MALWARE-CNC Win.Ransomware.Lockergoga binary download attempt
- [x] MALWARE-CNC Win.Ransomware.Lockergoga binary download attempt
- [x] MALWARE-CNC Win.Ransomware.Lockergoga binary download attempt
- [x] MALWARE-CNC Win.Trojan.Zacinlo outbound connection
- [ ] SERVER-WEBAPP Tpshop remote file include attempt
- [ ] SERVER-WEBAPP LG-Ericsson iPECS NMS 30M directory traversal attempt
- [ ] SERVER-WEBAPP LG-Ericsson iPECS NMS 30M directory traversal attempt
- [x] OS-WINDOWS Microsoft Windows RDP MS_T120 channel bind attempt
- [x] MALWARE-CNC Win.Trojan.TeamBot outbound cnc connection
- [x] MALWARE-CNC Win.Trojan.TeamBot outbound cnc connection
- [x] MALWARE-CNC Win.Trojan.TeamBot outbound cnc connection

- [x] MALWARE-CNC Win.Downloader.TeamBot outbound cnc connection
- [x] MALWARE-BACKDOOR Win.Backdoor.Chopper webshell inbound request attempt
- [x] MALWARE-CNC Win.Downloader.TeamBot additional payload download attempt
- [x] MALWARE-CNC Unix.Backdoor.Godlua variant outbound connection
- [x] MALWARE-CNC Win.Dropper.Clipbanker variant outbound connection
- [x] MALWARE-OTHER ANDR.Trojan.Agent outbound connection attempt
- [x] MALWARE-CNC Win.Trojan.BlackRAT variant inbound connection
- [x] MALWARE-CNC Win.Trojan.ModularInstaller variant outbound connection detected
- [x] MALWARE-CNC Win.Trojan.ModularInstaller variant outbound connection detected
- [x] MALWARE-CNC Win.Trojan.ModularInstaller variant outbound connection detected
- [x] MALWARE-CNC Osx.Trojan.Gmera variant outbound connection
- [x] MALWARE-CNC Win.Trojan.Silence variant outbound connection detected
- [ ] OS-LINUX Red Hat NetworkManager DHCP client command injection attempt
- [x] MALWARE-OTHER Xml.Phishing.Evernote outbound connection
- [x] FILE-IDENTIFY Portable Executable binary file magic detected
- [x] MALWARE-CNC Win.Trojan.XpertRAT inbound connection
- [x] SERVER-WEBAPP Citrix ADC and Gateway arbitrary code execution attempt
- [ ] INDICATOR-COMPROMISE RTF document with Equation and BITSAdmin download attempt
- [ ] MALWARE-CNC Win.Trojan.FormBook variant outbound connection
- [x] MALWARE-CNC Win.Trojan.Copperhedge outbound connection
- [x] MALWARE-CNC Unix.Malware.Drovorub cnc inbound connection attempt
- [ ] MALWARE-TOOLS GhostPack Rubeus kerberos request attempt
- [ ] MALWARE-CNC Win.Backdoor.SSLBeacon variant certificate exchange attempt
- [ ] MALWARE-CNC Cobalt Strike DNS beacon inbound TXT record
- [ ] MALWARE-BACKDOOR MultiOS.Malware.GORAT malware download attempt
- [ ] MALWARE-CNC MultiOS.Malware.GORAT outbound communications attempt
- [ ] MALWARE-CNC Win.Backdoor.CSBundle_Original stager outbound connection attempt
- [ ] MALWARE-CNC Win.Backdoor.CSBundle_Original Stager 2 download attempt
- [ ] MALWARE-CNC Win.Backdoor.CSBundle_Original outbound connection attempt
- [x] MALWARE-CNC Rat.Tool.CSBundleUSATodayServer variant inbound command attempt
- [ ] MALWARE-OTHER Cobalt Strike beacon inbound connection attempt
- [ ] MALWARE-OTHER Cobalt Strike beacon outbound connection attempt
- [ ] MALWARE-CNC Rat.Tool.FeyeYelp variant outbound beacon attempt
- [ ] MALWARE-BACKDOOR Cobalt Strike beacon connection attempt
- [ ] MALWARE-CNC Cobalt Strike beacon outbound connection attempt
- [x] MALWARE-CNC MultiOS.Malware.GORAT outbound communication attempt
- [x] MALWARE-CNC MultiOS.Malware.GORAT command and control SSL certificate
- [ ] MALWARE-CNC Win.Trojan.BasicPipeShell variant communication attempt
- [x] SERVER-MAIL Microsoft Exchange Server arbitrary file write attempt
- [ ] POLICY-OTHER F5 iControl REST interface tm.util.bash invocation attempt
- [x] MALWARE-BACKDOOR Win.Backdoor.Chopper webshell inbound request attempt
- [x] MALWARE-CNC User-Agent known malicious user agent - BURAN - Win.Trojan.Buran
- [x] MALWARE-CNC Win.Downloader.TeamBot outbound cnc connection
- [ ] SERVER-OTHER OpenBSD ISAKMP denial of service attempt
- [x] MALWARE-BACKDOOR Win.Backdoor.Agent webshell inbound request attempt
- [x] MALWARE-CNC Win.Trojan.BlackRAT variant outbound connection
- [x] MALWARE-CNC Win.Trojan.ModularInstaller variant outbound connection detected
- [x] MALWARE-CNC Win.Trojan.ModularInstaller variant outbound connection detected
- [x] MALWARE-CNC Win.Trojan.ModularInstaller variant outbound connection detected
- [x] MALWARE-CNC Win.Trojan.Amadey botnet outbound connection
- [x] MALWARE-CNC Win.Trojan.Silence variant outbound connection detected
- [x] MALWARE-CNC Andr.Trojan.Moonshine outbound connection
- [x] MALWARE-OTHER Xml.Phishing.Evernote outbound connection
- [x] FILE-IDENTIFY Portable Executable binary file magic detected
- [x] MALWARE-CNC Js.Trojan.FakeUpdate outbound connection
- [x] MALWARE-CNC Win.Trojan.XpertRAT outbound connection
- [x] SERVER-APACHE Apache Tomcat AJP connector arbitrary file access attempt
- [ ] INDICATOR-COMPROMISE RTF document with Equation and BITSAdmin download attempt
- [x] MALWARE-CNC Win.Trojan.Copperhedge outbound connection
- [x] MALWARE-CNC Win.Trojan.Copperhedge outbound connection
- [ ] MALWARE-TOOLS GhostPack Rubeus kerberos request attempt
- [ ] MALWARE-TOOLS GhostPack Rubeus kerberos request attempt
- [ ] MALWARE-CNC Cobalt Strike DNS beacon inbound TXT record
- [ ] MALWARE-BACKDOOR MultiOS.Malware.GORAT malware download attempt
- [ ] MALWARE-CNC MultiOS.Malware.GORAT outbound communications attempt
- [ ] MALWARE-CNC Win.Backdoor.CSBundle_Original inbound connection attempt
- [ ] MALWARE-CNC Win.Backdoor.CSBundle_Original outbound connection attempt
- [ ] MALWARE-CNC Win.Backdoor.CSBundle_Original Server 3 inbound beacon attempt
- [x] MALWARE-CNC Rat.Tool.CSBundleUSATodayServer variant inbound command attempt
- [ ] MALWARE-CNC potential Rat.Tool.CSBundleUSAToday connectivity check
- [ ] MALWARE-OTHER Cobalt Strike beacon outbound connection attempt
- [ ] MALWARE-OTHER Cobalt Strike beacon outbound connection attempt
- [ ] MALWARE-CNC Rat.Tool.FeyeYelp variant outbound beacon attempt
- [ ] MALWARE-CNC Cobalt Strike beacon outbound connection attempt
- [ ] MALWARE-CNC Cobalt Strike beacon inbound connection attempt
- [x] MALWARE-CNC MultiOS.Malware.GORAT command and control response attempt
- [ ] MALWARE-CNC Win.Trojan.BasicPipeShell variant communication attempt
- [ ] SERVER-OTHER HP Web JetAdmin file write attempt
- [x] SERVER-MAIL Microsoft Exchange Server arbitrary file write attempt
- [x] MALWARE-BACKDOOR Perl.Backdoor.PULSECHECK variant cnc connection

- ☐ MALWARE-BACKDOOR Perl.Backdoor.STEADYPULSE webshell variant access
- ☑ MALWARE-BACKDOOR Perl.Backdoor.HARDPULSE variant inbound cnc connection
- ☑ MALWARE-BACKDOOR Perl.Backdoor.ATRIUM variant inbound cnc connection
- ☑ MALWARE-BACKDOOR Perl.Backdoor.SLIGHTPULSE variant inbound cnc connection
- ☐ OS-WINDOWS Microsoft Windows HTTP protocol stack remote code execution attempt
- ☑ INDICATOR-COMPROMISE Revil Kaseya ransomware log clearing http upload
- ☑ SERVER-WEBAPP Microsoft Exchange autodiscover server side request forgery attempt
- ☑ SERVER-WEBAPP Microsoft Exchange autodiscover server side request forgery attempt
- ☐ OS-WINDOWS Microsoft Windows Content-Disposition CLSID command attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☐ INDICATOR-COMPROMISE JNDI LDAP searchResEntry dynamic code download attempt
- ☐ OS-WINDOWS Microsoft Windows Server 2003 smart card authentication buffer overflow attempt
- ☑ SERVER-WEBAPP Multiple products OGNL expression injection attempt
- ☑ MALWARE-BACKDOOR Jsp.Webshell.TinyUploader upload attempt
- ☑ MALWARE-BACKDOOR Jsp.Webshell.Behinder download attempt
- ☑ MALWARE-BACKDOOR Jsp.Webshell.Chopper upload attempt
- ☑ MALWARE-BACKDOOR Jsp.Webshell.Noop upload attempt
- ☑ SERVER-WEBAPP Atlassian Confluence OGNL expression injection attempt
- ☑ SERVER-WEBAPP Atlassian Confluence OGNL expression injection attempt
- ☑ SERVER-OTHER OpenSSL x509 crafted email address buffer overflow attempt

- ☐ MALWARE-BACKDOOR Perl.Backdoor.STEADYPULSE webshell variant access
- ☑ MALWARE-BACKDOOR Perl.Backdoor.STEADYPULSE variant inbound cnc connection
- ☑ MALWARE-BACKDOOR Perl.Backdoor.SLIGHTPULSE variant inbound cnc connection
- ☑ MALWARE-BACKDOOR Perl.Backdoor.ATRIUM variant inbound cnc connection
- ☐ POLICY-OTHER Active Directory Federation Services policy store transfer service request detected
- ☑ SERVER-WEBAPP Microsoft Exchange autodiscover server side request forgery attempt
- ☑ SERVER-WEBAPP Microsoft Exchange autodiscover server side request forgery attempt
- ☐ OS-WINDOWS Microsoft Windows Content-Disposition CLSID command attempt
- ☐ OS-WINDOWS Microsoft Windows Content-Disposition CLSID command attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☑ SERVER-OTHER Apache Log4j logging remote code execution attempt
- ☐ POLICY-OTHER Java User-Agent remote class download attempt
- ☑ SERVER-WEBAPP F5 BIG-IP iControl remote code execution attempt
- ☑ INDICATOR-COMPROMISE Python remote shell spawn attempt
- ☑ MALWARE-BACKDOOR Jsp.Webshell.Chopper webshell download attempt
- ☑ MALWARE-BACKDOOR Jsp.Webshell.Noop download attempt
- ☑ MALWARE-BACKDOOR Jsp.Webshell.Behinder upload attempt
- ☑ SERVER-WEBAPP Atlassian Confluence OGNL expression injection attempt
- ☑ SERVER-WEBAPP Atlassian Confluence OGNL expression injection attempt
- ☑ SERVER-WEBAPP Microsoft Exchange Server remote code execution attempt
- ☐ MALWARE-CNC Win.Dropper.Gamaredon command and control beacon attempt

- [x] SERVER-WEBAPP Atlassian Confluence remote code execution attempt
- [x] SERVER-WEBAPP Atlassian Confluence remote code execution attempt

- [x] **emerging-3coresec.rules** Hide
  - [x] ET 3CORESec Poor Reputation IP group 1
  - [x] ET 3CORESec Poor Reputation IP group 2
  - [x] ET 3CORESec Poor Reputation IP group 3
  - [x] ET 3CORESec Poor Reputation IP group 4
  - [x] ET 3CORESec Poor Reputation IP group 5
  - [x] ET 3CORESec Poor Reputation IP group 6
  - [x] ET 3CORESec Poor Reputation IP group 7
  - [x] ET 3CORESec Poor Reputation IP group 8
  - [x] ET 3CORESec Poor Reputation IP group 9
  - [x] ET 3CORESec Poor Reputation IP group 10
  - [x] ET 3CORESec Poor Reputation IP group 11
  - [x] ET 3CORESec Poor Reputation IP group 12
- [ ] **emerging-activex.rules** Show
- [x] **emerging-adware_pup.rules** Hide
  - [ ] ET ADWARE_PUP Gator Cookie
  - [ ] ET ADWARE_PUP Gator Agent Traffic
  - [ ] ET ADWARE_PUP Binet (download complete)
  - [ ] ET ADWARE_PUP Binet (set_pix)
  - [ ] ET ADWARE_PUP Binet (randreco.exe)
  - [ ] ET ADWARE_PUP User-Agent (iexplore)
  - [ ] ET ADWARE_PUP IE homepage hijacking
  - [ ] ET ADWARE_PUP shell browser vulnerability W9x/XP
  - [ ] ET ADWARE_PUP shell browser vulnerability NT/2K
  - [ ] ET ADWARE_PUP Bargain Buddy
  - [ ] ET ADWARE_PUP Shop At Home Select.com Install Attempt
  - [ ] ET ADWARE_PUP Shop At Home Select.com Install Download
  - [ ] ET ADWARE_PUP F1Organizer Reporting
  - [ ] ET ADWARE_PUP Mindset Interactive Install (1)
  - [ ] ET ADWARE_PUP Mindset Interactive Install (2)
  - [ ] ET ADWARE_PUP F1Organizer Install Attempt
  - [x] ET ADWARE_PUP Ezula Related User-Agent (mez)
  - [ ] ET ADWARE_PUP SpywareLabs VirtualBouncer Seeking Instructions
  - [ ] ET ADWARE_PUP TopMoxie Reporting Data to External Host
  - [ ] ET ADWARE_PUP TopMoxie Retrieving Data (downloads)
  - [ ] ET ADWARE_PUP TopMoxie Retrieving Data (common)
  - [ ] ET ADWARE_PUP Binet Ad Retrieval
  - [x] ET ADWARE_PUP Gator/Claria Data Submission
  - [ ] ET ADWARE_PUP Gator New Code Download
  - [ ] ET ADWARE_PUP Fun Web Products Install
  - [ ] ET ADWARE_PUP MyWebSearch Toolbar Receiving Configuration
  - [ ] ET ADWARE_PUP Salongas Infection
  - [ ] ET ADWARE_PUP MarketScore.com Spyware Configuration Access
  - [ ] ET ADWARE_PUP Avres Agent Receiving Instructions
  - [ ] ET ADWARE_PUP WhenUClick.com App and Search Bar Install (1)
  - [ ] ET ADWARE_PUP WhenUClick.com App and Search Bar Install (2)
  - [ ] ET ADWARE_PUP WhenUClick.com Clock Sync App Checkin
  - [ ] ET ADWARE_PUP WhenUClick.com Weather App Checkin
  - [ ] ET ADWARE_PUP WhenUClick.com Clock Sync App Checkin (1)
  - [ ] ET ADWARE_PUP WhenUClick.com Clock Sync App Checkin (2)
  - [ ] ET ADWARE_PUP WhenUClick.com Weather App Checkin (1)
  - [ ] ET ADWARE_PUP WhenUClick.com Weather App Checkin (2)
  - [ ] ET ADWARE_PUP WhenUClick.com WhenUSave App Checkin
  - [ ] ET ADWARE_PUP WhenUClick.com WhenUSave Data Retrieval (offersdata)
  - [ ] ET ADWARE_PUP WhenUClick.com Desktop Bar Install
  - [ ] ET ADWARE_PUP WhenUClick.com WhenUSave Data Retrieval (Searchdb)
  - [ ] ET ADWARE_PUP Hotbar Install (1)
  - [ ] ET ADWARE_PUP Hotbar Install (2)
  - [ ] ET ADWARE_PUP Hotbar Install (3)
  - [ ] ET ADWARE_PUP Hotbar Agent Reporting Information
  - [ ] ET ADWARE_PUP Hotbar Agent Upgrading
  - [ ] ET ADWARE_PUP Hotbar Agent Partner Checkin
  - [ ] ET ADWARE_PUP ISearchTech.com XXXPornToolbar Reporting
  - [ ] ET ADWARE_PUP ISearchTech.com XXXPornToolbar Activity (1)
  - [ ] ET ADWARE_PUP Hotbar Agent Activity
  - [ ] ET ADWARE_PUP Comet Systems Spyware Traffic
  - [ ] ET ADWARE_PUP Keenvalue Update Engine
  - [ ] ET ADWARE_PUP FlashTrack Agent Retrieving New App Code
  - [ ] ET ADWARE_PUP Fun Web Products SmileyCentral
  - [ ] ET ADWARE_PUP SideStep Bar Install
  - [ ] ET ADWARE_PUP SideStep Bar Reporting Data
  - [x] ET ADWARE_PUP Casino on Net Reporting Data
  - [ ] ET ADWARE_PUP Casino on Net Ping Hit
  - [ ] ET ADWARE_PUP Casino on Net Data Download
  - [ ] ET ADWARE_PUP Ebates Install
  - [ ] ET ADWARE_PUP Casino on Net Install
  - [ ] ET ADWARE_PUP UPX encrypted file download possible malware
  - [ ] ET ADWARE_PUP CometSystems Spyware
  - [ ] ET ADWARE_PUP Twaintec Download Attempt
  - [ ] ET ADWARE_PUP Twaintec Ad Retrieval
  - [ ] ET ADWARE_PUP Twaintec Reporting Data
  - [ ] ET ADWARE_PUP F1Organizer Config Download
  - [x] ET ADWARE_PUP Regnow.com Access
  - [ ] ET ADWARE_PUP Regnow.com Gamehouse.com Access
  - [ ] ET ADWARE_PUP Statblaster Receiving New configuration (update)
  - [ ] ET ADWARE_PUP Advertising.com Data Post (villains)
  - [ ] ET ADWARE_PUP Advertising.com Data Post (cakedeal)
  - [x] ET ADWARE_PUP Gator/Clarian Agent
  - [ ] ET ADWARE_PUP Wild Tangent Agent Installation
  - [ ] ET ADWARE_PUP Internet Optomizer Reporting Data
  - [ ] ET ADWARE_PUP Wild Tangent Agent Checking In
  - [ ] ET ADWARE_PUP Wild Tangent Agent Traffic
  - [ ] ET ADWARE_PUP Rdxrp.com Traffic
  - [ ] ET ADWARE_PUP Traffic Syndicate Add/Remove
  - [ ] ET ADWARE_PUP Wild Tangent Agent
  - [ ] ET ADWARE_PUP Traffic Syndicate Agent Updating (1)
  - [ ] ET ADWARE_PUP Traffic Syndicate Agent Updating (2)
  - [x] ET ADWARE_PUP Webhancer Data Upload
  - [ ] ET ADWARE_PUP Speedera Agent (Specific)
  - [ ] ET ADWARE_PUP Wild Tangent New Install
  - [x] ET ADWARE_PUP Websearch.com Spyware
  - [x] ET ADWARE_PUP Ezula Install .exe
  - [ ] ET ADWARE_PUP Ezula Installer Download
  - [x] ET ADWARE_PUP BInet Information Upload
  - [ ] ET ADWARE_PUP LocalNRD Spyware Checkin
  - [ ] ET ADWARE_PUP OfferOptimizer.com Spyware
  - [ ] ET ADWARE_PUP Bonziportal Traffic
  - [ ] ET ADWARE_PUP MarketScore.com Spyware Access
  - [x] ET ADWARE_PUP ISearchTech.com XXXPornToolbar Activity (2)
  - [ ] ET ADWARE_PUP Internet Optimizer Spyware Install
  - [ ] ET ADWARE_PUP Bfast.com Spyware
  - [ ] ET ADWARE_PUP E2give Related Reporting Install
  - [ ] ET ADWARE_PUP E2give Related Receiving Config
  - [x] ET ADWARE_PUP E2give Related Downloading Code
  - [ ] ET ADWARE_PUP E2give Related Reporting
  - [ ] ET ADWARE_PUP Abox Download
  - [ ] ET ADWARE_PUP Abox Install Report
  - [ ] ET ADWARE_PUP Statblaster.MemoryWatcher Download
  - [ ] ET ADWARE_PUP Overpro Spyware Bundle Install

- [ ] ET ADWARE_PUP 2nd-thought (W32.Daqa.C) Download
- [ ] ET ADWARE_PUP Wintools Download/Configure
- [ ] ET ADWARE_PUP Bundleware Spyware CHM Download
- [ ] ET ADWARE_PUP Couponage Configure
- [ ] ET ADWARE_PUP Bundleware Spyware cab Download
- [ ] ET ADWARE_PUP Sexmaniack Install Tracking
- [ ] ET ADWARE_PUP Xpire.info Multiple Spyware Installs Occuring
- [ ] ET ADWARE_PUP Xpire.info Multiple Spyware Installs (3)
- [ ] ET ADWARE_PUP Xpire.info Multiple Spyware Installs (5)
- [ ] ET ADWARE_PUP Xpire.info Multiple Spyware Installs (6)
- [ ] ET ADWARE_PUP Xpire.info Spyware Exploit
- [x] ET ADWARE_PUP Searchmeup Spyware Install (prog)
- [ ] ET ADWARE_PUP Coolsearch Spyware Install
- [ ] ET ADWARE_PUP MediaTickets Spyware Install
- [x] ET ADWARE_PUP Searchmeup Spyware Install (mstask)
- [ ] ET ADWARE_PUP thebestsoft4u.com Spyware Install (2)
- [ ] ET ADWARE_PUP Spygalaxy.ws Spyware Checkin
- [ ] ET ADWARE_PUP Xpire.info Spyware Checkin
- [x] ET ADWARE_PUP Clickspring.net Spyware Reporting Successful Install
- [x] ET ADWARE_PUP Outerinfo.com Spyware Advertising Campaign Download
- [x] ET ADWARE_PUP Internet Optimizer Activity User-Agent (IOKernel)
- [x] ET ADWARE_PUP Clickspring.net Spyware Reporting
- [ ] ET ADWARE_PUP Medialoads.com Spyware Config
- [ ] ET ADWARE_PUP Medialoads.com Spyware Identifying Country of Origin
- [ ] ET ADWARE_PUP SurfAssistant.com Spyware Install
- [ ] ET ADWARE_PUP SurfAssistant.com Spyware Reporting
- [ ] ET ADWARE_PUP Websearch.com Outbound Dialer Retrieval
- [ ] ET ADWARE_PUP Spywaremover Activity
- [ ] ET ADWARE_PUP Virtumonde Spyware Code Download mmdom.exe
- [ ] ET ADWARE_PUP ak-networks.com Spyware Code Download
- [x] ET ADWARE_PUP Searchmiracle.com Spyware Install (silent_install)
- [ ] ET ADWARE_PUP Spyspotter.com Install
- [ ] ET ADWARE_PUP Oenji.com Install
- [ ] ET ADWARE_PUP Searchmiracle.com Spyware Install (v3cab)
- [x] ET ADWARE_PUP Suspected PUP/PUA User-Agent (OSSProxy)
- [x] ET ADWARE_PUP PUP/PUA OSSProxy HTTP Header
- [ ] ET ADWARE_PUP Spyware Stormer/Error Guard Activity
- [ ] ET ADWARE_PUP MarketScore.com Spyware Proxied Traffic (mitmproxy agent)
- [ ] ET ADWARE_PUP MarketScore.com Spyware Activity (1)
- [ ] ET ADWARE_PUP Microgaming.com Spyware Installation (dlhelper)
- [ ] ET ADWARE_PUP Microgaming.com Spyware Reporting Installation
- [ ] ET ADWARE_PUP Toprebates.com Install (1)
- [ ] ET ADWARE_PUP Toprebates.com User Confirming Membership
- [ ] ET ADWARE_PUP Search Scout Related Spyware (results)
- [ ] ET ADWARE_PUP GlobalPhon.com Dialer
- [ ] ET ADWARE_PUP Comet Systems Spyware Reporting
- [ ] ET ADWARE_PUP GlobalPhon.com Dialer (add_ocx)
- [x] ET ADWARE_PUP Webhancer Data Post
- [ ] ET ADWARE_PUP Windows executable sent when remote host claims to send an image
- [ ] ET ADWARE_PUP ISearchTech Toolbar Data Submission
- [ ] ET ADWARE_PUP Windupdates.com Spyware Install
- [x] ET ADWARE_PUP Shop at Home Select Spyware User-Agent (Bundle)
- [x] ET ADWARE_PUP Context Plus Spyware Install
- [x] ET ADWARE_PUP Context Plus Spyware User-Agent (Envolo)
- [ ] ET ADWARE_PUP Shop at Home Select Spyware Heartbeat
- [ ] ET ADWARE_PUP Tibsystems Spyware Install (1)
- [x] ET ADWARE_PUP SurfSidekick Activity
- [ ] ET ADWARE_PUP A-d-w-a-r-e.com Activity (cmd)
- [ ] ET ADWARE_PUP ak-networks.com Spyware Code Install
- [x] ET ADWARE_PUP Enhance My Search Spyware User-Agent (HelperH)
- [ ] ET ADWARE_PUP Pynix.dll BHO Activity
- [x] ET ADWARE_PUP MediaTickets Download
- [ ] ET ADWARE_PUP Bundleware Spyware Download
- [ ] ET ADWARE_PUP Couponage Download
- [ ] ET ADWARE_PUP ContextPanel Reporting
- [ ] ET ADWARE_PUP Overpro Spyware Games
- [ ] ET ADWARE_PUP Xpire.info Multiple Spyware Installs (1)
- [ ] ET ADWARE_PUP Xpire.info Multiple Spyware Installs (2)
- [ ] ET ADWARE_PUP Xpire.info Multiple Spyware Installs (4)
- [ ] ET ADWARE_PUP Xpire.info Multiple Spyware Installs CHM Exploit
- [ ] ET ADWARE_PUP Xpire.info Multiple Spyware Installs (7)
- [x] ET ADWARE_PUP Xpire.info Spyware Install Reporting
- [x] ET ADWARE_PUP Searchmeup Spyware Receiving Commands
- [x] ET ADWARE_PUP Searchmeup Spyware Install (systime)
- [ ] ET ADWARE_PUP thebestsoft4u.com Spyware Install (1)
- [ ] ET ADWARE_PUP Searchmeup Spyware Install (d.exe)
- [x] ET ADWARE_PUP Tibsystems Spyware Download
- [ ] ET ADWARE_PUP ICQ-Update.biz Reporting Install
- [x] ET ADWARE_PUP ISearchTech.com XXXPornToolbar Activity (IST)
- [ ] ET ADWARE_PUP Outerinfo.com Spyware Install
- [x] ET ADWARE_PUP Outerinfo.com Spyware Activity
- [x] ET ADWARE_PUP Look2me Spyware Activity (1)
- [ ] ET ADWARE_PUP Clickspring.net Spyware Reporting
- [ ] ET ADWARE_PUP Smartpops.com Spyware Install rh.exe
- [ ] ET ADWARE_PUP Medialoads.com Spyware Reporting (register.cgi)
- [ ] ET ADWARE_PUP Smartpops.com Spyware Update
- [ ] ET ADWARE_PUP Smartpops.com Spyware Install
- [ ] ET ADWARE_PUP Spywaremover Activity
- [ ] ET ADWARE_PUP SpywareLabs Application Install
- [ ] ET ADWARE_PUP Virtumonde Spyware Code Download bkinst.exe
- [x] ET ADWARE_PUP Searchmiracle.com Spyware Installer silent.exe Download
- [x] ET ADWARE_PUP Searchmiracle.com Spyware Install (protector.exe)
- [ ] ET ADWARE_PUP Spyspotter.com Access
- [ ] ET ADWARE_PUP Spyspotter.com Access Likely Spyware
- [ ] ET ADWARE_PUP Xpire.info Install Report
- [ ] ET ADWARE_PUP MarketScore.com Spyware SSL Access
- [ ] ET ADWARE_PUP Spyware Stormer Reporting Data
- [x] ET ADWARE_PUP BInet Information Install Report
- [ ] ET ADWARE_PUP MarketScore.com Spyware Upgrading
- [ ] ET ADWARE_PUP MarketScore.com Spyware Activity (2)
- [ ] ET ADWARE_PUP Microgaming.com Spyware Installation (2)
- [ ] ET ADWARE_PUP Microgaming.com Spyware Casino App Install
- [ ] ET ADWARE_PUP Toprebates.com Install (2)
- [ ] ET ADWARE_PUP Search Scout Related Spyware (content)
- [ ] ET ADWARE_PUP Comet Systems Spyware Traffic (context.xml)
- [ ] ET ADWARE_PUP GlobalPhon.com Dialer Download
- [ ] ET ADWARE_PUP GlobalPhon.com Dialer (no_pop)
- [ ] ET ADWARE_PUP Metarewards Spyware Activity
- [ ] ET ADWARE_PUP Webhancer Agent Activity
- [ ] ET ADWARE_PUP Search Relevancy Spyware
- [x] ET ADWARE_PUP YourSiteBar User-Agent (istsvc)
- [ ] ET ADWARE_PUP Windupdates.com Spyware Loggin Data
- [x] ET ADWARE_PUP Context Plus Spyware User-Agent (Apropos)
- [ ] ET ADWARE_PUP Flingstone Spyware Install (sportsinteraction)
- [x] ET ADWARE_PUP Shop at Home Select Spyware User-Agent (SAH)
- [ ] ET ADWARE_PUP Flingstone Spyware Install (cxtpls)
- [ ] ET ADWARE_PUP A-d-w-a-r-e.com Activity (popup)
- [ ] ET ADWARE_PUP Tibsystems Spyware Install (2)
- [x] ET ADWARE_PUP UCMore Spyware User-Agent (UCmore)
- [ ] ET ADWARE_PUP Searchmiracle.com Spyware Install (install)
- [ ] ET ADWARE_PUP My-Stats.com Spyware Checkin
- [x] ET ADWARE_PUP ABX Toolbar ActiveX Install

- [x] ET ADWARE_PUP Media Pass ActiveX Install
- [ ] ET ADWARE_PUP Incredisearch.com Spyware Activity
- [ ] ET ADWARE_PUP 404Search Spyware User-Agent (404search)
- [x] ET ADWARE_PUP EZULA Spyware User Agent
- [x] ET ADWARE_PUP Hotbar Spyware User-Agent (Hotbar)
- [x] ET ADWARE_PUP MyWebSearch Spyware User-Agent (MyWebSearch)
- [x] ET ADWARE_PUP Spyware User-Agent (sureseeker)
- [ ] ET ADWARE_PUP Surfplayer Spyware User-Agent (SurferPlugin)
- [x] ET ADWARE_PUP Visicom Spyware User-Agent (Visicom)
- [ ] ET ADWARE_PUP Begin2Search.com Spyware
- [ ] ET ADWARE_PUP ToolbarPartner Spyware Spambot Retrieving Target Emails
- [x] ET ADWARE_PUP SurfSidekick Download
- [x] ET ADWARE_PUP UCMore Spyware Reporting
- [ ] ET ADWARE_PUP TargetNetworks.net Spyware Reporting (req)
- [ ] ET ADWARE_PUP BTGrab.com Spyware Downloading Ads
- [x] ET ADWARE_PUP 180solutions Spyware Keywords Download
- [ ] ET ADWARE_PUP 180solutions Spyware Install
- [x] ET ADWARE_PUP Better Internet Spyware User-Agent (poller)
- [ ] ET ADWARE_PUP ESyndicate Spyware Install (esyndicateinst.exe)
- [ ] ET ADWARE_PUP GrandstreetInteractive.com Install
- [ ] ET ADWARE_PUP Internet Fuel.com Install
- [ ] ET ADWARE_PUP Overpro Spyware Install Report
- [x] ET ADWARE_PUP Grandstreet Interactive Spyware User-Agent (IEP)
- [ ] ET ADWARE_PUP Shop at Home Select Spyware Install
- [ ] ET ADWARE_PUP Topconverting Spyware Reporting
- [ ] ET ADWARE_PUP TargetNetworks.net Spyware Reporting (tn)
- [ ] ET ADWARE_PUP XupiterToolbar Spyware User-Agent (XupiterToolbar)
- [x] ET ADWARE_PUP MySearch Products Spyware User-Agent (MySearch)
- [ ] ET ADWARE_PUP C4tdownload.com Spyware Activity
- [ ] ET ADWARE_PUP IEHelp.net Spyware Installer
- [x] ET ADWARE_PUP yupsearch.com Spyware Install - protector.exe
- [ ] ET ADWARE_PUP CWS qck.cc Spyware Installer (web.php)
- [x] ET ADWARE_PUP yupsearch.com Spyware Install - sideb.exe
- [x] ET ADWARE_PUP CoolWebSearch Spyware (Feat)
- [ ] ET ADWARE_PUP iWon Spyware (iWonSearchAssistant)
- [ ] ET ADWARE_PUP Searchfeed.com Spyware 1
- [ ] ET ADWARE_PUP Searchfeed.com Spyware 3
- [ ] ET ADWARE_PUP Searchfeed.com Spyware 5
- [ ] ET ADWARE_PUP Searchfeed.com Spyware 7
- [ ] ET ADWARE_PUP Fun Web Products Smileychooser Spyware
- [ ] ET ADWARE_PUP Fun Web Products Smileychooser Spyware
- [ ] ET ADWARE_PUP EZSearch Spyware Reporting Search Category
- [ ] ET ADWARE_PUP Transponder Spyware Activity
- [ ] ET ADWARE_PUP Alexa Spyware Reporting URL
- [ ] ET ADWARE_PUP Comet Systems Spyware Update Download
- [ ] ET ADWARE_PUP 180solutions Spyware versionconfig POST
- [x] ET ADWARE_PUP Miva User-Agent (TPSystem)
- [x] ET ADWARE_PUP Spyware Related User-Agent (UtilMind HTTPGet)
- [ ] ET ADWARE_PUP Movies-etc User-Agent (IOInstall)
- [ ] ET ADWARE_PUP iframebiz - sploit.anr
- [x] ET ADWARE_PUP iframebiz - loadadv***.exe
- [ ] ET ADWARE_PUP Trafficsector.com Spyware Install
- [ ] ET ADWARE_PUP SurfSidekick Activity (rinfo)
- [ ] ET ADWARE_PUP adservs.com Spyware
- [ ] ET ADWARE_PUP Corpsespyware.net Distribution - bos.biz
- [ ] ET ADWARE_PUP Corpsespyware.net - msits.exe access
- [ ] ET ADWARE_PUP Spyaxe Spyware DB Update
- [ ] ET ADWARE_PUP Spyaxe Spyware Checkin
- [ ] ET ADWARE_PUP DelFin Project Spyware (payload)
- [ ] ET ADWARE_PUP Hotbar Agent Subscription POST
- [ ] ET ADWARE_PUP Incredisearch.com Spyware Ping
- [ ] ET ADWARE_PUP Likely Trojan/Spyware Installer Requested (1)
- [x] ET ADWARE_PUP Easy Search Bar Spyware User-Agent (ESB)
- [x] ET ADWARE_PUP Fun Web Products Spyware User-Agent (FunWebProducts)
- [x] ET ADWARE_PUP Fun Web Products Spyware User-Agent (MyWay)
- [ ] ET ADWARE_PUP Search Engine 2000 Spyware User-Agent (searchengine)
- [x] ET ADWARE_PUP Spyware User-Agent (Sidesearch)
- [x] ET ADWARE_PUP Target Saver Spyware User-Agent (TSA)
- [ ] ET ADWARE_PUP DesktopTraffic Toolbar Spyware
- [x] ET ADWARE_PUP ToolbarPartner Spyware Agent Download (1)
- [ ] ET ADWARE_PUP Zenotecnico Adware
- [ ] ET ADWARE_PUP SurfSidekick Activity (ipixel)
- [x] ET ADWARE_PUP UCMore Spyware User-Agent (EI)
- [ ] ET ADWARE_PUP UCMore Spyware Downloading Ads
- [ ] ET ADWARE_PUP Shopnav Spyware Install
- [ ] ET ADWARE_PUP Better Internet Spyware User-Agent (thnall)
- [ ] ET ADWARE_PUP Topconverting Spyware Install
- [ ] ET ADWARE_PUP Wild Tangent Install
- [ ] ET ADWARE_PUP ESyndicate Spyware Install (sepinst.exe)
- [ ] ET ADWARE_PUP GrandstreetInteractive.com Update
- [ ] ET ADWARE_PUP jmnad1.com Spyware Install (2)
- [ ] ET ADWARE_PUP jmnad1.com Spyware Install (1)
- [ ] ET ADWARE_PUP Weird on the Web /180 Solutions Checkin
- [x] ET ADWARE_PUP Shopathomeselect .com Spyware User-Agent (WebDownloader)
- [ ] ET ADWARE_PUP OutBlaze.com Spyware Activity
- [ ] ET ADWARE_PUP 180solutions Spyware Defs Download
- [ ] ET ADWARE_PUP MyWaySearch Products Spyware User Agent
- [ ] ET ADWARE_PUP Pacimedia Spyware 1
- [ ] ET ADWARE_PUP CWS qck.cc Spyware Installer (in.php)
- [ ] ET ADWARE_PUP Searchmiracle.com Spyware Install - silent.exe
- [ ] ET ADWARE_PUP Likely Trojan/Spyware Installer Requested (2)
- [ ] ET ADWARE_PUP IEHelp.net Spyware checkin
- [ ] ET ADWARE_PUP 180solutions Spyware config Download
- [ ] ET ADWARE_PUP Hotbar Spyware User-Agent (host)
- [x] ET ADWARE_PUP Casalemedia Spyware Reporting URL Visited 2
- [ ] ET ADWARE_PUP Searchfeed.com Spyware 2
- [ ] ET ADWARE_PUP Searchfeed.com Spyware 4
- [ ] ET ADWARE_PUP Searchfeed.com Spyware 6
- [ ] ET ADWARE_PUP Searchfeed.com Spyware 8
- [ ] ET ADWARE_PUP Fun Web Products Cursorchooser Spyware
- [ ] ET ADWARE_PUP EZSearch Spyware Reporting Search Strings
- [ ] ET ADWARE_PUP EZSearch Spyware Reporting 2
- [ ] ET ADWARE_PUP VPP Technologies Spyware
- [ ] ET ADWARE_PUP VPP Technologies Spyware Reporting URL
- [ ] ET ADWARE_PUP Comet Systems Spyware Context Report
- [ ] ET ADWARE_PUP Adwave/MarketScore User-Agent (WTA)
- [x] ET ADWARE_PUP Miva Spyware User-Agent (Travel Update)
- [x] ET ADWARE_PUP Context Plus User-Agent (PTS)
- [x] ET ADWARE_PUP Internet Optimizer User-Agent (ROGUE)
- [ ] ET ADWARE_PUP iframebiz - loaderadv***.jar
- [x] ET ADWARE_PUP Zenotecnico Adware 2
- [x] ET ADWARE_PUP Zenotecnico Spyware Install Report
- [x] ET ADWARE_PUP iDownloadAgent Spyware User-Agent (iDownloadAgent)
- [ ] ET ADWARE_PUP Corpsespyware.net BlackList - pcpeek
- [ ] ET ADWARE_PUP Corpsespyware.net Distribution - studiolacase
- [ ] ET ADWARE_PUP Corpsespyware.net - msys.exe access
- [ ] ET ADWARE_PUP Spyaxe Spyware DB Version Check
- [ ] ET ADWARE_PUP Spyaxe Spyware User-Agent (spywareaxe)
- [ ] ET ADWARE_PUP DelFin Project Spyware (setup)
- [ ] ET ADWARE_PUP SideStep Bar Reporting Data (sbstart)

- [ ] ET ADWARE_PUP MyWebSearch Toolbar Traffic (bar config download)
- [x] ET ADWARE_PUP Freeze.com Spyware/Adware (Install)
- [ ] ET ADWARE_PUP Fun Web Products StationaryChooser Spyware
- [ ] ET ADWARE_PUP CWS Spy-Sheriff.com Infeced Buy Page Request
- [x] ET ADWARE_PUP Win32/Tibs Checkin
- [ ] ET ADWARE_PUP Bestcount.net Spyware Initial Infection Download
- [x] ET ADWARE_PUP Dollarrevenue.com Spyware Code Download
- [ ] ET ADWARE_PUP Jupitersatellites.biz Spyware Download
- [ ] ET ADWARE_PUP Possible Spambot Pulling IP List to Spam
- [ ] ET ADWARE_PUP /jk/exp.wmf Exploit Code Load Attempt
- [ ] ET ADWARE_PUP 180solutions Spyware Actionlibs Download
- [ ] ET ADWARE_PUP 180solutions (Zango) Spyware TB Installer Download
- [ ] ET ADWARE_PUP 180solutions (Zango) Spyware Event Activity Post
- [ ] ET ADWARE_PUP Content-loader.com Spyware Install
- [ ] ET ADWARE_PUP Content-loader.com (ownusa.info) Spyware Install
- [ ] ET ADWARE_PUP Fun Web Products SmileyCentral IEsp2 Install
- [ ] ET ADWARE_PUP Bestcount.net Spyware Data Upload
- [ ] ET ADWARE_PUP Thespyguard.com Spyware Update Check
- [ ] ET ADWARE_PUP Thespyguard.com Spyware Updating
- [x] ET ADWARE_PUP Best-targeted-traffic.com Spyware Checkin
- [ ] ET ADWARE_PUP Best-targeted-traffic.com Spyware Ping
- [ ] ET ADWARE_PUP Conduit Connect Toolbar Message Download(Many report to be benign)
- [ ] ET ADWARE_PUP MySearchNow.com Spyware
- [x] ET ADWARE_PUP Megaupload Spyware User-Agent (Megaupload)
- [ ] ET ADWARE_PUP New.net Spyware Checkin
- [ ] ET ADWARE_PUP SpySheriff Intial Phone Home
- [ ] ET ADWARE_PUP Travel Update Spyware
- [ ] ET ADWARE_PUP Effectivebrands.com Spyware Checkin
- [ ] ET ADWARE_PUP Comet Systems Spyware Cursor DL
- [ ] ET ADWARE_PUP Baidu.com Spyware Bar Reporting
- [x] ET ADWARE_PUP Trinityacquisitions.com and Maximumexperience.com Spyware Activity
- [x] ET ADWARE_PUP Errorsafe.com Fake antispyware User-Agent (ErrorSafe)
- [ ] ET ADWARE_PUP Gamehouse.com Activity
- [x] ET ADWARE_PUP MyGlobalSearch Spyware bar update 2
- [ ] ET ADWARE_PUP Yourscreen.com Spyware Download
- [x] ET ADWARE_PUP Freeze.com Spyware Download
- [ ] ET ADWARE_PUP Effectivebrands.com Spyware Checkin 2
- [ ] ET ADWARE_PUP Hotbar Agent Adopt/Zango
- [ ] ET ADWARE_PUP Spy-Not.com Spyware Pulling Fake Sigs
- [ ] ET ADWARE_PUP Spy-Not.com Spyware Updating
- [x] ET ADWARE_PUP SpamBlockerUtility Fake Anti-Spyware User-Agent (SpamBlockerUtility x.x.x)
- [ ] ET ADWARE_PUP Hotbar Keywords Download
- [x] ET ADWARE_PUP SurfAccuracy.com Spyware Updating
- [x] ET ADWARE_PUP Mysearch.com/Morpheus Bar Spyware User-Agent (Morpheus)
- [x] ET ADWARE_PUP Morpheus Spyware Install User-Agent (SmartInstaller)
- [ ] ET ADWARE_PUP WhenUClick.com WhenUSave Data Retrieval (DataChunksGZ)
- [ ] ET ADWARE_PUP Mysearch.com Spyware User-Agent (iMeshBar)
- [ ] ET ADWARE_PUP Epilot.com Spyware Reporting
- [ ] ET ADWARE_PUP CNSMIN (3721.com) Spyware Activity
- [ ] ET ADWARE_PUP CNSMIN (3721.com) Spyware Activity 3
- [x] ET ADWARE_PUP Outerinfo.com Spyware Checkin
- [ ] ET ADWARE_PUP xxxtoolbar.com Spyware Install User-Agent
- [x] ET ADWARE_PUP Dropspam.com Spyware Install User-Agent (DSInstall)
- [x] ET ADWARE_PUP My Search Spyware Config Download
- [x] ET ADWARE_PUP Freeze.com Spyware/Adware (Install Registration)
- [x] ET ADWARE_PUP CWS Trafcool.biz Related Installer
- [ ] ET ADWARE_PUP Bravesentry.com Fake Antispyware Download
- [ ] ET ADWARE_PUP Bestcount.net Spyware Downloading vxgame
- [x] ET ADWARE_PUP Elitemediagroup.net Spyware Config Download
- [ ] ET ADWARE_PUP SpySherriff Spyware Activity
- [ ] ET ADWARE_PUP Possible Spambot Checking in to Spam
- [ ] ET ADWARE_PUP Possible Spambot getting new exe
- [ ] ET ADWARE_PUP PopupSh.ocx Access Attempt
- [ ] ET ADWARE_PUP 180solutions (Zango) Spyware Installer Download
- [x] ET ADWARE_PUP 180solutions (Zango) Spyware Local Stats Post
- [ ] ET ADWARE_PUP 180 Solutions (Zango Installer) User Agent
- [ ] ET ADWARE_PUP Content-loader.com Spyware Install 2
- [ ] ET ADWARE_PUP TROJAN_VB Microjoin
- [ ] ET ADWARE_PUP Bestcount.net Spyware Exploit Download
- [ ] ET ADWARE_PUP Thespyguard.com Spyware Install
- [ ] ET ADWARE_PUP Hitvirus Fake AV Install
- [ ] ET ADWARE_PUP User-Agent (Informer from RBC)
- [x] ET ADWARE_PUP Best-targeted-traffic.com Spyware Install
- [ ] ET ADWARE_PUP 180solutions (Zango) Spyware Installer Config 2
- [ ] ET ADWARE_PUP Alexa Spyware Reporting
- [ ] ET ADWARE_PUP MyWebSearch Toolbar Receiving Config 2
- [ ] ET ADWARE_PUP New.net Spyware updating
- [x] ET ADWARE_PUP User-Agent (Download Agent) Possibly Related to TrinityAcquisitions.com
- [ ] ET ADWARE_PUP MarketScore Spyware Uploading Data
- [ ] ET ADWARE_PUP KMIP.net Spyware
- [x] ET ADWARE_PUP 180solutions Spyware (tracked event 2 reporting)
- [ ] ET ADWARE_PUP AntiVermins.com Fake Antispyware Package User-Agent (AntiVerminser)
- [ ] ET ADWARE_PUP Baidu.com Spyware Bar Pulling Content
- [ ] ET ADWARE_PUP User-Agent (Download UBAgent) - lop.com and other spyware
- [x] ET ADWARE_PUP Gamehouse.com User-Agent (GAMEHOUSE.NET.URL)
- [x] ET ADWARE_PUP MyGlobalSearch Spyware bar update
- [ ] ET ADWARE_PUP Winferno Registry Fix Spyware Download
- [x] ET ADWARE_PUP Yourscreen.com Spyware User-Agent (Freezelnet)
- [ ] ET ADWARE_PUP Catchonlife.com Spyware
- [ ] ET ADWARE_PUP Freeze.com Spyware/Adware (Pulling Ads)
- [ ] ET ADWARE_PUP Hotbar Zango Toolbar Spyware User Agent (ZangoToolbar)
- [ ] ET ADWARE_PUP Instafinder.com spyware
- [x] ET ADWARE_PUP Hotbar Tools Spyware User-Agent (hbtools)
- [x] ET ADWARE_PUP dialno Dialer User-Agent (dialno)
- [ ] ET ADWARE_PUP WhenUClick.com Application Version Check
- [ ] ET ADWARE_PUP SurfAccuracy.com Spyware Pulling Ads
- [x] ET ADWARE_PUP Zango Seekmo Bar Spyware User-Agent (Seekmo Toolbar)
- [ ] ET ADWARE_PUP Spyhealer Fake Anti-Spyware Install User-Agent (SpyHealer)
- [x] ET ADWARE_PUP Freeze.com Spyware User-Agent (YourScreen123)
- [x] ET ADWARE_PUP searchenginebar.com Spyware User-Agent (RX Bar)
- [ ] ET ADWARE_PUP Epilot.com Spyware Reporting Clicks
- [ ] ET ADWARE_PUP CNSMIN (3721.com) Spyware Activity 2
- [x] ET ADWARE_PUP clickspring.com Spyware Install User-Agent (CS Fingerprint Module)
- [x] ET ADWARE_PUP Surfaccuracy.com Spyware Install User-Agent (SF Installer)
- [ ] ET ADWARE_PUP Abcsearch.com Spyware Reporting
- [x] ET ADWARE_PUP Dropspam.com Spyware Reporting

- [ ] ET ADWARE_PUP Webbuying.net Spyware Install User-Agent (wbi_v0.90)
- [ ] ET ADWARE_PUP Deskwizz.com Spyware Install Code Download
- [ ] ET ADWARE_PUP Adware Command Client Checkin
- [ ] ET ADWARE_PUP Specificclick.net Spyware Activity
- [ ] ET ADWARE_PUP CoolDeskAlert Spyware Activity
- [ ] ET ADWARE_PUP Oemji Spyware User-Agent (Oemji)
- [ ] ET ADWARE_PUP DelFin Project Spyware (payload-alt)
- [ ] ET ADWARE_PUP Terminexor.com Spyware User-Agent (DInstaller2)
- [x] ET ADWARE_PUP Drivecleaner.com Spyware User-Agent (DriveCleaner Updater)
- [ ] ET ADWARE_PUP Mirar Spyware User-Agent (Mirar_KeywordContent)
- [x] ET ADWARE_PUP AskSearch Toolbar Spyware User-Agent (AskBar)
- [x] ET ADWARE_PUP Gamehouse.com Related Spyware User-Agent (Sprout Game)
- [ ] ET ADWARE_PUP Adwave.com Related Spyware User-Agent (STBHOGet)
- [ ] ET ADWARE_PUP E2give Spyware Reporting (check url)
- [ ] ET ADWARE_PUP Alawar Toolbar Spyware User-Agent (Alawar Toolbar)
- [ ] ET ADWARE_PUP KMIP.net Spyware 2
- [x] ET ADWARE_PUP WinSoftware.com Spyware User-Agent (NetInstaller)
- [ ] ET ADWARE_PUP Antivermins.com Spyware/Adware User-Agent (AntiVermeans)
- [ ] ET ADWARE_PUP Sytes.net Related Spyware Reporting
- [ ] ET ADWARE_PUP Winfixmaster.com Fake Anti-Spyware Install
- [ ] ET ADWARE_PUP Winfixmaster.com Fake Anti-Spyware User-Agent 2 (WinFix Master)
- [x] ET ADWARE_PUP User-Agent (DIALER)
- [ ] ET ADWARE_PUP Evidencenuker.com Fake AV/Anti-Spyware User-Agent (EVNUKER)
- [x] ET ADWARE_PUP Security-updater.com Spyware Posting Data
- [ ] ET ADWARE_PUP Baidu.com Spyware Bar Pulling Data
- [ ] ET ADWARE_PUP Findwhat.com Spyware (sendmedia)
- [ ] ET ADWARE_PUP Trojan User-Agent (Windows Updates Manager)
- [ ] ET ADWARE_PUP Baidu.com Spyware Bar Activity
- [ ] ET ADWARE_PUP Zango Spyware (tbrequest data post)
- [ ] ET ADWARE_PUP Malwarealarm.com Fake AV/AntiSpyware Download
- [ ] ET ADWARE_PUP MyWebSearch Toolbar Posting Activity Report
- [ ] ET ADWARE_PUP 51yes.com Spyware Reporting User Activity
- [ ] ET ADWARE_PUP Internet-optimizer.com Related Spyware User-Agent (SexTrackerWSI)
- [x] ET ADWARE_PUP Sality Virus User Agent Detected (KUKU)
- [x] ET ADWARE_PUP Adload.Generic Spyware User-Agent (91castInstallKernel)
- [ ] ET ADWARE_PUP CoolStreaming Toolbar (Conduit related) User-Agent (Coolstreaming Tool-Bar)
- [x] ET ADWARE_PUP Trafficadvance.net Spyware User-Agent (Internet 1.0)
- [x] ET ADWARE_PUP qq.com related Spyware User-Agent (QQGame)
- [ ] ET ADWARE_PUP Personalweb Spyware User-Agent (PWMI/1.0)
- [ ] ET ADWARE_PUP Mirar Bar Spyware User-Agent (Mirar_Toolbar)
- [ ] ET ADWARE_PUP Bizconcept.info Spyware Checkin
- [x] ET ADWARE_PUP Spylocked Fake Anti-Spyware User-Agent (SpyLocked)
- [x] ET ADWARE_PUP Qcbar/Adultlinks Spyware User-Agent (IBSBand)
- [ ] ET ADWARE_PUP Webbuying.net Spyware Installing
- [x] ET ADWARE_PUP Deskwizz.com Spyware Install INI Download
- [ ] ET ADWARE_PUP Webbuying.net Spyware Install User-Agent 2 (wb v1.6.4)
- [ ] ET ADWARE_PUP K8l.info Spyware Activity
- [ ] ET ADWARE_PUP Suspicious User-Agent (Toolbar) Possibly Malware/ Spyware
- [ ] ET ADWARE_PUP DelFin Project Spyware (setup-alt)
- [ ] ET ADWARE_PUP Virusblast.com Fake AV/Anti-Spyware User-Agent (ad-protect)
- [ ] ET ADWARE_PUP Errornuker.com Fake Anti-Spyware User-Agent (ERRORNUKER)
- [x] ET ADWARE_PUP malwarewipeupdate.com Spyware User-Agent (MalwareWipe)
- [x] ET ADWARE_PUP AskSearch Spyware User-Agent (AskSearchAssistant)
- [x] ET ADWARE_PUP User-Agent (ms)
- [ ] ET ADWARE_PUP SpyDawn.com Fake Anti-Spyware User-Agent (SpyDawn)
- [x] ET ADWARE_PUP Bestoffersnetwork.com Related Spyware User-Agent (TBONAS)
- [x] ET ADWARE_PUP Toplist.cz Related Spyware Checkin
- [ ] ET ADWARE_PUP Supergames.aavalue.com Spyware
- [x] ET ADWARE_PUP WinSoftware.com Spyware User-Agent (WinSoftware)
- [ ] ET ADWARE_PUP Msgplus.net Spyware/Adware User-Agent (MsgPlus3)
- [x] ET ADWARE_PUP CommonName.com Spyware/Adware User-Agent (CommonName Agent)
- [ ] ET ADWARE_PUP Bravesentry.com Fake Antispyware Updating
- [ ] ET ADWARE_PUP Winfixmaster.com Fake Anti-Spyware User-Agent (WinFixMaster)
- [ ] ET ADWARE_PUP Privacyprotector.com Fake Anti-Spyware Install
- [ ] ET ADWARE_PUP Winsoftware.com Fake AV User-Agent (DNS Extractor)
- [x] ET ADWARE_PUP CoolWebSearch Spyware User-Agent (iefeatsl)
- [ ] ET ADWARE_PUP Mirarsearch.com Spyware Posting Data
- [ ] ET ADWARE_PUP Findwhat.com Spyware (clickthrough)
- [ ] ET ADWARE_PUP MalwareWiped.com Spyware User-Agent (MalwareWiped)
- [ ] ET ADWARE_PUP Worm.Pyks HTTP C&C Traffic User-Agent (skw00001)
- [ ] ET ADWARE_PUP Alexa Spyware Reporting URL Visited
- [ ] ET ADWARE_PUP Malwarealarm.com Fake AV/AntiSpyware Updating
- [x] ET ADWARE_PUP EELoader Malware Packages User-Agent (EELoader)
- [ ] ET ADWARE_PUP Alexa Spyware Redirecting User
- [x] ET ADWARE_PUP dns-look-up.com Spyware User-Agent (KRSystem)
- [ ] ET ADWARE_PUP Baidu.com Spyware Sobar Bar Activity
- [x] ET ADWARE_PUP Adload.Generic Spyware User-Agent (ProxyDown)
- [ ] ET ADWARE_PUP Generic.Malware.dld User-Agent (Sickloader)
- [ ] ET ADWARE_PUP Effectivebrands.com Spyware User-Agent (GTBank)
- [x] ET ADWARE_PUP debelizombi.com (Rizo) related Spyware User-Agent (mc_v1.2.6)
- [ ] ET ADWARE_PUP QQHelper related Spyware User-Agent (H)
- [x] ET ADWARE_PUP Mirar Bar Spyware User-Agent (Mbar)
- [x] ET ADWARE_PUP Statblaster.com Spyware User-Agent (fetcher)
- [x] ET ADWARE_PUP NavExcel Spyware User-Agent (NavHelper)
- [x] ET ADWARE_PUP User Agent (TEST) - Likely Webhancer Related Spyware
- [ ] ET ADWARE_PUP Effectivebrands.com Spyware User-Agent (atsu)

- [x] ET ADWARE_PUP Ask.com Toolbar/Spyware User-Agent (AskPBar)
- [x] ET ADWARE_PUP Win-touch.com Spyware User-Agent (WTRecover)
- [ ] ET ADWARE_PUP Mycashbank.co.kr Spyware User-Agent (pint_agency)
- [ ] ET ADWARE_PUP Vaccineprogram.co.kr Related Spyware User-Agent (anycleaner)
- [x] ET ADWARE_PUP Doctorvaccine.co.kr Related Spyware User-Agent (DoctorVaccine)
- [ ] ET ADWARE_PUP Doctorpro.co.kr Related Spyware User-Agent (doctorpro1)
- [ ] ET ADWARE_PUP Doctorpro.co.kr Related Fake Anti-Spyware Checkin (open)
- [ ] ET ADWARE_PUP Karine.co.kr Related Spyware User-Agent (Access down)
- [ ] ET ADWARE_PUP Doctorpro.co.kr Related Fake Anti-Spyware Checkin (ret)
- [x] ET ADWARE_PUP Cpushpop.com Spyware User-Agent (CPUSH_UPDATER)
- [ ] ET ADWARE_PUP Zango Cash Spyware User-Agent (ZC-Bridgev26)
- [x] ET ADWARE_PUP Mirage.ru Related Spyware User-Agent (szNotifyIdent)
- [ ] ET ADWARE_PUP User-Agent (AntiSpyware) - Likely 2squared.com related
- [ ] ET ADWARE_PUP SpyShredder Fake Anti-Spyware Install Download
- [x] ET ADWARE_PUP NewWeb/Sudui.com Spyware User-Agent (updatesodui)
- [x] ET ADWARE_PUP TryMedia Spyware User-Agent (TryMedia_DM_2.0.0)
- [ ] ET ADWARE_PUP Advertisementserver.com Spyware Checkin
- [ ] ET ADWARE_PUP VirusProtectPro Spyware User-Agent (VirusProtectPro)
- [ ] ET ADWARE_PUP Viruscheck.co.kr Fake Antispyware User-Agent (viruscheck)
- [x] ET ADWARE_PUP Spyware User-Agent (XXX)
- [x] ET ADWARE_PUP Winxpperformance.com Related Spyware User-Agent (Microsoft Internet Browser)
- [x] ET ADWARE_PUP Spyware User-Agent (install_s)
- [ ] ET ADWARE_PUP IEDefender (iedefender.com) Fake Antispyware User Agent (IEDefender 2.1)
- [ ] ET ADWARE_PUP Popads123.com Related Spyware User-Agent (LmaokaazLdr)
- [x] ET ADWARE_PUP Antivirgear.com Fake Anti-Spyware User-Agent (AntiVirGear)
- [ ] ET ADWARE_PUP host-domain-lookup.com spyware related Checkin
- [ ] ET ADWARE_PUP Alfaantivirus.com Fake Anti-Virus User-Agent (IM Download)
- [ ] ET ADWARE_PUP Kpang.com Related Trojan User-Agent (kpangupdate)
- [x] ET ADWARE_PUP Theinstalls.com Initial Checkin
- [ ] ET ADWARE_PUP Doctorvaccine.co.kr Related Spyware-User Agent (ers)
- [x] ET ADWARE_PUP User-Agent (ie) - Possible Trojan Downloader
- [x] ET ADWARE_PUP Errclean.com Related Spyware User-Agent (Locus NetInstaller)
- [ ] ET ADWARE_PUP OneStepSearch Host Activity
- [x] ET ADWARE_PUP User-Agent (microsoft) - Possible Trojan Downloader
- [ ] ET ADWARE_PUP Softcashier.com Spyware Install Checkin
- [x] ET ADWARE_PUP Vombanetwork Spyware User-Agent (VombaProductsInstaller)
- [x] ET ADWARE_PUP Mycomclean.com Spyware User-Agent (HTTP_GET_COMM)
- [ ] ET ADWARE_PUP Virusheat.com Fake Anti-Spyware User-Agent (VirusHeat 4.3)
- [ ] ET ADWARE_PUP Deepdo.com Toolbar/Spyware User Agent (DeepdoUpdate)
- [x] ET ADWARE_PUP Win-touch.com Spyware User-Agent (WTInstaller)
- [ ] ET ADWARE_PUP Vaccineprogram.co.kr Related Spyware User-Agent (Museon)
- [x] ET ADWARE_PUP Vaccineprogram.co.kr Related Spyware User Agent (pcsafe)
- [x] ET ADWARE_PUP Platinumreward.co.kr Spyware User-Agent (WT_GET_COMM)
- [ ] ET ADWARE_PUP Doctorpro.co.kr Related Fake Anti-Spyware Mac Check
- [ ] ET ADWARE_PUP Karine.co.kr Related Spyware User Agent (chk Profile)
- [ ] ET ADWARE_PUP Doctorpro.co.kr Related Fake Anti-Spyware Post
- [ ] ET ADWARE_PUP Doctorpro.co.kr Related Fake Anti-Spyware Post (api_result)
- [x] ET ADWARE_PUP Debelizombi.com Spyware User-Agent (blahrx)
- [x] ET ADWARE_PUP Zango Cash Spyware User-Agent (ZC XML-RPC C++ Client)
- [ ] ET ADWARE_PUP User-Agent (Dummy)
- [ ] ET ADWARE_PUP Vikiller.com Fake Antispyware User-Agent (vikiller ctrl...)
- [x] ET ADWARE_PUP NewWeb/Sudui.com Spyware User-Agent (B Register)
- [x] ET ADWARE_PUP NewWeb/Sudui.com Spyware User-Agent (aaaabbb)
- [ ] ET ADWARE_PUP Advertisementserver.com Spyware Initial Checkin
- [x] ET ADWARE_PUP klm123.com Spyware User Agent
- [ ] ET ADWARE_PUP Viruscheck.co.kr Related Fake Anti-Spyware Post (chkvs)
- [ ] ET ADWARE_PUP Ufixer.com Fake Antispyware User-Agent (Ultimate Fixer)
- [ ] ET ADWARE_PUP Spyware User-Agent (QdrBi Starter)
- [ ] ET ADWARE_PUP AVSystemcare.com.com Fake Anti-Virus Product
- [x] ET ADWARE_PUP Spyware User-Agent (count)
- [x] ET ADWARE_PUP Zredirector.com Related Spyware User-Agent (BndDriveLoader)
- [ ] ET ADWARE_PUP Softwarereferral.com Adware Checkin
- [ ] ET ADWARE_PUP Guard-Center.com Fake AntiVirus Post-Install Checkin
- [x] ET ADWARE_PUP host-domain-lookup.com spyware related Start Report
- [ ] ET ADWARE_PUP User-Agent (Internet Explorer (compatible))
- [ ] ET ADWARE_PUP PCDoc.co.kr Fake AV User-Agent (PCDoc11)
- [ ] ET ADWARE_PUP PCDoc.co.kr Fake AV User-Agent (mypcdoctor)
- [ ] ET ADWARE_PUP Rabio Spyware/Adware Initial Registration
- [x] ET ADWARE_PUP Drpcclean.com Related Spyware User-Agent (DrPCClean Transmit)
- [x] ET ADWARE_PUP User-Agent (Mozilla) - Possible Spyware Related
- [x] ET ADWARE_PUP System-defender.com Fake AV Install Checkin
- [x] ET ADWARE_PUP User-Agent (Internet Explorer 6.0) - Possible Trojan Downloader
- [x] ET ADWARE_PUP User-Agent (Firefox) - Possible Trojan Downloader
- [ ] ET ADWARE_PUP Vombanetworks.com Spyware Installer Checkin
- [ ] ET ADWARE_PUP Mycomclean.com Spyware User-Agent (SHINI)
- [x] ET ADWARE_PUP User-Agent (Example)

- [ ] ET ADWARE_PUP User-Agent (HTTP_CONNECT)
- [x] ET ADWARE_PUP Searchspy.co.kr Spyware User-Agent (HTTPGETDATA)
- [x] ET ADWARE_PUP Searchspy.co.kr Spyware User-Agent (HTTP_FILEDOWN)
- [ ] ET ADWARE_PUP Donkeyhote.co.kr Spyware User-Agent (UDonkey)
- [x] ET ADWARE_PUP User-Agent (User-Agent Mozilla/4.0 (compatible))
- [ ] ET ADWARE_PUP Geopia.com Fake Anti-Spyware/AV User-Agent (fian3manager)
- [ ] ET ADWARE_PUP SysVenFak Fake AV Package User-Agent (gh2008)
- [ ] ET ADWARE_PUP User-Agent (popup)
- [x] ET ADWARE_PUP User-Agent (double dashes)
- [x] ET ADWARE_PUP Snoopstick.net Related Spyware User-Agent (SnoopStick Updater)
- [ ] ET ADWARE_PUP Msconfig.co.kr Related User-Agent (GLOBALx)
- [ ] ET ADWARE_PUP Dokterfix.com Fake AV User-Agent (Magic NetInstaller)
- [ ] ET ADWARE_PUP User-Agent (2 spaces)
- [ ] ET ADWARE_PUP Sears.com/Kmart.com My SHC Community spyware download
- [x] ET ADWARE_PUP User-Agent (Internet)
- [ ] ET ADWARE_PUP Servicepack.kr Fake Patch Software Checkin
- [ ] ET ADWARE_PUP Blank User-Agent (descriptor but no string)
- [ ] ET ADWARE_PUP Kwsearchguide.com Related Spyware Keepalive
- [ ] ET ADWARE_PUP Soft-Show.cn Related Fake AV Install
- [ ] ET ADWARE_PUP Speed-runner.com Fake Speed Test User-Agent (SRInstaller)
- [ ] ET ADWARE_PUP Soft-Show.cn Related Fake AV Install Ad Pull
- [ ] ET ADWARE_PUP Avsystemcare.com Fake AV User-Agent (LocusSoftware NetInstaller)
- [ ] ET ADWARE_PUP Sidelinker.com-Upspider.com Spyware Checkin
- [ ] ET ADWARE_PUP V-Clean.com Fake AV Checkin
- [ ] ET ADWARE_PUP Winxdefender.com Fake AV Package Post Install Checkin
- [x] ET ADWARE_PUP vaccine-program.co.kr Related Spyware User-Agent (vaccine)
- [ ] ET ADWARE_PUP UbrenQuatroRusDldr Downloader User-Agent (UbrenQuatroRusDldr 096044)
- [ ] ET ADWARE_PUP yeps.co.kr Related User-Agent (ISecu)
- [x] ET ADWARE_PUP Misspelled Mozilla User-Agent (Mozila)
- [x] ET ADWARE_PUP Suspicious User-Agent (Nimo Software HTTP Retriever 1.0)
- [x] ET ADWARE_PUP Antispywaremaster.com/Privacyprotector.com Fake AV Checkin
- [x] ET ADWARE_PUP Adaware.BarACE Checkin and Update
- [ ] ET ADWARE_PUP Shopcenter.co .kr Spyware Install Report
- [ ] ET ADWARE_PUP Gooochi Related Spyware Ad pull
- [ ] ET ADWARE_PUP Advert-network.com Related Spyware Updating
- [ ] ET ADWARE_PUP EMO/PCPrivacyCleaner Rougue Secuirty App GET Checkin
- [ ] ET ADWARE_PUP Adware.Look2Me Activity
- [ ] ET ADWARE_PUP Searchtool.co.kr Fake Product User-Agent (searchtoolup)
- [x] ET ADWARE_PUP ZCOM Adware/Spyware User-Agent (ZCOM Software)
- [x] ET ADWARE_PUP iwin.com Games/Spyware User-Agent (iWin GameInfo Installer Helper)
- [x] ET ADWARE_PUP ezday.co .kr Related Spyware User-Agent (Ezshop)
- [ ] ET ADWARE_PUP Kpang.com Spyware User-Agent (auctionplusup)
- [x] ET ADWARE_PUP Searchspy.co.kr Spyware User-Agent (HTTPFILEDOWN)
- [x] ET ADWARE_PUP User-Agent (Explorer)
- [ ] ET ADWARE_PUP Gcashback.co.kr Spyware User-Agent (InvokeAd)
- [ ] ET ADWARE_PUP Geopia.com Fake Anti-Spyware/AV User-Agent (fs3update)
- [x] ET ADWARE_PUP User-Agent (HTTP)
- [ ] ET ADWARE_PUP SysVenFak Fake AV Package Victim Checkin (victim.php)
- [ ] ET ADWARE_PUP Nguide.co.kr Fake Security Tool User-Agent (nguideup)
- [x] ET ADWARE_PUP Hex Encoded IP HTTP Request - Likely Malware
- [ ] ET ADWARE_PUP Msconfig.co.kr Related User Agent (BACKMAN)
- [x] ET ADWARE_PUP Fake Wget User-Agent (wget 3.0) - Likely Hostile
- [ ] ET ADWARE_PUP Direct-web.co.kr Related Spyware Checkin
- [ ] ET ADWARE_PUP Vaccine-program.co.kr Related Spyware Checkin
- [ ] ET ADWARE_PUP Easydownloadsoft.com Fake Anti-Virus User-Agent (IM Downloader)
- [x] ET ADWARE_PUP User-Agent (Win95)
- [ ] ET ADWARE_PUP Privacyprotector Related Spyware User-Agent (Ssol NetInstaller)
- [ ] ET ADWARE_PUP Kwsearchguide.com Related Spyware Checkin
- [x] ET ADWARE_PUP Alexa Search Toolbar User-Agent 2 (Alexa Toolbar)
- [x] ET ADWARE_PUP Win-touch.com Spyware User-Agent (WinTouch)
- [ ] ET ADWARE_PUP Speed-runner.com Fake Speed Test User-Agent (SpeedRunner)
- [ ] ET ADWARE_PUP 360safe.com related Fake Security Product Update (KillerSet)
- [ ] ET ADWARE_PUP Speed-runner.com Fake Speed Test User-Agent (SRRecover)
- [ ] ET ADWARE_PUP Sidelinker.com-Upspider.com Spyware Count
- [ ] ET ADWARE_PUP WinButler User-Agent (WinButler)
- [ ] ET ADWARE_PUP Pcclear.co.kr/Pcclear.com Fake AV User-Agent (PCClearPlus)
- [x] ET ADWARE_PUP Sidebar Related Spyware User-Agent (Sidebar Client)
- [ ] ET ADWARE_PUP BndVeano4GetDownldr Downloader User-Agent (BndVeano4GetDownldr)
- [ ] ET ADWARE_PUP yeps.co.kr Related User-Agent (ISUpd)
- [x] ET ADWARE_PUP my247eshop .com User-Agent
- [x] ET ADWARE_PUP ZenoSearch Spyware User-Agent
- [x] ET ADWARE_PUP AntiSpywareMaster.com Fake AV User-Agent (AsmUpdater)
- [ ] ET ADWARE_PUP Seekmo.com Spyware Data Upload
- [ ] ET ADWARE_PUP Adsincontext.com Related Spyware User-Agent (Connector v1.2)
- [x] ET ADWARE_PUP Realtimegaming.com Online Casino Spyware Gaming Checkin
- [ ] ET ADWARE_PUP Advert-network.com Related Spyware Checking for Updates
- [ ] ET ADWARE_PUP Deepdo Toolbar User-Agent (FavUpdate)
- [ ] ET ADWARE_PUP Cleancop.co.kr Fake AV User-Agent (CleancopUpdate)
- [ ] ET ADWARE_PUP Sogou.com Spyware User-Agent (SogouIMEMiniSetup)
- [ ] ET ADWARE_PUP Systemdoctor.com/Antivir2008 related Fake Anti-Virus User-Agent (AntivirXP)
- [x] ET ADWARE_PUP Casino Related Spyware User-Agent Detected (Viper 4.0)
- [ ] ET ADWARE_PUP Internet-antivirus.com Related Fake AV User-Agent (Update Internet Antivirus)

- [ ] ET ADWARE_PUP AV2010 Rogue Security Application User-Agent (AV2010)
- [x] ET ADWARE_PUP Trojan.FakeAV.SystemDefender Checkin
- [ ] ET ADWARE_PUP User-Agent (bdsclk) - Possible Admoke Admware
- [ ] ET ADWARE_PUP AdWare.Win32.Yokbar Checkin URL
- [x] ET ADWARE_PUP Matcash Trojan Related Spyware Code Download
- [ ] ET ADWARE_PUP AdWare.Win32.MWGuide checkin
- [x] ET ADWARE_PUP Smileware Connection Spyware Related User-Agent (Smileware Connection)
- [ ] ET ADWARE_PUP MySideSearch.com Spyware Install
- [ ] ET ADWARE_PUP Hotbar.com Related Spyware Activity Report
- [x] ET ADWARE_PUP Simbar Spyware User-Agent Detected
- [x] ET ADWARE_PUP User-Agent (FileDownloader)
- [ ] ET ADWARE_PUP User-Agent (get_site1)
- [ ] ET ADWARE_PUP Viruskill.co.kr Fake AV User-Agent Detected (virus_kill)
- [x] ET ADWARE_PUP NewWeb User-Agent (Lobo Lunar)
- [x] ET ADWARE_PUP Pigeon.AYX/AVKill Related User-Agent (CTTBasic)
- [ ] ET ADWARE_PUP User-Agent (Mozilla/4.8 ru)
- [x] ET ADWARE_PUP User-Agent (AgavaDwnl) - Possibly Xema
- [x] ET ADWARE_PUP Downloader Checkin - Downloads Rogue Adware
- [ ] ET ADWARE_PUP Adware PlusDream - GET Config Download/Update
- [x] ET ADWARE_PUP IE Toolbar User-Agent (IEToolbar)
- [ ] ET ADWARE_PUP QVOD Related Spyware/Malware User-Agent (Qvod)
- [x] ET ADWARE_PUP 2020search/PowerSearch Toolbar Adware/Spyware - GET
- [x] ET ADWARE_PUP Topgame-online.com Ruch Casino Install User-Agent (RichCasino)
- [ ] ET ADWARE_PUP Casalemedia Spyware Reporting URL Visited 3
- [x] ET ADWARE_PUP User-Agent (MyIE/1.0)
- [ ] ET ADWARE_PUP User-Agent (ONANDON)
- [x] ET ADWARE_PUP User-Agent (M0zilla)
- [x] ET ADWARE_PUP User-Agent (MSIE7 na)
- [ ] ET ADWARE_PUP Executable purporting to be .cfg file with no Referer - Likely Malware
- [x] ET ADWARE_PUP User-Agent Mozilla/3.0
- [x] ET ADWARE_PUP User-Agent (SogouExplorerMiniSetup)
- [x] ET ADWARE_PUP Trojan.Win32.InternetAntivirus User-Agent (General Antivirus)
- [x] ET ADWARE_PUP User-Agent (Live Enterprise Suite)
- [ ] ET ADWARE_PUP Fake Mozilla UA Outbound (Mozilla/0.xx)
- [ ] ET ADWARE_PUP User-Agent (gomtour)
- [ ] ET ADWARE_PUP User-Agent (i-scan)
- [ ] ET ADWARE_PUP User-Agent (Yodao Desktop Dict)
- [x] ET ADWARE_PUP User-Agent (webcount)
- [ ] ET ADWARE_PUP User-Agent (Suggestion)
- [x] ET ADWARE_PUP Likely Hostile User-Agent (Forthgoer)
- [x] ET ADWARE_PUP User-Agent (CustomSpy)
- [x] ET ADWARE_PUP User-Agent (TALWinInetHTTPClient)
- [ ] ET ADWARE_PUP User-Agent (C\\WINDOWS\\system32\ \NetLogom.exe)
- [x] ET ADWARE_PUP User-Agent (http-get-demo) Possible Reverse Web Shell
- [x] ET ADWARE_PUP Adware.Kraddare Checkin
- [ ] ET ADWARE_PUP Outbound AlphaServer User-Agent (Powered By 64-Bit Alpha Processor)
- [x] ET ADWARE_PUP User-Agent (HTTP_Query)
- [ ] ET ADWARE_PUP Hotbar Agent User-Agent (PinballCorp)
- [ ] ET ADWARE_PUP iframebiz - /qwertyuiyw12ertyuytre/adv***.php
- [ ] ET ADWARE_PUP Admoke/Adload.AFB!tr.dldr Checkin
- [ ] ET ADWARE_PUP AdWare.Win32.Yokbar User-Agent Detected (YOK Agent)
- [ ] ET ADWARE_PUP Zenosearch Malware Checkin HTTP POST
- [x] ET ADWARE_PUP Zenosearch Malware Checkin HTTP POST (2)
- [ ] ET ADWARE_PUP AdWare.Win32.MWGuide keepalive
- [ ] ET ADWARE_PUP Popupblockade.com Spyware Related User-Agent (PopupBlockade/1.63.0.2/Reg)
- [ ] ET ADWARE_PUP Hotbar.com Related Spyware Install Report
- [x] ET ADWARE_PUP User-Agent (Mozilla/4.0 (compatible))
- [ ] ET ADWARE_PUP User-Agent (IE_6.0)
- [ ] ET ADWARE_PUP Adware/Spyware Trymedia.com EXE download
- [ ] ET ADWARE_PUP User-Agent (GETJOB)
- [x] ET ADWARE_PUP Fake AV User-Agent (N1)
- [ ] ET ADWARE_PUP Adware-Mirar Reporting (BAR)
- [ ] ET ADWARE_PUP No-ad.co.kr Fake AV Related User-Agent (U2Clean)
- [ ] ET ADWARE_PUP User-Agent (HelpSrvc)
- [x] ET ADWARE_PUP MySideSearch Browser Optimizer
- [x] ET ADWARE_PUP W3i Related Adware/Spyware
- [ ] ET ADWARE_PUP Pivim Multibar User-Agent (Pivim Multibar)
- [x] ET ADWARE_PUP RubyFortune Spyware Capabilities User-Agent (Microgaming Install Program) - GET
- [ ] ET ADWARE_PUP FakeAV Windows Protection Suite/ReleaseXP.exe User-Agent (Releasexp)
- [ ] ET ADWARE_PUP Adware/Antivirus360 Config to client
- [x] ET ADWARE_PUP ErrorNuker FakeAV User-Agent (ERRN2004 (Windows XP))
- [x] ET ADWARE_PUP User-Agent (User Agent) - Likely Hostile
- [ ] ET ADWARE_PUP www.vaccinekiller.com Related Spyware User-Agent (VaccineKillerIU)
- [ ] ET ADWARE_PUP Win32/InternetAntivirus User-Agent (Internet Antivirus Pro)
- [ ] ET ADWARE_PUP User-Agent (CrazyBro)
- [ ] ET ADWARE_PUP Executable purporting to be .txt file with no Referer - Likely Malware
- [x] ET ADWARE_PUP User-Agent (???)
- [x] ET ADWARE_PUP Generic Adware Install Report
- [x] ET ADWARE_PUP User-Agent (Fast Browser Search)
- [x] ET ADWARE_PUP chnsystem.com Spyware User-Agent (Update1.0)
- [ ] ET ADWARE_PUP Fake Mozilla User-Agent (Mozilla/0.xx) Inbound
- [ ] ET ADWARE_PUP Infobox3 Spyware User-Agent (InfoBox)
- [ ] ET ADWARE_PUP Recuva User-Agent (OpenPage) - likely trojan dropper
- [x] ET ADWARE_PUP User-Agent (Save)
- [x] ET ADWARE_PUP User-Agent (Download Master) - Possible Malware Downloader
- [x] ET ADWARE_PUP Sogou Toolbar Checkin
- [x] ET ADWARE_PUP User-Agent (Mozilla/4.0 (SP3 WINLD))
- [x] ET ADWARE_PUP User-Agent (XieHongWei-HttpDown/2.0)
- [x] ET ADWARE_PUP User-Agent (browserbob.com)
- [ ] ET ADWARE_PUP User-Agent (KRMAK) Butterfly Bot download
- [x] ET ADWARE_PUP Win32/Agent.PMS Variant CnC Activity
- [x] ET ADWARE_PUP User-Agent (Microsoft Internet Explorer 6.0) Possible Reverse Web Shell
- [ ] ET ADWARE_PUP Inbound AlphaServer User-Agent (Powered By 64-Bit Alpha Processor)
- [x] ET ADWARE_PUP MSIL.Amiricil.gen HTTP Checkin
- [ ] ET ADWARE_PUP User-Agent (dbcount)
- [ ] ET ADWARE_PUP User-Agent (RangeCheck/0.1)

- [ ] ET ADWARE_PUP HTML.Psyme.Gen Reporting
- [ ] ET ADWARE_PUP CryptMEN HTTP library purporting to be MSIE to PHP HTTP 1.0
- [x] ET ADWARE_PUP ASKTOOLBAR.DLL Reporting
- [x] ET ADWARE_PUP AdVantage Malware URL Infection Report
- [x] ET ADWARE_PUP Lookup of Malware Domain twothousands.cm Likely Infection
- [ ] ET ADWARE_PUP Suspicious Chinese Content-Language zh-cn Which May be Malware Related
- [x] ET ADWARE_PUP All Numerical .cn Domain Likely Malware Related
- [ ] ET ADWARE_PUP Mozilla 3.0 and Indy Library User-Agent Likely Hostile
- [x] ET ADWARE_PUP Optimum Installer User-Agent IE6 on Windows XP
- [x] ET ADWARE_PUP All Numerical .ru Domain HTTP Request Likely Malware Related
- [x] ET ADWARE_PUP Possible FakeAV Binary Download
- [x] ET ADWARE_PUP Known Malicious User-Agent (x) Win32/Tracur.A or OneStep Adware Related
- [x] ET ADWARE_PUP Sidetab or Related Trojan Checkin
- [x] ET ADWARE_PUP Win32.EZula Adware Reporting Successful Install
- [x] ET ADWARE_PUP SweetIM Install in Progress
- [x] ET ADWARE_PUP Adrevmedia Related Media Manager Spyware Checkin
- [x] ET ADWARE_PUP W32/SpeedRunner User-Agent SRRemove
- [x] ET ADWARE_PUP HTTP Connection to go2000.cn - Common Malware Checkin Server
- [ ] ET ADWARE_PUP SurfSideKick Activity (iinfo)
- [ ] ET ADWARE_PUP Win32/Wizpop Initial Checkin
- [x] ET ADWARE_PUP Win32/Adware.Kraddare.FJ Checkin
- [x] ET ADWARE_PUP UBar Trojan/Adware Checkin 2
- [ ] ET ADWARE_PUP Zugo Toolbar Spyware/Adware download request
- [x] ET ADWARE_PUP Win32/Adware.Winggo.AB Checkin
- [x] ET ADWARE_PUP W32/SmartPops Adware Outbound Off-Port MSSQL Communication
- [ ] ET ADWARE_PUP W32/Adware.Ibryte User-Agent (ic Windows NT 5.1 MSIE 6.0 Firefox/ Def)
- [x] ET ADWARE_PUP Rebate Informer User-Agent (REBATEINF)
- [x] ET ADWARE_PUP Tool.InstallToolbar.24 Reporting
- [x] ET ADWARE_PUP Adware.Gen5 Reporting
- [ ] ET ADWARE_PUP Win32/Eorezo-B Adware Checkin
- [x] ET ADWARE_PUP Common Adware Library ISX User Agent Detected
- [x] ET ADWARE_PUP W32/OpenTrio User-Agent (Open3)
- [x] ET ADWARE_PUP W32/GameplayLabs.Adware Installer Checkin
- [x] ET ADWARE_PUP AdWare.Win32.Sushi.au Checkin
- [x] ET ADWARE_PUP Carder Card Checking Tool try2check.me SSL Certificate on Off Port
- [x] ET ADWARE_PUP W32/GameVance Adware User Agent
- [x] ET ADWARE_PUP W32/SoftonicDownloader.Adware User Agent
- [ ] ET ADWARE_PUP W32/PaPaPaEdge.Adware/Gambling Poker-Edge Checkin
- [x] ET ADWARE_PUP Adware/FakeAV.Kraddare Checkin UA
- [ ] ET ADWARE_PUP W32/GameVance Adware Server Reponse To Client Checkin
- [x] ET ADWARE_PUP W32/Dialer.Adultchat Checkin
- [x] ET ADWARE_PUP Win32.Bublik.B/Birele/Variant.Kazy.66443 Checkin
- [ ] ET ADWARE_PUP Malicious pusk.exe download
- [ ] ET ADWARE_PUP W32/OnlineGames User Agent loadMM
- [x] ET ADWARE_PUP W32/Eorezo.Adware CnC Beacon
- [x] ET ADWARE_PUP AdWare.MSIL.Solimba.b GET
- [x] ET ADWARE_PUP Suspicious User Agent Smart-RTP
- [x] ET ADWARE_PUP Adware pricepeep Adware.Shopper.297
- [x] ET ADWARE_PUP User-Agent (Gbot)
- [ ] ET ADWARE_PUP CryptMEN HTTP library purporting to be MSIE to PHP HTTP 1.1
- [x] ET ADWARE_PUP User-Agent (AdVantage)
- [ ] ET ADWARE_PUP User-Agent (mrgud)
- [ ] ET ADWARE_PUP Suspicious Russian Content-Language Ru Which May Be Malware Related
- [x] ET ADWARE_PUP User-Agent (0xa10xa1HttpClient)
- [x] ET ADWARE_PUP All Numerical .ru Domain Lookup Likely Malware Related
- [ ] ET ADWARE_PUP Unknown Malware PUTLINK Command Message
- [x] ET ADWARE_PUP Lowercase mozilla/2.0 User-Agent Likely Malware
- [x] ET ADWARE_PUP overtls.com adware request
- [ ] ET ADWARE_PUP Possible Windows executable sent ASCII-hex-encoded
- [x] ET ADWARE_PUP RogueAntiSpyware.AntiVirusPro Checkin
- [x] ET ADWARE_PUP Artro Downloader User-Agent Detected
- [x] ET ADWARE_PUP Unknown Malware patchlist.xml Request
- [x] ET ADWARE_PUP Zugo.com SearchToolbar User-Agent (SearchToolbar)
- [ ] ET ADWARE_PUP Adware/CommonName Reporting
- [ ] ET ADWARE_PUP W32/Baigoo User Agent
- [x] ET ADWARE_PUP Win32/Onescan FraudWare User-Agent
- [x] ET ADWARE_PUP Suspicious User-Agent (go-diva)
- [ ] ET ADWARE_PUP Win32/Wizpop Checkin
- [x] ET ADWARE_PUP UBar Trojan/Adware Checkin 1
- [x] ET ADWARE_PUP UBar Trojan/Adware Checkin 3
- [ ] ET ADWARE_PUP Adware/Helpexpress User Agent HXLogOnly
- [x] ET ADWARE_PUP Suspicious User-Agent (MediaLabsSiteInstaller)
- [ ] ET ADWARE_PUP Adware-Win32/EoRezo Reporting
- [x] ET ADWARE_PUP Win32/SWInformer.B Checkin
- [ ] ET ADWARE_PUP Spyware.Agent.elbb lava.cn Game Exe Download
- [ ] ET ADWARE_PUP Win32-Adware.Hotclip.A Reporting
- [ ] ET ADWARE_PUP Win32/SmartTab PUP Install Activity
- [x] ET ADWARE_PUP W32/OpenCandy Adware Checkin
- [ ] ET ADWARE_PUP Malicious ad_track.php file Reporting
- [x] ET ADWARE_PUP W32/MediaGet Checkin
- [x] ET ADWARE_PUP W32/PlaySushi User-Agent
- [x] ET ADWARE_PUP Carder Card Checking Tool try2check.me SSL Certificate
- [x] ET ADWARE_PUP W32/GameVance Adware Checkin
- [x] ET ADWARE_PUP W32/MediaGet.Adware Installer Download
- [x] ET ADWARE_PUP W32/LoudMo.Adware Checkin
- [x] ET ADWARE_PUP BitCoinPlus Embedded site forcing visitors to mine BitCoins
- [ ] ET ADWARE_PUP Win32/Pdfjsc.XD Related Checkin (microsoft_predator_client header field)
- [ ] ET ADWARE_PUP W32/GameVance User-Agent (aw v3)
- [ ] ET ADWARE_PUP Malicious file bitdefender_isecurity.exe download
- [ ] ET ADWARE_PUP PCMightyMax Agent PCMM.Installer
- [x] ET ADWARE_PUP W32/OnlineGames Checkin
- [x] ET ADWARE_PUP suspicious User-Agent (vb wininet)
- [x] ET ADWARE_PUP Adware.Win32/SProtector.A Client Checkin
- [x] ET ADWARE_PUP AdWare.MSIL.Solimba.b POST
- [x] ET ADWARE_PUP Suspicious User Agent Custom_56562_HttpClient/ VER_STR_COMMA
- [x] ET ADWARE_PUP Adware.Ezula Checkin

- [x] ET ADWARE_PUP Adware.Gamevance.AV Checkin
- [x] ET ADWARE_PUP W32/Wajam.Adware Successful Install
- [x] ET ADWARE_PUP W32/Linkular.Adware Icons.dat Second Stage Download
- [x] ET ADWARE_PUP W32/InstallRex.Adware Initial CnC Beacon
- [x] ET ADWARE_PUP Adware.PUQD Checkin
- [x] ET ADWARE_PUP W32/BettrExperience.Adware Initial Checkin
- [x] ET ADWARE_PUP W32/BettrExperience.Adware Update Checkin
- [x] ET ADWARE_PUP Suspicious User Agent EXE2
- [x] ET ADWARE_PUP Suspicious User Agent Mozi11a
- [x] ET ADWARE_PUP Potentially Unwanted Application AirInstaller
- [ ] ET ADWARE_PUP W32/InstallMonetizer.Adware Beacon 1
- [x] ET ADWARE_PUP RelevantKnowledge Adware CnC Beacon
- [x] ET ADWARE_PUP Win32.AdWare.iBryte.C Install
- [x] ET ADWARE_PUP AdWare.Win32.Yotoon.hs Checkin
- [x] ET ADWARE_PUP SoundCloud Downloader Install Beacon
- [ ] ET ADWARE_PUP W32/DownloadAdmin.Adware CnC Beacon
- [x] ET ADWARE_PUP W32/iBryte.Adware Affiliate Campaign Executable Download
- [ ] ET ADWARE_PUP DomainIQ Check-in
- [x] ET ADWARE_PUP PUP Win32/DownloadGuide.A
- [x] ET ADWARE_PUP W32/RocketfuelNextUp.Adware CnC Beacon
- [x] ET ADWARE_PUP Adware.MultiInstaller checkin 2
- [x] ET ADWARE_PUP OptimizerPro Checkin
- [x] ET ADWARE_PUP PUP Optimizer Pro Adware GET or POST to C2
- [x] ET ADWARE_PUP MultiPlug.A checkin
- [x] ET ADWARE_PUP PUP Win32.SoftPulse Retrieving data
- [x] ET ADWARE_PUP W32/Stan Malvertising.Dropper CnC Beacon
- [x] ET ADWARE_PUP Win32/SoftPulse.H Checkin
- [x] ET ADWARE_PUP Win32/DealPly Checkin
- [x] ET ADWARE_PUP Win32/CloudScout Checkin
- [x] ET ADWARE_PUP PUP W32/DownloadGuide.D
- [x] ET ADWARE_PUP PUP.Win32.BoBrowser User-Agent (LogEvents)
- [x] ET ADWARE_PUP PUP.Win32.BoBrowser User-Agent (BoBrowser)
- [x] ET ADWARE_PUP W32/MultiPlug.Adware Adfraud Traffic
- [x] ET ADWARE_PUP MALWARE W32/WinWrapper.Adware POST CnC Beacon
- [x] ET ADWARE_PUP Potentially Unwanted Application AirInstaller CnC Beacon
- [ ] ET ADWARE_PUP Windows executable sent when remote host claims to send an image M2
- [x] ET ADWARE_PUP W32/PicColor Adware CnC Beacon
- [x] ET ADWARE_PUP Win32/Toolbar.Conduit.AG Checkin
- [x] ET ADWARE_PUP PUP Win32/Conduit.SearchProtect.O CnC Beacon
- [x] ET ADWARE_PUP PUP Win32/DownloadAssistant.A Checkin
- [x] ET ADWARE_PUP OSX ADWARE/Mackeeper Checkin
- [x] ET ADWARE_PUP DealPly Adware CnC Beacon
- [x] ET ADWARE_PUP DealPly Adware CnC Beacon 3
- [x] ET ADWARE_PUP OSX/Fake Flash Player Download Oct 20
- [x] ET ADWARE_PUP Win32/SmartTab PUP Install Activity 2
- [x] ET ADWARE_PUP OSX/Adware.Pirrit CnC Activity 1
- [x] ET ADWARE_PUP OSX/Adware.Pirrit Web Injects
- [x] ET ADWARE_PUP Win32/Adware.Adposhel.A Checkin 4
- [x] ET ADWARE_PUP Successful QuizScope Installation
- [x] ET ADWARE_PUP Conduit Trovi Adware/PUA
- [x] ET ADWARE_PUP InstallCore PUA/Adware Activity M2
- [x] ET ADWARE_PUP InstallCore PUA/Adware Activity M4
- [x] ET ADWARE_PUP W32/Toolbar.WIDGI User-Agent (WidgiToolbar-)
- [x] ET ADWARE_PUP PCAccelerate Pro PUA/Adware User-Agent
- [x] ET ADWARE_PUP Win32/Hadsruda!bit Adware/PUA Installation Activity
- [x] ET ADWARE_PUP LoadMoney Checkin 5
- [x] ET ADWARE_PUP Crossrider Spyware Checkin
- [x] ET ADWARE_PUP W32/Linkular.Adware Successful Install Beacon
- [x] ET ADWARE_PUP GMUnpackerInstaller.A Checkin
- [x] ET ADWARE_PUP W32/InstallRex.Adware Report CnC Beacon
- [x] ET ADWARE_PUP Win32/OutBrowse.G Variant Checkin
- [x] ET ADWARE_PUP W32/BettrExperience.Adware POST Checkin
- [x] ET ADWARE_PUP W32/AdLoad.Downloader Download
- [x] ET ADWARE_PUP Win32.Magania
- [x] ET ADWARE_PUP Suspicious User-Agent (gettingAnswer)
- [ ] ET ADWARE_PUP W32/Safekeeper.Adware CnC Beacon
- [ ] ET ADWARE_PUP W32/InstallMonetizer.Adware Beacon 2
- [x] ET ADWARE_PUP BetterInstaller
- [x] ET ADWARE_PUP Win32/Toolbar.CrossRider.A Checkin
- [x] ET ADWARE_PUP W32/Linkular.Adware Successful Install Beacon (2)
- [x] ET ADWARE_PUP W32/Amonetize.Downloader Executable Download Request
- [ ] ET ADWARE_PUP W32/DownloadAdmin.Adware Executable Download Request
- [x] ET ADWARE_PUP W32/PullUpdate.Adware CnC Beacon
- [x] ET ADWARE_PUP Adware.MultiInstaller
- [x] ET ADWARE_PUP PUP Win32.SoftPulse Checkin
- [x] ET ADWARE_PUP Miuref/Boaxxe Checkin
- [x] ET ADWARE_PUP Downloader.NSIS.OutBrowse.b Checkin
- [x] ET ADWARE_PUP PUP Optimizer Pro Adware Download
- [x] ET ADWARE_PUP W32/SearchSuite Install CnC Beacon
- [x] ET ADWARE_PUP Win32/BrowseFox.H Checkin 2
- [x] ET ADWARE_PUP MAC/Conduit Component Download
- [ ] ET ADWARE_PUP W32/Kyle Malvertising.Dropper CnC Beacon
- [x] ET ADWARE_PUP Adware.InstallCore.B Checkin
- [x] ET ADWARE_PUP PUP Win32/ELEX Checkin
- [x] ET ADWARE_PUP Win32/DomaIQ Checkin
- [x] ET ADWARE_PUP W32/iBryte.Adware Installer Download
- [x] ET ADWARE_PUP PUP.Win32.BoBrowser User-Agent (VersionDwl)
- [ ] ET ADWARE_PUP MultiPlug.J Checkin
- [x] ET ADWARE_PUP W32/WinWrapper.Adware Initial Install Beacon
- [x] ET ADWARE_PUP MALWARE W32/WinWrapper.Adware User-Agent
- [ ] ET ADWARE_PUP AdWare.Win32.BetterSurf.b SSL Cert
- [x] ET ADWARE_PUP PUP Win32/AdWare.Sendori User-Agent
- [x] ET ADWARE_PUP W32/Softpulse PUP Install Failed Beacon
- [x] ET ADWARE_PUP PUP.GigaClicks Checkin
- [x] ET ADWARE_PUP Win32/DownloadAssistant.A PUP CnC
- [x] ET ADWARE_PUP PUP TheSZ AutoUpdate CnC Beacon
- [x] ET ADWARE_PUP W32/DownloadAdmin.Adware User-Agent
- [x] ET ADWARE_PUP DealPly Adware CnC Beacon 2
- [x] ET ADWARE_PUP PUA Boxore User-Agent
- [x] ET ADWARE_PUP DealPly Adware CnC Beacon 4
- [x] ET ADWARE_PUP OSX/Adware.Pirrit CnC Checkin
- [x] ET ADWARE_PUP OSX/Adware.Pirrit CnC Activity 2
- [x] ET ADWARE_PUP Win32/Adware.Adposhel.A Checkin 3
- [x] ET ADWARE_PUP Win32/InstallCore Initial Install Activity 1
- [x] ET ADWARE_PUP SearchProtect PUA User-Agent Observed
- [x] ET ADWARE_PUP InstallCore PUA/Adware Activity M1
- [x] ET ADWARE_PUP InstallCore PUA/Adware Activity M3
- [x] ET ADWARE_PUP Toolbar User-Agent (BrandThunderHelper)
- [ ] ET ADWARE_PUP PUP/DriverRestore Sending System Information to Affiliate
- [x] ET ADWARE_PUP TopTools PUP Install Activity
- [x] ET ADWARE_PUP MSIL/Adload.AT Beacon
- [x] ET ADWARE_PUP Malicious Chrome Extension

- [x] ET ADWARE_PUP MultiPlug.J Checkin
- [x] ET ADWARE_PUP Loadmoney User Agent
- [x] ET ADWARE_PUP Loadmoney.A Checkin 2
- [x] ET ADWARE_PUP Loadmoney.A Checkin 4
- [x] ET ADWARE_PUP Loadmoney.A Checkin 7
- [x] ET ADWARE_PUP Loadmoney.A Checkin 8
- [x] ET ADWARE_PUP Loadmoney Checkin 2
- [x] ET ADWARE_PUP Loadmoney Checkin 3
- [ ] ET ADWARE_PUP InstallCore Variant CnC Checkin
- [ ] ET ADWARE_PUP Win32/LoadMoney Adware Activity
- [x] ET ADWARE_PUP Malicious Chrome Ext. DNS Query For Adware CnC (startupfraction)
- [ ] ET ADWARE_PUP Malicious Chrome Ext. DNS Query For Adware CnC (go.querymo)
- [x] ET ADWARE_PUP Malicious Adware Chrome Extension Detected (1)
- [x] ET ADWARE_PUP [PTsecurity] WebToolbar.Win32.Searchbar.k HTTP JSON Artifact
- [x] ET ADWARE_PUP Suspicious Darkwave Popads Pop Under Redirect
- [x] ET ADWARE_PUP Java.Deathbot Requesting Proxies
- [x] ET ADWARE_PUP Suspicious User-Agent (GeneralDownloadApplication)
- [x] ET ADWARE_PUP Win32.LoadMoney User Agent 2
- [x] ET ADWARE_PUP Rogue.WinPCDefender Checkin
- [x] ET ADWARE_PUP Observed Malicious SSL Cert (OSX/Calender 2 Mining)
- [x] ET ADWARE_PUP Observed Win32/Foniad Domain (acinster .info in TLS SNI)
- [x] ET ADWARE_PUP Observed Win32/Foniad Domain (efishedo .info in TLS SNI)
- [x] ET ADWARE_PUP Observed Win32/Foniad Domain (insupposity .info in TLS SNI)
- [x] ET ADWARE_PUP Observed Win32/Foniad Domain (suggedin .info in DNS Lookup)
- [x] ET ADWARE_PUP WiseCleaner Installed (PUA)
- [x] ET ADWARE_PUP [eSentire] Win32/Adware.Adposhel.lgvk CnC Checkin
- [x] ET ADWARE_PUP Fake Adobe Update Download
- [x] ET ADWARE_PUP AppControls.com User-Agent
- [x] ET ADWARE_PUP PUA Related User-Agent (WINTERNET)
- [x] ET ADWARE_PUP AppControls.com User-Agent
- [x] ET ADWARE_PUP LNKR CnC Activity M1
- [x] ET ADWARE_PUP LNKR CnC Activity M3
- [x] ET ADWARE_PUP LNKR Request for LNKR js file M2
- [x] ET ADWARE_PUP LNKR landing page (possible compromised site) M1
- [x] ET ADWARE_PUP LNKR landing page (possible compromised site) M3
- [x] ET ADWARE_PUP LNKR landing page (possible compromised site) M5
- [x] ET ADWARE_PUP Observed OSX/PremierOpinionD Collection Domain in TLS SNI
- [x] ET ADWARE_PUP Win32/DealPly Configuration File Inbound
- [x] ET ADWARE_PUP Win32/GameHack.DJC CnC Activity
- [x] ET ADWARE_PUP Win32/Adware.iBryte.BO CnC Activity
- [x] ET ADWARE_PUP SoftwareTracking Site - Install Report
- [x] ET ADWARE_PUP Win32/Adware.Bang5mai.BB CnC Activity M1
- [x] ET ADWARE_PUP PrivaZer Checkin
- [x] ET ADWARE_PUP OSX/Bundalore Loader Activity
- [x] ET ADWARE_PUP Win32/InstallDisck SMTP Checkin
- [x] ET ADWARE_PUP Win32/DownloadAssistant.G Variant Error Report
- [x] ET ADWARE_PUP GreatArcadeHits CnC Activity
- [x] ET ADWARE_PUP Win32/Adware.Bang5mai.BB CnC Activity M3
- [x] ET ADWARE_PUP Ads2Srv Bundle Installer Offer Request
- [x] ET ADWARE_PUP Win32/YTDDownloader.F Variant CnC Activity
- [x] ET ADWARE_PUP Crackswin Downloader Activity
- [ ] ET ADWARE_PUP Windows executable sent when remote host claims to send an image M3
- [x] ET ADWARE_PUP Loadmoney.A Checkin 1
- [x] ET ADWARE_PUP Loadmoney.A Checkin 3
- [x] ET ADWARE_PUP Loadmoney.A Checkin 6
- [x] ET ADWARE_PUP Loadmoney.A Checkin 5
- [x] ET ADWARE_PUP Loadmoney Checkin 1
- [ ] ET ADWARE_PUP Win32.LoadMoney User Agent
- [x] ET ADWARE_PUP Loadmoney Checkin 4
- [x] ET ADWARE_PUP ProxyGearPro Proxy Tool PUA
- [ ] ET ADWARE_PUP [PTsecurity] Adware/Rukometa(LoadMoney) Fake PNG File
- [x] ET ADWARE_PUP Malicious Chrome Ext. DNS Query For Adware CnC (search.feedvertizus)
- [x] ET ADWARE_PUP Malicious Chrome Ext. DNS Query For Adware CnC (opurie)
- [x] ET ADWARE_PUP Malicious Adware Chrome Extension Detected (2)
- [x] ET ADWARE_PUP [PTsecurity] Adware.SearchGo (start_page)
- [x] ET ADWARE_PUP [PTsecurity] DeathBot.Java (Minecraft Spambot)
- [x] ET ADWARE_PUP [PTsecurity] Adware.FileFinder Activity
- [x] ET ADWARE_PUP Win32/Adware.Adposhel.A Checkin 5
- [ ] ET ADWARE_PUP Win32/LoadMoney Adware Activity M2
- [x] ET ADWARE_PUP APN/Ask Toolbar PUA/PUP User-Agent
- [x] ET ADWARE_PUP Observed Win32/Foniad Domain (maraukog .info in TLS SNI)
- [x] ET ADWARE_PUP Observed Win32/Foniad Domain (aclassigned .info in TLS SNI)
- [x] ET ADWARE_PUP Observed Win32/Foniad Domain (enclosely .info in TLS SNI)
- [x] ET ADWARE_PUP Observed Win32/Foniad Domain (suggedin .info in TLS SNI)
- [x] ET ADWARE_PUP Lavasoft PUA/Adware Client Install
- [x] ET ADWARE_PUP Antibody Software Installed (PUA)
- [x] ET ADWARE_PUP Luxsoft Win32/ICLoader User-Agent
- [x] ET ADWARE_PUP Fake Adobe Update Request
- [x] ET ADWARE_PUP AppControls.com User-Agent
- [x] ET ADWARE_PUP OSX ADWARE/AD Injector
- [x] ET ADWARE_PUP LNKR Request for validate-site.js
- [x] ET ADWARE_PUP LNKR CnC Activity M2
- [x] ET ADWARE_PUP LNKR Request for LNKR js file M1
- [x] ET ADWARE_PUP LNKR Possible Response for LNKR js file
- [x] ET ADWARE_PUP LNKR landing page (possible compromised site) M2
- [x] ET ADWARE_PUP LNKR landing page (possible compromised site) M4
- [x] ET ADWARE_PUP Win32/Agent.NDV Receiving Task Config File
- [x] ET ADWARE_PUP Win32/DealPly CnC Checkin
- [x] ET ADWARE_PUP Win32/DealPly Reporting Details to CnC
- [x] ET ADWARE_PUP BundledInstaller PUA/PUP Downloader
- [x] ET ADWARE_PUP SoftwareTracking Site - Download Report
- [x] ET ADWARE_PUP Win32/Adware.Adposhel.A Checkin M6
- [x] ET ADWARE_PUP Win32/Adware.Bang5mai.BB CnC Activity M2
- [x] ET ADWARE_PUP Win32/GameHack.COG Variant CnC Activity
- [x] ET ADWARE_PUP Observed DNS Query to OSX/Bundalore Domain
- [x] ET ADWARE_PUP Win32/DownloadAssistant.Q Variant Checkin
- [x] ET ADWARE_PUP Win32/Adware.Agent.NPP CnC Activity
- [x] ET ADWARE_PUP Win32/YTDDownloader.F Activity
- [x] ET ADWARE_PUP Win32/RiskWare.YouXun.X CnC Server Response
- [x] ET ADWARE_PUP Win32/Adware.YoutubeDownloaderGuru.A Variant CnC Activity
- [x] ET ADWARE_PUP Observed DNS Query to Malvertising Related Domain
- [x] ET ADWARE_PUP Win32/Adware.Qjwmonkey.H Variant CnC Activity

- [x] ET ADWARE_PUP Win32/Adware.Qjwmonkey.H Variant CnC Activity M2
- [x] ET ADWARE_PUP MediaDrug CnC Activity
- [x] ET ADWARE_PUP Predator Anti Ban CnC Activity
- [x] ET ADWARE_PUP Downer.B Variant Checkin
- [x] ET ADWARE_PUP DownLoadAdmin Activity
- [x] ET ADWARE_PUP Win32/Zonebac Traffic Redirect
- [x] ET ADWARE_PUP Haken Clicker CnC Activity
- [x] ET ADWARE_PUP DownloadAssistant Activity
- [x] ET ADWARE_PUP Win32/Adware.BrowSecX.AB Install Log Sent
- [x] ET ADWARE_PUP SilverSpeedup Generic PUA Software UA
- [x] ET ADWARE_PUP Windows Explorer Tab Add-on Post Install Checkin
- [x] ET ADWARE_PUP VilnyNet VPN Install Started
- [x] ET ADWARE_PUP Win32/Adware.Agent.NSU CnC Activity M2
- [x] ET ADWARE_PUP Win32/Adware.Vonteera.M Variant CnC Activity
- [x] ET ADWARE_PUP OSX/Adware.Pirrit CnC Activity 3
- [x] ET ADWARE_PUP Win32/Spy.Agent.QCL Variant Activity (POST)
- [x] ET ADWARE_PUP Win32/TrojanClicker Variant Activity (GET)
- [x] ET ADWARE_PUP NivesroCheat CnC Activity M2
- [x] ET ADWARE_PUP Socelars Related Domain in DNS Lookup
- [x] ET ADWARE_PUP Observed Honeygain Domain (api .honeygain .com in TLS SNI)
- [x] ET ADWARE_PUP Win32/MobiGame Install Stats Checkin M2
- [x] ET ADWARE_PUP Win32/Eyoorun.D Variant Checkin
- [x] ET ADWARE_PUP Observed DNS Query to Known PUA Host Domain
- [x] ET ADWARE_PUP SecureDriverUpdater Checkin
- [x] ET ADWARE_PUP Lantern Checkin
- [x] ET ADWARE_PUP Win32/2345.H Variant Activity (POST)
- [x] ET ADWARE_PUP Kuwo Music Installer Log
- [x] ET ADWARE_PUP Win32/GameHack.ADW CnC Activity
- [x] ET ADWARE_PUP Bluebox Data Exfiltration
- [x] ET ADWARE_PUP Win/Malware.FileTour Variant Checkin
- [x] ET ADWARE_PUP Win/Malware.Filetour Variant Checkin M2
- [x] ET ADWARE_PUP AlphabetSoup Adware Extension CnC Checkin
- [x] ET ADWARE_PUP Win32 Handy Cafe Checkin
- [x] ET ADWARE_PUP DriverPack Update Checkin
- [x] ET ADWARE_PUP Win32/ReImageRepair.T CnC Checkin
- [x] ET ADWARE_PUP CoinSurf Proxy Client Registration
- [x] ET ADWARE_PUP CoinSurf Proxy CnC Response (Refesh Token)
- [x] ET ADWARE_PUP Win32/Swjoy.A Telemetry Checkin
- [x] ET ADWARE_PUP pdfspeedup Initial CnC Checkin
- [x] ET ADWARE_PUP Win32/ReImageRepair.T CnC Cookie Pattern
- [x] ET ADWARE_PUP MuLauncher Telemetry Gathering Attempt
- [x] ET ADWARE_PUP ZeroTier P2P VPN Activity M1
- [ ] ET ADWARE_PUP Observed DNS Query to PUP Domain (superdiag .xyz)
- [x] ET ADWARE_PUP Win32/DownWare.G Installer Request
- [x] ET ADWARE_PUP Win32/Adware.Agent.NSF CnC Checkin M1
- [x] ET ADWARE_PUP DriverTurbo Domain (driverfinderpro .com) in DNS Lookup
- [x] ET ADWARE_PUP Win32/Adware.Neoreklami.MI Activity M1
- [x] ET ADWARE_PUP Win32/Atshz.A Checkin
- [x] ET ADWARE_PUP Observed DNS Query to PUP Domain (omnatuor .com)
- [x] ET ADWARE_PUP Win32/VoipRaider Data Collection Attempt
- [x] ET ADWARE_PUP BoostBeast Task Request M2
- [x] ET ADWARE_PUP BoostBeast Checkin M2
- [x] ET ADWARE_PUP Win32/Presenoker Checkin
- [x] ET ADWARE_PUP Win32/Packed.FlyStudio.AA Checkin
- [x] ET ADWARE_PUP Win32/VrBrothers Checkin
- [x] ET ADWARE_PUP MacOS/OnlineAppNotice Activity
- [x] ET ADWARE_PUP Win32/Adware.VrBrothers.AI Variant CnC Activity
- [x] ET ADWARE_PUP SUPERAntiSpyware Install Checkin
- [x] ET ADWARE_PUP ZoomInfo Contact Contributor Install
- [x] ET ADWARE_PUP FormatFactory Install Checkin
- [x] ET ADWARE_PUP Win32/InstallCore.GF CnC Activity
- [x] ET ADWARE_PUP Win32/Xetapp Installer Checkin
- [x] ET ADWARE_PUP Observed DownloadAssistant User-Agent
- [x] ET ADWARE_PUP FLV/Youtube Downloader Install Activity
- [x] ET ADWARE_PUP STOPzilla Download Accelerator Activity
- [x] ET ADWARE_PUP Win32/Sogou.H Variant Request
- [x] ET ADWARE_PUP Win32/Qihoo360.J Variant Install Report
- [x] ET ADWARE_PUP Win32/RemoteUtilities Checkin via SMTP
- [x] ET ADWARE_PUP DriverPack Domain in DNS Query
- [x] ET ADWARE_PUP SuperAntiSpyware Install Checkin
- [x] ET ADWARE_PUP OSX/Adware.Pirrit CnC Activity 4
- [x] ET ADWARE_PUP Win32/Spy.Agent.QCL Variant Activity (POST) M2
- [x] ET ADWARE_PUP Nivesro Cheat CnC Activity M1
- [x] ET ADWARE_PUP Win32/TrojanDownloader.Agent.BXA CnC Activity
- [x] ET ADWARE_PUP ThunderUnion Install Checkin
- [x] ET ADWARE_PUP Win32/MobiGame Install Stats Checkin M1
- [x] ET ADWARE_PUP Win32/MobiGame Install Stats Checkin M3
- [x] ET ADWARE_PUP Win32/TrojanDownloader.Adload.NSD Variant Checkin
- [x] ET ADWARE_PUP Win32.Perinet CnC Checkin
- [x] ET ADWARE_PUP Win32/Systweak Checkin M2
- [x] ET ADWARE_PUP Win32/RemoteUtilities Checkin via SMTP M2
- [x] ET ADWARE_PUP Win32/DownWare.V Checkin
- [x] ET ADWARE_PUP Win32/Hao123.C Variant CnC Activity
- [x] ET ADWARE_PUP Win32/2144FlashPlayer.E Checkin
- [x] ET ADWARE_PUP Win/Malware.Filetour Variant Checkin M1
- [x] ET ADWARE_PUP Win/Malware.FileTour Variant Checkin
- [x] ET ADWARE_PUP Win/Malware.Filetour Variant Checkin M3
- [x] ET ADWARE_PUP Win32/Mando Activity (GET)
- [x] ET ADWARE_PUP Observed DNS Query to DriverPack Domain (.drp .su)
- [ ] ET ADWARE_PUP Observed DNS Query to Restoro PUP Domain (restoro .com)
- [x] ET ADWARE_PUP CoinSurf Proxy CnC Response
- [x] ET ADWARE_PUP CoinSurf Proxy Client Login
- [x] ET ADWARE_PUP CoinSurf Proxy CnC Response (Network Configuration)
- [x] ET ADWARE_PUP Observed PUA SSL/TLS Certificate (HoneyGain)
- [x] ET ADWARE_PUP pdfspeedup Keep-Alive
- [x] ET ADWARE_PUP Win32/ReImageRepair.T CnC Activity
- [x] ET ADWARE_PUP Win32/Speedbit Variant Checkin
- [x] ET ADWARE_PUP Win32/Adware.InstallCommerce.A CnC Checkin
- [x] ET ADWARE_PUP Win32/SuperDiag PUP CnC Activity
- [x] ET ADWARE_PUP Win32/Adware.WDJiange.A CnC Checkin M1
- [x] ET ADWARE_PUP DriverTurbo Domain (driverturbo .com) in DNS Lookup
- [x] ET ADWARE_PUP DriverFinder User-Agent Observed in HTTP Traffic
- [x] ET ADWARE_PUP Win32/Adware.Neoreklami.MI Activity M2
- [x] ET ADWARE_PUP Win32/Atshz.A Checkin M2
- [x] ET ADWARE_PUP Tensorshare Google Analytics Checkin
- [x] ET ADWARE_PUP BoostBeast Task Request M1
- [x] ET ADWARE_PUP BoostBeast Checkin M1
- [x] ET ADWARE_PUP BoostBeast Task Response
- [x] ET ADWARE_PUP Win32/Pearfoos.B!ml Checkin
- [x] ET ADWARE_PUP Win32/DealPly.EJ Checkin
- [x] ET ADWARE_PUP PUP/SpamFighter CnC Request
- [x] ET ADWARE_PUP DNS Query to Neoreklami (service-domain .xyz)

- [x] ET ADWARE_PUP DNS Query to Neoreklami (check-data .xyz)
- [x] ET ADWARE_PUP DNS Query to Neoreklami (vadimmqz .beget .tech)
- [x] ET ADWARE_PUP DNS Query to Neoreklami Domain (testupdate .info)
- [x] ET ADWARE_PUP DNS Query to Neoreklami Domain (133455789 .xyz)
- [x] ET ADWARE_PUP Win32/FeIQ Activity (GET)
- [x] ET ADWARE_PUP Win32/TrojanDownloader Variant Activity (GET)
- [x] ET ADWARE_PUP Suspected Adware/AccessMembre Domain in DNS Lookup (iconm1 .com)
- [x] ET ADWARE_PUP Suspected Adware/AccessMembre Checkin M2
- [x] ET ADWARE_PUP Suspected Adware/AccessMembre Checkin M3
- [x] ET ADWARE_PUP Bypass Ticket Monitoring Domain in DNS Lookup (www .bypass .cn)
- [x] ET ADWARE_PUP Observed Bypass Ticket Monitoring Domain (www .bypass .cn in TLS SNI)
- [x] ET ADWARE_PUP Bypass Ticket Monitoring Activity (POST)
- [x] ET ADWARE_PUP Bypass Ticket Monitoring Activity (POST)
- [x] ET ADWARE_PUP DNS Query to PacketShare Proxy API Domain (api .packetshare .io)
- [x] ET ADWARE_PUP Observed PacketShare Proxy Domain Domain (api .packetshare .io in TLS SNI)
- [x] ET ADWARE_PUP PacketShare Proxy Connection Init (POST)
- [x] ET ADWARE_PUP PacketShare Proxy Connection Heartbeat (POST)
- [x] ET ADWARE_PUP PacketShare Proxy Client Login (GET)
- [x] ET ADWARE_PUP Observed DNS Query to PC Optimizer Software Domain (fortect .com)
- [x] ET ADWARE_PUP Observed PC Optimizer Software Domain (fortect .com in TLS SNI)
- [ ] ET ADWARE_PUP DNS Query to Seetrol RAT Domain (seetrol .com)
- [ ] ET ADWARE_PUP DNS Query to Seetrol RAT Domain (seetrol .kr)
- [x] ET ADWARE_PUP Observed Seetrol RAT Domain (seetrol .kr in TLS SNI)
- [x] ET ADWARE_PUP Observed Seetrol RAT Domain (seetrol .com in TLS SNI)
- [x] ET ADWARE_PUP Seetrol Remote Administration Tool Download
- [x] ET ADWARE_PUP Query to Seetrol RAT Domain (seetrol .co .kr)
- [x] ET ADWARE_PUP Observed Seetrol RAT Domain (seetrol .co .kr in TLS SNI)
- [x] ET ADWARE_PUP Drivermax Utility Checkin Activity
- [x] ET ADWARE_PUP SimpleHelp Remote Access Software Activity
- [x] ET ADWARE_PUP NBP Mac PUP User-Agent Observed
- [x] ET ADWARE_PUP Muzcat Media Player User-Agent Observed (muzcat)

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

- [x] ET ATTACK_RESPONSE FTP inaccessible directory access COM1
- [x] ET ATTACK_RESPONSE FTP inaccessible directory access COM2
- [x] ET ATTACK_RESPONSE FTP inaccessible directory access COM3
- [x] ET ATTACK_RESPONSE FTP inaccessible directory access COM4
- [x] ET ATTACK_RESPONSE FTP inaccessible directory access LPT1
- [x] ET ATTACK_RESPONSE FTP inaccessible directory access LPT2
- [x] ET ATTACK_RESPONSE FTP inaccessible directory access LPT3
- [x] ET ATTACK_RESPONSE FTP inaccessible directory access LPT4
- [x] ET ATTACK_RESPONSE FTP inaccessible directory access AUX
- [x] ET ATTACK_RESPONSE FTP inaccessible directory access NULL
- [x] ET ATTACK_RESPONSE Zone-H.org defacement notification
- [ ] ET ATTACK_RESPONSE Outbound PHP Connection
- [x] ET ATTACK_RESPONSE Possible /etc/passwd via HTTP (linux style)
- [x] ET ATTACK_RESPONSE Hostile FTP Server Banner (StnyFtpd)
- [x] ET ATTACK_RESPONSE Hostile FTP Server Banner (Reptile)
- [x] ET ATTACK_RESPONSE Hostile FTP Server Banner (Bot Server)
- [x] ET ATTACK_RESPONSE Possible /etc/passwd via HTTP (BSD style)
- [x] ET ATTACK_RESPONSE Possible /etc/passwd via SMTP (linux style)
- [x] ET ATTACK_RESPONSE Possible /etc/passwd via SMTP (BSD style)
- [x] ET ATTACK_RESPONSE Unusual FTP Server Banner (warFTPd)
- [x] ET ATTACK_RESPONSE Unusual FTP Server Banner (freeFTPd)
- [x] ET ATTACK_RESPONSE r57 phpshell footer detected
- [ ] ET ATTACK_RESPONSE r57 phpshell source being uploaded
- [x] ET ATTACK_RESPONSE Weak Netbios Lanman Auth Challenge Detected
- [x] ET ATTACK_RESPONSE x2300 phpshell detected
- [ ] ET ATTACK_RESPONSE c99shell phpshell detected
- [ ] ET ATTACK_RESPONSE RFI Scanner detected
- [ ] ET ATTACK_RESPONSE C99 Modified phpshell detected
- [ ] ET ATTACK_RESPONSE lila.jpg phpshell detected
- [ ] ET ATTACK_RESPONSE ALBANIA id.php detected
- [ ] ET ATTACK_RESPONSE Mic22 id.php detected
- [ ] ET ATTACK_RESPONSE Off-Port FTP Without Banners - user
- [ ] ET ATTACK_RESPONSE Off-Port FTP Without Banners - pass
- [ ] ET ATTACK_RESPONSE Off-Port FTP Without Banners - retr
- [x] ET ATTACK_RESPONSE Unusual FTP Server Banner on High Port (WinFtpd)
- [x] ET ATTACK_RESPONSE Unusual FTP Server Banner on High Port (StnyFtpd)
- [x] ET ATTACK_RESPONSE Windows LMHosts File Download - Likely DNSChanger Infection
- [x] ET ATTACK_RESPONSE Possible MS CMD Shell opened on local system
- [ ] ET ATTACK_RESPONSE Possible ASPXSpy Request
- [ ] ET ATTACK_RESPONSE Possible ASPXSpy Related Activity
- [ ] ET ATTACK_RESPONSE Possible ASPXSpy Upload Attempt
- [x] ET ATTACK_RESPONSE Unusual FTP Server Banner (fuckFtpd)
- [x] ET ATTACK_RESPONSE Unusual FTP Server Banner (NzmxFtpd)
- [ ] ET ATTACK_RESPONSE Cisco TclShell TFTP Read Request
- [x] ET ATTACK_RESPONSE Cisco TclShell TFTP Download
- [ ] ET ATTACK_RESPONSE HTTP 401 Unauthorized
- [ ] ET ATTACK_RESPONSE Frequent HTTP 401 Unauthorized - Possible Brute Force Attack
- [ ] ET ATTACK_RESPONSE Metasploit Meterpreter File Download Detected
- [ ] ET ATTACK_RESPONSE Metasploit Meterpreter Process List (ps) Command Detected
- [ ] ET ATTACK_RESPONSE Metasploit Meterpreter Getuid Command Detected
- [ ] ET ATTACK_RESPONSE Metasploit Meterpreter Process Migration Detected
- [ ] ET ATTACK_RESPONSE Metasploit Meterpreter ipconfig Command Detected
- [ ] ET ATTACK_RESPONSE Metasploit Meterpreter Sysinfo Command Detected
- [ ] ET ATTACK_RESPONSE Metasploit Meterpreter Route Command Detected
- [ ] ET ATTACK_RESPONSE Metasploit Meterpreter Kill Process Command Detected
- [ ] ET ATTACK_RESPONSE Metasploit Meterpreter Print Working Directory Command Detected
- [ ] ET ATTACK_RESPONSE Metasploit Meterpreter View Current Process ID Command Detected
- [ ] ET ATTACK_RESPONSE Metasploit Meterpreter Execute Command Detected
- [ ] ET ATTACK_RESPONSE Metasploit Meterpreter System Reboot/ Shutdown Detected
- [ ] ET ATTACK_RESPONSE Metasploit Meterpreter System Get Idle Time Command Detected

- [ ] ET ATTACK_RESPONSE Metasploit Meterpreter Make Directory Command Detected
- [ ] ET ATTACK_RESPONSE Metasploit Meterpreter Remove Directory Command Detected
- [ ] ET ATTACK_RESPONSE Metasploit Meterpreter Change Directory Command Detected
- [ ] ET ATTACK_RESPONSE Metasploit Meterpreter List (ls) Command Detected
- [ ] ET ATTACK_RESPONSE Metasploit Meterpreter rev2self Command Detected
- [ ] ET ATTACK_RESPONSE Metasploit Meterpreter Enabling/Disabling of Keyboard Detected
- [ ] ET ATTACK_RESPONSE Metasploit Meterpreter Enabling/Disabling of Mouse Detected
- [ ] ET ATTACK_RESPONSE Metasploit Meterpreter File/Memory Interaction Detected
- [x] ET ATTACK_RESPONSE Metasploit Meterpreter Registry Interation Detected
- [ ] ET ATTACK_RESPONSE Metasploit Meterpreter File Upload Detected
- [ ] ET ATTACK_RESPONSE Metasploit/Meterpreter - Sending metsrv.dll to Compromised Host
- [ ] ET ATTACK_RESPONSE Metasploit Meterpreter Channel Interaction Detected, Likely Interaction With Executable
- [ ] ET ATTACK_RESPONSE Possible Ipconfig Information Detected in HTTP Response
- [ ] ET ATTACK_RESPONSE Ipconfig Response Detected
- [ ] ET ATTACK_RESPONSE Metasploit/Meterpreter - Sending metsrv.dll to Compromised Host
- [x] ET ATTACK_RESPONSE Matahari client
- [x] ET ATTACK_RESPONSE Backdoor reDuh http initiate
- [x] ET ATTACK_RESPONSE Backdoor reDuh http tunnel
- [x] ET ATTACK_RESPONSE Windows 7 CMD Shell from Local System
- [x] ET ATTACK_RESPONSE WSO - WebShell Activity - WSO Title
- [x] ET ATTACK_RESPONSE WSO - WebShell Activity - POST structure
- [x] ET ATTACK_RESPONSE MySQL User Account Enumeration
- [x] ET ATTACK_RESPONSE Obfuscated JS - Possible URL Encoded JS Inbound
- [x] ET ATTACK_RESPONSE Obfuscated JS - URL Encoded Unescape Function Call Inbound
- [x] ET ATTACK_RESPONSE Net User Command Response
- [x] ET ATTACK_RESPONSE Possible IPMI 2.0 RAKP Remote SHA1 Password Hash Retrieval RAKP message 2 status code Unauthorized Name
- [x] ET ATTACK_RESPONSE Non-Local Burp Proxy Error
- [x] ET ATTACK_RESPONSE Obfuscated Eval String 1
- [x] ET ATTACK_RESPONSE Obfuscated Eval String 2
- [x] ET ATTACK_RESPONSE Obfuscated Eval String 3
- [x] ET ATTACK_RESPONSE Obfuscated Eval String 4
- [x] ET ATTACK_RESPONSE Obfuscated Eval String 5
- [x] ET ATTACK_RESPONSE Obfuscated Eval String 6
- [x] ET ATTACK_RESPONSE Obfuscated Eval String (Single Q) 1
- [x] ET ATTACK_RESPONSE Obfuscated Eval String (Single Q) 2
- [x] ET ATTACK_RESPONSE Obfuscated Eval String (Single Q) 3
- [x] ET ATTACK_RESPONSE Obfuscated Eval String (Single Q) 4
- [x] ET ATTACK_RESPONSE Obfuscated Eval String (Single Q) 5
- [x] ET ATTACK_RESPONSE Obfuscated Eval String (Single Q) 6
- [x] ET ATTACK_RESPONSE Obfuscated Eval String (Single Q) 7
- [x] ET ATTACK_RESPONSE Obfuscated Eval String 7
- [x] ET ATTACK_RESPONSE python shell spawn attempt
- [x] ET ATTACK_RESPONSE Probably Evil Long Unicode string only string and unescape 1
- [x] ET ATTACK_RESPONSE Probably Evil Long Unicode string only string and unescape 2
- [x] ET ATTACK_RESPONSE Probably Evil Long Unicode string only string and unescape 3
- [x] ET ATTACK_RESPONSE Probably Evil Long Unicode string only string and unescape 3
- [x] ET ATTACK_RESPONSE webr00t WebShell Access
- [x] ET ATTACK_RESPONSE PHP script in OptimizePress Upload Directory Possible WebShell Access
- [x] ET ATTACK_RESPONSE Linksys Router Returning Device Settings To External Source
- [x] ET ATTACK_RESPONSE Possible MS CMD Shell opened on local system 2
- [x] ET ATTACK_RESPONSE Output of id command from HTTP server
- [x] ET ATTACK_RESPONSE Microsoft Powershell Banner Outbound
- [x] ET ATTACK_RESPONSE Microsoft CScript Banner Outbound
- [x] ET ATTACK_RESPONSE Microsoft WMIC Prompt Outbound
- [x] ET ATTACK_RESPONSE Microsoft Netsh Firewall Disable Output Outbound
- [x] ET ATTACK_RESPONSE SysInternals sc.exe Output Outbound
- [ ] ET ATTACK_RESPONSE MySQL error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE MySQL error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE MySQL error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE MySQL error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE MySQL error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE MySQL error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE PostgreSQL error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE PostgreSQL error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE PostgreSQL error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE PostgreSQL error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE PostgreSQL error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE PostgreSQL error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE Microsoft SQL error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE Microsoft SQL error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE Microsoft SQL error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE Microsoft SQL error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE Microsoft SQL error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE Microsoft SQL error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE Microsoft Access error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE Microsoft Access error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE Oracle error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE Oracle error in HTTP response, possible SQL injection point

- [ ] ET ATTACK_RESPONSE Oracle error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE Oracle error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE DB2 error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE Informix error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE Firebird error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE SQLite error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE SQLite error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE SQLite error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE SAP MaxDB error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE Sybase error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE Ingres error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE Ingres error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE HSQLDB error in HTTP response, possible SQL injection point
- [x] ET ATTACK_RESPONSE Possible CVE-2016-1287 Inbound Reverse CLI Shellcode
- [x] ET ATTACK_RESPONSE 401TRG Perl DDoS IRCBot File Download
- [x] ET ATTACK_RESPONSE Inbound PowerShell Checking for Virtual Host (Win32_Fan WMI)
- [x] ET ATTACK_RESPONSE Inbound PowerShell Checking for Virtual Host (Win32_PointingDevice WMI)
- [x] ET ATTACK_RESPONSE Inbound PowerShell Checking for Virtual Host (Win32_BaseBoard WMI)
- [x] ET ATTACK_RESPONSE Possible System Enumeration via WMI Queries (AntiSpywareProduct)
- [x] ET ATTACK_RESPONSE Possibly Malicious VBS Writing to Persistence Registry Location
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded New-Object (ctT2J) in DNS TXT Response
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded New-Object (V3LU9iam) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded New-Object (dy1PYmplY3) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Start-Process (RhcnQtUHJ) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Start-Process (RhcnQtUHJvY2) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Start-Process (YXJ0LVByb2Nlc3) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-WmiMethod (52b2tlLVdtaU1) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-WmiMethod (52b2tlLVdtaU1ldG) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-WmiMethod (dm9rZS1XbWlNZXRob2) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-Command (dm9rZS1Db21) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-Command (52b2tlLUNvbW1) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-Command (52b2tlLUNvbW1hbm) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell Base64 Encoded Content Command Common In Powershell Stagers M1
- [x] ET ATTACK_RESPONSE UTF8 base64 string /This Program/ in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE UTF8 base64 string /This Program/ in DNS TXT Reponse
- [ ] ET ATTACK_RESPONSE Oracle error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE DB2 error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE DB2 error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE Firebird error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE SQLite error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE SQLite error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE SQLite error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE SAP MaxDB error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE Sybase error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE Sybase error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE Ingres error in HTTP response, possible SQL injection point
- [ ] ET ATTACK_RESPONSE Frontbase error in HTTP response, possible SQL injection point
- [x] ET ATTACK_RESPONSE Metasploit Meterpreter Reverse HTTPS certificate
- [x] ET ATTACK_RESPONSE Possible BeEF HTTP Headers Inbound
- [x] ET ATTACK_RESPONSE passwd file Outbound from WEB SERVER Linux
- [x] ET ATTACK_RESPONSE Inbound PowerShell Checking for Virtual Host (MSAcpi_ThermalZoneTemperature WMI)
- [x] ET ATTACK_RESPONSE Inbound PowerShell Checking for Virtual Host (Win32_DiskDevice WMI)
- [x] ET ATTACK_RESPONSE Possible System Enumeration via WMI Queries (AntiVirusProduct)
- [x] ET ATTACK_RESPONSE Possible System Enumeration via WMI Queries (FirewallProduct)
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded New-Object (V3LU9) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded New-Object (dy1PYmp) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded New-Object (XctT2JqZW) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Start-Process (FydC1Qcm9) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Start-Process (YXJ0LVByb2N) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Start-Process (GFydC1Qcm9jZX) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-WmiMethod (Zva2UtV21pTWV) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-WmiMethod (dm9rZS1XbWlNZXR) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-WmiMethod (nZva2UtV21pTWV0aG) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-Command (Zva2UtQ29) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-Command (nZva2UtQ29tbW) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell Execution String Base64 Encoded Invoke-Command (dm9rZS1Db21tYW) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell NoProfile Command Received In Powershell Stagers
- [x] ET ATTACK_RESPONSE PowerShell Base64 Encoded Content Command Common In Powershell Stagers M2
- [x] ET ATTACK_RESPONSE UTF8 base64 string /This Program/ in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE UTF16-LE base64 string /This Program/ in DNS TXT Reponse

- [x] ET ATTACK_RESPONSE UTF16-LE base64 string /This Program/ in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE UTF8 base64 wide string /This Program/ in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE UTF8 base64 wide string /This Program/ in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE UTF16-LE base64 wide string /This Program/ in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE UTF8 base64 reversed string /This Program/ in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE UTF8 base64 reversed string /This Program/ in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE UTF16 base64 reversed string /This Program/ in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE LaZagne Artifact Outbound in FTP
- [x] ET ATTACK_RESPONSE Windows SCM DLL Hijack Command Inbound via HTTP M2
- [x] ET ATTACK_RESPONSE Windows SCM DLL Hijack Command (UTF-16) Inbound via HTTP M2
- [x] ET ATTACK_RESPONSE Windows SCM DLL Hijack Command (UTF-16) Inbound via HTTP M3
- [ ] ET ATTACK_RESPONSE Possible Remote System32 DLL Hijack Command Inbound via HTTP (T1038, T1105)
- [x] ET ATTACK_RESPONSE Windows 64bit procdump Dump File Exfiltration
- [x] ET ATTACK_RESPONSE Muhstik Botnet Download Activity (GET)
- [x] ET ATTACK_RESPONSE Obfuscated Batch Script Inbound M2
- [x] ET ATTACK_RESPONSE Bash Script Inbound - Kill Coin Mining Related Processes
- [x] ET ATTACK_RESPONSE Possible CVE-2021-44228 Payload via LDAPv3 Response
- [x] ET ATTACK_RESPONSE Possible CVE-2021-44228 Payload via LDAPv3 Response M2
- [x] ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Security Scanner Domain (log4shell .huntress .com)
- [x] ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Callback Domain (ceye .io)
- [x] ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Callback Domain (pwn .af)
- [x] ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Callback Domain (scannermcscanface-edgescan .com)
- [x] ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Callback Domain (scanworld .net)
- [x] ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Security Scanner Domain (log4j. leakix .net)
- [x] ET ATTACK_RESPONSE Possible ELEFANTE/ElephantBeetle Command Tunneling M1
- [x] ET ATTACK_RESPONSE Possible ELEFANTE/ElephantBeetle Enumeration Activity M1
- [x] ET ATTACK_RESPONSE Possible ELEFANTE/ElephantBeetle Lateral Movement Activity
- [x] ET ATTACK_RESPONSE PowerShell Geo Check Before Execution
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE UTF16-LE base64 string /This Program/ in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE UTF8 base64 wide string /This Program/ in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE UTF16-LE base64 wide string /This Program/ in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE UTF16-LE base64 wide string /This Program/ in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE UTF8 base64 reversed string /This Program/ in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE UTF16 base64 reversed string /This Program/ in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE UTF16 base64 reversed string /This Program/ in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE Windows SCM DLL Hijack Command Inbound via HTTP M1
- [x] ET ATTACK_RESPONSE Windows SCM DLL Hijack Command (UTF-16) Inbound via HTTP M1
- [x] ET ATTACK_RESPONSE Windows SCM DLL Hijack Command Inbound via HTTP M3
- [x] ET ATTACK_RESPONSE Possible Lateral Movement - File Creation Request in Remote System32 Directory (T1105)
- [x] ET ATTACK_RESPONSE PowerShell Internet Connectivity Check via Network GUID Inbound
- [x] ET ATTACK_RESPONSE Windows 32bit procdump Dump File Exfiltration
- [x] ET ATTACK_RESPONSE Obfuscated Batch Script Inbound M1
- [ ] ET ATTACK_RESPONSE Obfuscated VBS Inbound - Underscore Var/ Chr/math
- [ ] ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Callback Domain (bingsearchlib .com)
- [x] ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Callback Domain (rce .ee)
- [x] ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Security Scanner Domain (log4j .binaryedge .io)
- [x] ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Security Scanner Domain (kryptoslogic-cve-2021-44228 .com)
- [x] ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Callback Domain (oob .li)
- [x] ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Callback Domain (notburpcollaborator .net)
- [x] ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Callback Domain (service .exfil .site)
- [x] ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Callback Domain (log .exposedbotnets .ru)
- [x] ET ATTACK_RESPONSE DNS Query for Observed CVE-2021-44228 Security Scanner Domain (canarytokens .com)
- [x] ET ATTACK_RESPONSE Possible ELEFANTE/ElephantBeetle Command Tunneling M2
- [x] ET ATTACK_RESPONSE Possible ELEFANTE/ElephantBeetle Enumeration Activity M2
- [x] ET ATTACK_RESPONSE Apache Spark RPC - Unauthenticated RegisterApplication - Successfully Registered (CVE-2020-9480)
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed

- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed

- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed

- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed

- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed

- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed

- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed

- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE Havoc/Sliver Framework TLS Certificate Observed
- [x] ET ATTACK_RESPONSE HTML Smuggling Powershell Payload In href
- [x] ET ATTACK_RESPONSE HTML Smuggling Powershell Payload In iframe
- [x] ET ATTACK_RESPONSE net user Command Output via HTTP POST
- [x] ET ATTACK_RESPONSE Nishang Invoke-PowerShellTcp Shell Prompt Outbound
- [x] ET ATTACK_RESPONSE Possible WebShell Upload Attempt via Directory Traversal M1
- [x] ET ATTACK_RESPONSE Possible WebShell Upload Attempt via Directory Traversal M2
- [x] ET ATTACK_RESPONSE MalDoc/Generik.ILNMZZB Payload Inbound
- [x] ET ATTACK_RESPONSE JS/Spy.Banker.LD Credit Card Skimmer Inbound
- [x] ET ATTACK_RESPONSE VBA/Subdoc.B Obfuscated Payload Inbound
- [x] ET ATTACK_RESPONSE Possible PowerShell AMSI Bypass Inbound
- [x] ET ATTACK_RESPONSE PowerShell String Base64 Encoded Invoke-RestMethod (dm9rZS1SZXN0TWV0) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell String Base64 Encoded Invoke-RestMethod (Zva2UtUmVzdE1ld) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell String Base64 Encoded Invoke-RestMethod (2b2tlLVJlc3RNZX) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell String Base64 Encoded Text.Encoding (ZXh0LkVuY29k) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell String Base64 Encoded Text.Encoding (V4dC5FbmNvZ) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE PowerShell String Base64 Encoded Text.Encoding (leHQuRW5jb2) in DNS TXT Reponse
- [x] ET ATTACK_RESPONSE VBS/TrojanDownloader.Agent.YLH Payload Inbound
- [x] ET ATTACK_RESPONSE Interactive Reverse Shell Without TTY (Outbound)
- [x] ET ATTACK_RESPONSE Nemesis Admin Panel Inbound
- [x] ET ATTACK_RESPONSE Nemesis Admin Panel Inbound
- [x] ET ATTACK_RESPONSE Possible PaperCut MF/NG Post Exploitation Domain in DNS Lookup (windowcsupdates .com)
- [x] ET ATTACK_RESPONSE Possible PaperCut MF/NG Post Exploitation Domain in DNS Lookup (anydeskupdate .com)
- [x] ET ATTACK_RESPONSE Possible PaperCut MF/NG Post Exploitation Domain in DNS Lookup (anydeskupdates .com)
- [x] ET ATTACK_RESPONSE Possible PaperCut MF/NG Post Exploitation Domain in DNS Lookup (windowservicecemter .com)
- [x] ET ATTACK_RESPONSE Possible PaperCut MF/NG Post Exploitation Domain in DNS Lookup (winserverupdates .com)
- [x] ET ATTACK_RESPONSE Possible PaperCut MF/NG Post Exploitation Domain in DNS Lookup (netviewremote .com)
- [x] ET ATTACK_RESPONSE Possible PaperCut MF/NG Post Exploitation Domain in DNS Lookup (updateservicecenter .com)
- [x] ET ATTACK_RESPONSE Possible PaperCut MF/NG Post Exploitation Domain in DNS Lookup (windowservicecenter .com)
- [x] ET ATTACK_RESPONSE Possible PaperCut MF/NG Post Exploitation Domain in DNS Lookup (windowservicecentar .com)
- [x] ET ATTACK_RESPONSE Mystic Stealer Admin Panel Inbound
- [x] ET ATTACK_RESPONSE reNgine Recon Panel Inbound
- [x] ET ATTACK_RESPONSE MrRobot LYON Admin Panel Inbound
- [x] ET ATTACK_RESPONSE Amadey CnC Panel Inbound
- [x] ET ATTACK_RESPONSE Mana Tools-Lone Wolf Admin Panel Inbound
- [x] ET ATTACK_RESPONSE FightAgent WebShell Response Outbound
- [x] ET ATTACK_RESPONSE Possible /etc/shadow via HTTP M1
- [x] ET ATTACK_RESPONSE Possible /etc/shadow via HTTP M2
- [x] ET ATTACK_RESPONSE Possible /etc/shadow via HTTP M3
- [x] ET ATTACK_RESPONSE Possible /etc/shadow via HTTP M4
- [x] ET ATTACK_RESPONSE Possible arp command output via HTTP (Linux Style)
- [x] ET ATTACK_RESPONSE Possible arp command output via HTTP (Windows Style)
- [x] ET ATTACK_RESPONSE Possible arp command output via HTTP (MacOS Style)
- [x] ET ATTACK_RESPONSE Possible hosts File Output via HTTP (Windows Style)
- [x] ET ATTACK_RESPONSE Possible hosts File Output via HTTP (Linux Style)
- [x] GPL ATTACK_RESPONSE command completed
- [x] GPL ATTACK_RESPONSE command error
- [x] GPL ATTACK_RESPONSE file copied ok
- [x] GPL ATTACK_RESPONSE id check returned root
- [x] GPL ATTACK_RESPONSE del attempt
- [x] GPL ATTACK_RESPONSE directory listing
- [ ] GPL ATTACK_RESPONSE Invalid URL
- [ ] GPL ATTACK_RESPONSE directory listing
- [x] GPL ATTACK_RESPONSE index of /cgi-bin/ response
- [ ] GPL ATTACK_RESPONSE id check returned userid
- [x] GPL ATTACK_RESPONSE id check returned nobody
- [x] GPL ATTACK_RESPONSE id check returned web
- [ ] GPL ATTACK_RESPONSE id check returned http
- [x] GPL ATTACK_RESPONSE id check returned apache
- [x] GPL ATTACK_RESPONSE isakmp login failed

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

- [x] ET CNC Feodo Tracker Reported CnC Server group 1
- [x] ET CNC Feodo Tracker Reported CnC Server group 2
- [x] ET CNC Feodo Tracker Reported CnC Server group 3
- [x] ET CNC Feodo Tracker Reported CnC Server group 4
- [x] ET CNC Feodo Tracker Reported CnC Server group 5
- [x] ET CNC Feodo Tracker Reported CnC Server group 6
- [x] ET CNC Feodo Tracker Reported CnC Server group 7
- [x] ET CNC Feodo Tracker Reported CnC Server group 8
- [x] ET CNC Feodo Tracker Reported CnC Server group 9
- [x] ET CNC Feodo Tracker Reported CnC Server group 10
- [x] ET CNC Feodo Tracker Reported CnC Server group 11
- [x] ET CNC Feodo Tracker Reported CnC Server group 12
- [x] ET CNC Feodo Tracker Reported CnC Server group 13
- [x] ET CNC Feodo Tracker Reported CnC Server group 14
- [x] ET CNC Feodo Tracker Reported CnC Server group 15
- [x] ET CNC Feodo Tracker Reported CnC Server group 16
- [x] ET CNC Feodo Tracker Reported CnC Server group 17
- [x] ET CNC Feodo Tracker Reported CnC Server group 18
- [x] ET CNC Feodo Tracker Reported CnC Server group 19
- [x] ET CNC Feodo Tracker Reported CnC Server group 20
- [x] ET CNC Feodo Tracker Reported CnC Server group 21
- [x] ET CNC Feodo Tracker Reported CnC Server group 22
- [x] ET CNC Feodo Tracker Reported CnC Server group 23

- [ ] **emerging-chat.rules** Show
- [x] **emerging-ciarmy.rules** Hide

- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 1
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 2
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 3
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 4
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 5
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 6
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 7
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 8
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 9
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 10
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 11
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 12
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 13
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 14
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 15
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 16
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 17
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 18
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 19
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 20
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 21
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 22
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 23
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 24
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 25
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 26
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 27
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 28
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 29
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 30
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 31
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 32
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 33
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 34
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 35
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 36
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 37
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 38
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 39
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 40
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 41
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 42
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 43
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 44
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 45
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 46
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 47
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 48
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 49
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 50
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 51
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 52
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 53
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 54
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 55
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 56
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 57
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 58
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 59
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 60
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 61
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 62
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 63
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 64
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 65
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 66
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 67
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 68
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 69
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 70
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 71
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 72
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 73
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 74
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 75
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 76
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 77
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 78
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 79
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 80
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 81
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 82
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 83
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 84
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 85
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 86
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 87
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 88
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 89
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 90
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 91
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 92
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 93
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 94
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 95
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 96
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 97
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 98
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 99
- [x] ET CINS Active Threat Intelligence Poor Reputation IP group 100

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

- [x] ET COINMINER Possible BitCoin Miner User-Agent (miner)
- [x] ET COINMINER Bitcoin Mining Extensions Header
- [x] ET COINMINER W32/BitCoinMiner.MultiThreat Subscribe/Authorize Stratum Protocol Message
- [x] ET COINMINER W32/BitCoinMiner.MultiThreat Stratum Protocol Mining.Notify Initial Connection Server Response
- [x] ET COINMINER W32/BitCoinMiner.MultiThreat Stratum Protocol Mining.Notify Work Server Response
- [ ] ET COINMINER W32/BitCoinMiner Fake Flash Player Distribution Campaign - December 2013
- [x] ET COINMINER W32/BitCoinMiner.MultiThreat Getblocktemplate Protocol Server Connection
- [x] ET COINMINER W32/BitCoinMiner.MultiThreat Getblocktemplate Protocol Server Coinbasetxn Begin Mining Response
- [x] ET COINMINER PrimeCoinMiner.Protominer
- [x] ET COINMINER Cryptexplorer API Check - Potential CoinMiner Traffic
- [ ] ET COINMINER CoinMiner Malicious Authline Seen in JAR Backdoor
- [x] ET COINMINER Crypto Coin Miner Login
- [x] ET COINMINER CoinHive In-Browser Miner Detected
- [x] ET COINMINER Observed DNS Query to Browser Coinminer (crypto-loot[.]com)
- [x] ET COINMINER CoinMiner Malicious Authline Seen After CVE-2017-10271 Exploit
- [x] ET COINMINER Observed Coin-Hive In Browser Mining Domain (coin-hive .com in TLS SNI)
- [x] ET COINMINER Observed Malicious SSL Cert (Coin-Hive In Browser Mining)
- [x] ET COINMINER Observed Malicious SSL Cert (Coinhive URL Shortener)

- [x] ET COINMINER Random Hash Pascalcoin Miner Checkin
- [x] ET COINMINER Observed Suspicious SSL Cert (Minerpool - CoinMining)
- [x] ET COINMINER Win32/Ymacco.AA2F Checking (Multiple OS)
- [x] ET COINMINER Win32/Ymacco.AA2F Checking (Multiple OS)
- [x] ET COINMINER Observed DNS Query to herominers Domain (herominers .com)
- [x] ET COINMINER CoinMiner Domain in DNS Lookup (pool .hashvault .pro)
- [ ] ET COINMINER Panchan Mining Rig CnC Activity (Outbound)
- [x] ET COINMINER Observed DNS Query to Cryptocurrency Mining Pool Domain (xmr .2miners .com)
- [x] ET COINMINER Win32/Repl_it Coin Miner CnC Checkin
- [x] ET COINMINER Win32/Duino-Coin Miner CnC Checkin
- [x] ET COINMINER Observed DNS Query to Monero Miner Related Domain (monerohash .com)

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

- [x] ET COMPROMISED Known Compromised or Hostile Host Traffic group 1
- [x] ET COMPROMISED Known Compromised or Hostile Host Traffic group 2
- [x] ET COMPROMISED Known Compromised or Hostile Host Traffic group 3
- [x] ET COMPROMISED Known Compromised or Hostile Host Traffic group 4
- [x] ET COMPROMISED Known Compromised or Hostile Host Traffic group 5
- [x] ET COMPROMISED Known Compromised or Hostile Host Traffic group 6
- [x] ET COMPROMISED Known Compromised or Hostile Host Traffic group 7
- [x] ET COMPROMISED Known Compromised or Hostile Host Traffic group 8
- [x] ET COMPROMISED Known Compromised or Hostile Host Traffic group 9

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

- [ ] ET CURRENT_EVENTS SWF served from /tmp/
- [ ] ET CURRENT_EVENTS Download of Microsft Office File From Russian Content-Language Website
- [ ] ET CURRENT_EVENTS Download of Microsoft Office File From Chinese Content-Language Website
- [ ] ET CURRENT_EVENTS Download of PDF File From Russian Content-Language Website
- [ ] ET CURRENT_EVENTS Download of PDF File From Chinese Content-Language Website
- [ ] ET CURRENT_EVENTS WindowsLive Imposter Site WindowsLive.png
- [ ] ET CURRENT_EVENTS WindowsLive Imposter Site blt .png
- [ ] ET CURRENT_EVENTS WindowsLive Imposter Site Payload Download
- [ ] ET CURRENT_EVENTS Adobe Flash Unicode SWF File Embedded in Office File Caution - Could be Hostile
- [ ] ET CURRENT_EVENTS Lizamoon Related Compromised site served to local client
- [ ] ET CURRENT_EVENTS Potential Lizamoon Client Request /ur.php
- [ ] ET CURRENT_EVENTS Fake Shipping Invoice Request to JPG.exe Executable
- [ ] ET CURRENT_EVENTS Clickfraud Framework Request
- [ ] ET CURRENT_EVENTS Phoenix/Fiesta URI Requested Contains /? and hex
- [ ] ET CURRENT_EVENTS DNS Query for Known Hostile Domain (gooqlepics .com)
- [ ] ET CURRENT_EVENTS Adobe PDF Universal 3D file corrupted download 1
- [ ] ET CURRENT_EVENTS Adobe PDF Universal 3D file corrupted download 2
- [ ] ET CURRENT_EVENTS JavaScript Obfuscation JSXX Script
- [ ] ET CURRENT_EVENTS Obfuscated Content Using Dadongs JSXX 0.41 VIP Obfuscation Script
- [ ] ET CURRENT_EVENTS Italian Spam Campaign
- [ ] ET CURRENT_EVENTS JavaScript Determining OS MAC and Serving Java Archive File
- [ ] ET CURRENT_EVENTS Jembot PHP Webshell (hell.php)
- [ ] ET CURRENT_EVENTS FedEX Spam Inbound
- [ ] ET CURRENT_EVENTS UPS Spam Inbound
- [ ] ET CURRENT_EVENTS Post Express Spam Inbound
- [ ] ET CURRENT_EVENTS webshell used In timthumb attacks GIF98a 16129xX with PHP
- [ ] ET CURRENT_EVENTS RedKit - Jar File Naming Algorithm
- [ ] ET CURRENT_EVENTS NuclearPack - PDF Naming Algorithm
- [ ] ET CURRENT_EVENTS Unknown - Java Request .jar from dl.dropbox.com
- [ ] ET CURRENT_EVENTS Request to .in FakeAV Campaign June 19 2012 exe or zip
- [ ] ET CURRENT_EVENTS Runforestrun Malware Campaign Infected Website
- [ ] ET CURRENT_EVENTS JS.Runfore Malware Campaign Request
- [ ] ET CURRENT_EVENTS HeapLib JS Library
- [ ] ET CURRENT_EVENTS Googlebot UA POST to /uploadify.php
- [ ] ET CURRENT_EVENTS Scalaxy Jar file
- [ ] ET CURRENT_EVENTS Hacked Website Response /*km0ae9gr6m*/ Jun 25 2012
- [ ] ET CURRENT_EVENTS Hacked Website Response /*qhk6sa6g1c*/ Jun 25 2012
- [ ] ET CURRENT_EVENTS Incognito - Payload Request - /load.php by Java Client
- [ ] ET CURRENT_EVENTS g01pack - 32Char.php by Java Client
- [ ] ET CURRENT_EVENTS Unknown_s=1 - Payload Requested - 32AlphaNum?s=1 Java Request
- [ ] ET CURRENT_EVENTS RedKit PluginDetect Rename Saigon
- [ ] ET CURRENT_EVENTS FoxxySoftware - Comments
- [ ] ET CURRENT_EVENTS FoxxySoftware - Comments(2)
- [ ] ET CURRENT_EVENTS FoxxySoftware - Hit Counter Access
- [ ] ET CURRENT_EVENTS Possible Remote PHP Code Execution (php.pjpg)
- [ ] ET CURRENT_EVENTS SofosFO Jar file 10/17/12
- [ ] ET CURRENT_EVENTS Sophos PDF Standard Encryption Key Length Buffer Overflow
- [ ] ET CURRENT_EVENTS Sophos PDF Standard Encryption Key Length Buffer Overflow
- [ ] ET CURRENT_EVENTS SofosFO Jar file 09 Nov 12
- [ ] ET CURRENT_EVENTS SibHost Jar Request
- [ ] ET CURRENT_EVENTS Fake Google Chrome Update/Install
- [ ] ET CURRENT_EVENTS Possible SibHost PDF Request
- [ ] ET CURRENT_EVENTS CritXPack Jar Request (3)
- [ ] ET CURRENT_EVENTS RedDotv2 Jar March 18 2013

- [ ] ET CURRENT_EVENTS Winwebsec/Zbot/Luder Checkin Response
- [ ] ET CURRENT_EVENTS Possible Microsoft Office PNG overflow attempt invalid tEXt chunk length
- [ ] ET CURRENT_EVENTS CritX/SafePack/FlashPack URI Format June 17 2013 3
- [ ] ET CURRENT_EVENTS c0896 Hacked Site Response (Outbound) 1
- [ ] ET CURRENT_EVENTS c0896 Hacked Site Response (Outbound) 2
- [ ] ET CURRENT_EVENTS c0896 Hacked Site Response (Outbound) 3
- [ ] ET CURRENT_EVENTS c0896 Hacked Site Response Octal (Outbound)
- [ ] ET CURRENT_EVENTS c0896 Hacked Site Response (Outbound) 4
- [ ] ET CURRENT_EVENTS Fake FedEX/Pony spam campaign URI Struct 2
- [ ] ET CURRENT_EVENTS Fake Trojan Dropper purporting to be missing application - findloader
- [ ] ET CURRENT_EVENTS 0f2490 Hacked Site Response (Inbound)
- [ ] ET CURRENT_EVENTS 0f2490 Hacked Site Response (Outbound)
- [ ] ET CURRENT_EVENTS AutoIT C&C Check-In 2013-08-23 URL
- [ ] ET CURRENT_EVENTS Sakura Sep 10 2013
- [ ] ET CURRENT_EVENTS Possible J7u21 click2play bypass
- [ ] ET CURRENT_EVENTS DotkaChef Payload October 09
- [ ] ET CURRENT_EVENTS D-LINK Router Backdoor via Specific UA
- [ ] ET CURRENT_EVENTS Tenda Router Backdoor 1
- [ ] ET CURRENT_EVENTS Tenda Router Backdoor 2
- [ ] ET CURRENT_EVENTS 81a338 Hacked Site Response (Outbound)
- [ ] ET CURRENT_EVENTS 81a338 Hacked Site Response (Inbound)
- [ ] ET CURRENT_EVENTS FlashPack Oct 23 2013
- [ ] ET CURRENT_EVENTS Netgear WNDR4700 Auth Bypass
- [ ] ET CURRENT_EVENTS Netgear WNDR3700 Auth Bypass
- [ ] ET CURRENT_EVENTS Alpha Networks ADSL2/2+ router remote administration password disclosure
- [ ] ET CURRENT_EVENTS Host Domain .bit
- [ ] ET CURRENT_EVENTS Fredcot campaign IRC CnC
- [ ] ET CURRENT_EVENTS Possible WhiteLotus Java Payload
- [ ] ET CURRENT_EVENTS Possible WhiteLotus IE Payload
- [ ] ET CURRENT_EVENTS Fake Media Player malware binary requested
- [ ] ET CURRENT_EVENTS JJEncode Encoded Script Inside of PDF Likely Evil
- [ ] ET CURRENT_EVENTS Polling/Check-in/Compromise from fake DHL mailing campaign
- [ ] ET CURRENT_EVENTS Hostile fake DHL mailing campaign
- [ ] ET CURRENT_EVENTS Safe/CritX/FlashPack Payload
- [ ] ET CURRENT_EVENTS Possible Safe/CritX/FlashPack Edwards Packed PluginDetect
- [ ] ET CURRENT_EVENTS SofosFO/GrandSoft PDF
- [ ] ET CURRENT_EVENTS Current Asprox Spam Campaign
- [ ] ET CURRENT_EVENTS Current Asprox Spam Campaign 2
- [ ] ET CURRENT_EVENTS Possible FakeAV .exe.vbe HTTP Content-Disposition
- [ ] ET CURRENT_EVENTS CritX/SafePack/FlashPack SilverLight file as eot
- [ ] ET CURRENT_EVENTS Possible Safe/CritX/FlashPack Common Filename javadb.php
- [ ] ET CURRENT_EVENTS Possible Safe/CritX/FlashPack Common Filename javaim.php
- [ ] ET CURRENT_EVENTS Possible Safe/CritX/FlashPack Common Filename javarh.php
- [ ] ET CURRENT_EVENTS Dell Kace backdoor
- [ ] ET CURRENT_EVENTS EMET.DLL in jjencode
- [ ] ET CURRENT_EVENTS Hikvision DVR Synology Recon Scan Checkin
- [ ] ET CURRENT_EVENTS Possible Deep Panda WateringHole Related URI Struct
- [ ] ET CURRENT_EVENTS Win32.RBrute Scan (Outgoing)
- [ ] ET CURRENT_EVENTS Win32.RBrute Scan (incoming)
- [ ] ET CURRENT_EVENTS Win32.RBrute http server request
- [ ] ET CURRENT_EVENTS Win32.RBrute http response
- [ ] ET CURRENT_EVENTS Possible Inbound SNMP Router DoS (TTL 1)
- [ ] ET CURRENT_EVENTS Possible Inbound SNMP Router DoS (Disable Forwarding)
- [ ] ET CURRENT_EVENTS Likely Evil XMLDOM Detection of Local File
- [ ] ET CURRENT_EVENTS Possible ShellCode Passed as Argument to FlashVars
- [ ] ET CURRENT_EVENTS Safe/CritX/FlashPack Java Payload
- [ ] ET CURRENT_EVENTS Offensive Security EMET Bypass Observed in BleedingLife Variant Aug 26 2014
- [ ] ET CURRENT_EVENTS ScanBox Framework used in WateringHole Attacks
- [ ] ET CURRENT_EVENTS ScanBox Framework used in WateringHole Attacks (POST) PluginData
- [ ] ET CURRENT_EVENTS ScanBox Framework used in WateringHole Attacks KeepAlive
- [ ] ET CURRENT_EVENTS FAKEIE 11.0 Minimal Headers (flowbit set)
- [ ] ET CURRENT_EVENTS Possible TWiki RCE attempt
- [ ] ET CURRENT_EVENTS Possible TWiki Apache config file upload attempt
- [ ] ET CURRENT_EVENTS excessive fatal alerts (possible POODLE attack against client)
- [ ] ET CURRENT_EVENTS FlashPack Payload URI Struct Oct 16 2014
- [ ] ET CURRENT_EVENTS BlackEnergy URI Struct Oct 17 2014 BE1
- [ ] ET CURRENT_EVENTS BlackEnergy URI Struct Oct 17 2014 BE2
- [ ] ET CURRENT_EVENTS BlackEnergy URI Struct Oct 17 2014 BE3
- [ ] ET CURRENT_EVENTS BlackEnergy URI Struct Oct 17 2014 BE4
- [ ] ET CURRENT_EVENTS BlackEnergy URI Struct Oct 17 2014 BE5
- [ ] ET CURRENT_EVENTS FlashPack Payload URI Struct Oct 22 2014
- [ ] ET CURRENT_EVENTS SSL SinkHole Cert Possible Infected Host
- [ ] ET CURRENT_EVENTS Possible FlashPack (FlashOnly) Payload Struct Nov 19 2014
- [ ] ET CURRENT_EVENTS Magnitude Flash Payload
- [ ] ET CURRENT_EVENTS SoakSoak Malware GET request
- [ ] ET CURRENT_EVENTS DNS Query SoakSoak Malware (soaksoak .ru)
- [ ] ET CURRENT_EVENTS Unauthorized SSL Cert for Google Domains
- [ ] ET CURRENT_EVENTS Chrome Form Data Theft April 06 2015
- [ ] ET CURRENT_EVENTS Chrome Cookie Data Theft April 06 2015
- [ ] ET CURRENT_EVENTS IonCube Encoded Page (no alert)
- [ ] ET CURRENT_EVENTS Evil JS iframe Embedded In GIF
- [ ] ET CURRENT_EVENTS NullHole URI Struct Jul 22 2015 M3
- [ ] ET CURRENT_EVENTS Possible Locky Payload DL Sept 26 2017 M1
- [ ] ET CURRENT_EVENTS Possible Locky Payload DL Sept 26 2017 M2
- [ ] ET CURRENT_EVENTS CERTEGO Possible JScript Coming Over SMB v2
- [ ] ET CURRENT_EVENTS Possible Locky Payload DL Sept 26 2017 M3
- [ ] ET CURRENT_EVENTS Possible Locky Payload DL Sept 26 2017 M4
- [ ] ET CURRENT_EVENTS Python Eval Compile seen in HTTP Request Headers
- [ ] ET CURRENT_EVENTS Brushaloader Domain in DNS Lookup 2019-05-30
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle Original GET]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.DNS.BEACON.[CSBundle DNS]
- [x] ET CURRENT_EVENTS [Fireeye] HackTool.TCP.Rubeus.[nonce]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle NYTIMES Server]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle Original Server 3]
- [x] ET CURRENT_EVENTS [Fireeye] HackTool.UDP.Rubeus.[nonce]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.GORAT.[POST]

- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle USAToday Server]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle Original Server]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle Original Stager]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle MSOffice Server]
- [ ] ET CURRENT_EVENTS [Fireeye] Backdoor.DNS.BEACON.[CSBundle DNS]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle USAToday GET]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle MSOffice POST]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle NYTIMES POST]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[Yelp Request]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle Original Server 2]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle MSOffice Server]
- [x] ET CURRENT_EVENTS [Fireeye] HackTool.UDP.Rubeus.[nonce 2]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.GORAT.[Build ID]
- [x] ET CURRENT_EVENTS [Fireeye] M.HackTool.SMB.Impacket-Obfuscation.[Service Names] M1
- [x] ET CURRENT_EVENTS [Fireeye] M.HackTool.SMB.Impacket-Obfuscation.[Service Names] M3
- [x] ET CURRENT_EVENTS [Fireeye] M.HackTool.SMB.Impacket-Obfuscation.[Service Names] M5
- [x] ET CURRENT_EVENTS [Fireeye] M.HackTool.SMB.Impacket-Obfuscation.[Service Names] M7
- [x] ET CURRENT_EVENTS [Fireeye] M.HackTool.SMB.Impacket-Obfuscation.[Service Names] M9
- [x] ET CURRENT_EVENTS Possible Crypto Drainer Enumerate
- [x] ET CURRENT_EVENTS Sliver Related Domain in DNS Lookup
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (mamsolutions .us)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (newsforward .quest)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (mamsolution .us)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (a-techsolutions .us)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (newsagent .quest)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (mvpconsultant .us)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (everyavenuetravel .site)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (netsecurity-essential .com)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (foddylearn .com)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (glamorousfeeds .com)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (trendingonfeed .com)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (feedsonbudget .com)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (viralonspot .com)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (printertechnicahelp .com)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (globalnews .cloud)
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle USAToday Server]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle NYTIMES GET]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.GORAT.[SID1]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[Yelp GET]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle CDN GET]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle Original POST]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle Original Stager 2]
- [x] ET CURRENT_EVENTS [Fireeye] HackTool.TCP.Rubeus.[nonce 2]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle MSOffice GET]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle MSOffice POST]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.HTTP.BEACON.[CSBundle NYTIMES Server]
- [x] ET CURRENT_EVENTS [Fireeye] POSSIBLE HackTool.TCP.Rubeus.[User32LogonProcesss]
- [x] ET CURRENT_EVENTS [Fireeye] Backdoor.SSL.BEACON.[CSBundle Ajax]
- [x] ET CURRENT_EVENTS [Fireeye] M.HackTool.SMB.Impacket-Obfuscation.[Service Names] M2
- [x] ET CURRENT_EVENTS [Fireeye] M.HackTool.SMB.Impacket-Obfuscation.[Service Names] M4
- [x] ET CURRENT_EVENTS [Fireeye] M.HackTool.SMB.Impacket-Obfuscation.[Service Names] M6
- [x] ET CURRENT_EVENTS [Fireeye] M.HackTool.SMB.Impacket-Obfuscation.[Service Names] M8
- [x] ET CURRENT_EVENTS Possible Crypto Drainer Fetch
- [x] ET CURRENT_EVENTS Sliver Related Domain in DNS Lookup (saleforces-it .com)
- [x] ET CURRENT_EVENTS NATO Themed Maldoc Related Domain in DNS Lookup (am .my-zo .org)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (minielectronic .in)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (polussuo .com)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (antivirusphonenumber .org)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (puppyandcats .online)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (humaantouch .com)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (comsecurityessentials .support)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (hardwarecloseout .com)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (weeklylive .info)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (decfurnish .com)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (issat .us)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (aksconsulting .us)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (tissatweb .us)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (furnitureshopone .us)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (mainlytrendy .com)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (thespeedoflite .com)

- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (quickbooktechnicalsupport .org)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (financialtrending .com)
- [ ] ET CURRENT_EVENTS Observed DNS Query to Known Malvertising Domain (tissat .us)
- [x] ET CURRENT_EVENTS GitHub/CicleCI Themed Phishing Domain in DNS Lookup (circle-ci .com)
- [x] ET CURRENT_EVENTS GitHub/CicleCI Themed Phishing Domain in DNS Lookup (emails-circleci .com)
- [x] ET CURRENT_EVENTS GitHub/CicleCI Themed Phishing Domain in DNS Lookup (circle-cl .com)
- [x] ET CURRENT_EVENTS GitHub/CicleCI Themed Phishing Domain in DNS Lookup (email-circleci .com)
- [ ] ET CURRENT_EVENTS Observed Credit Card Scam Exfil Domain in DNS Lookup
- [ ] ET CURRENT_EVENTS Observed Credit Card Scam Exfil Domain (postasico .top in TLS SNI)
- [x] ET CURRENT_EVENTS Abused Domain Delivering Malicious Payloads in DNS Lookup (one-click .cc)
- [x] ET CURRENT_EVENTS Abused Domain Delivering Malicious Payloads in DNS Lookup (freeclickr .com)
- [ ] ET CURRENT_EVENTS Predator Spyware Infection Chain Related Domain in DNS Lookup (verifyurl .me)
- [ ] ET CURRENT_EVENTS Predator Spyware Infection Chain Related Domain (verifyurl .me in TLS SNI)
- [ ] ET CURRENT_EVENTS Predator Spyware Infection Chain Related Domain in DNS Lookup (sec-flare .com)
- [ ] ET CURRENT_EVENTS Observed Predator Spyware Infection Chain Related Domain Domain (sec-flare .com in TLS SNI)
- [ ] ET CURRENT_EVENTS Possible Atlassian Confluence CVE-2023-22515 Scan Activity
- [ ] ET CURRENT_EVENTS Possible Atlassian Confluence CVE-2023-22515 Scan Activity
- [ ] ET CURRENT_EVENTS Possible Atlassian Confluence CVE-2023-22515 Scan Activity - Clone

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

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

- [ ] ET DOS Cisco Router HTTP DoS
- [ ] ET DOS Cisco 514 UDP flood DoS
- [ ] ET DOS Catalyst memory leak attack
- [ ] ET DOS Possible Microsoft SQL Server Remote Denial Of Service Attempt
- [ ] ET DOS Excessive SMTP MAIL-FROM DDoS
- [ ] ET DOS ICMP Path MTU lowered below acceptable threshold
- [ ] ET DOS Microsoft Streaming Server Malformed Request
- [ ] ET DOS FreeBSD NFS RPC Kernel Panic
- [ ] ET DOS NetrWkstaUserEnum Request with large Preferred Max Len
- [ ] ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack
- [ ] ET DOS DNS BIND 9 Dynamic Update DoS attempt
- [ ] ET DOS Potential Inbound NTP denial-of-service attempt (repeated mode 7 request)
- [ ] ET DOS Potential Inbound NTP denial-of-service attempt (repeated mode 7 reply)
- [ ] ET DOS Possible MYSQL GeomFromWKB() function Denial Of Service Attempt
- [ ] ET DOS Possible MYSQL SELECT WHERE to User Variable Denial Of Service Attempt
- [ ] ET DOS Netgear DG632 Web Management Denial Of Service Attempt
- [ ] ET DOS Possible Cisco PIX/ASA Denial Of Service Attempt (Hping Created Packets)
- [ ] ET DOS Cisco 4200 Wireless Lan Controller Long Authorisation Denial of Service Attempt
- [ ] ET DOS IBM DB2 kuddb2 Remote Denial of Service Attempt
- [ ] ET DOS Possible Cisco ASA 5500 Series Adaptive Security Appliance Remote SIP Inspection Device Reload Denial of Service Attempt
- [ ] ET DOS ntop Basic-Auth DOS inbound
- [ ] ET DOS ntop Basic-Auth DOS outbound
- [ ] ET DOS Possible SolarWinds TFTP Server Read Request Denial Of Service Attempt
- [ ] ET DOS SolarWinds TFTP Server Long Write Request Denial Of Service Attempt
- [ ] ET DOS Possible VNC ClientCutText Message Denial of Service/ Memory Corruption Attempt
- [ ] ET DOS Possible MySQL ALTER DATABASE Denial Of Service Attempt
- [x] ET DOS User-Agent used in known DDoS Attacks Detected outbound
- [x] ET DOS User-Agent used in known DDoS Attacks Detected inbound
- [x] ET DOS User-Agent used in known DDoS Attacks Detected outbound 2
- [x] ET DOS User-Agent used in known DDoS Attacks Detected inbound 2
- [ ] ET DOS Outbound Low Orbit Ion Cannon LOIC Tool Internal User May Be Participating in DDOS
- [ ] ET DOS Inbound Low Orbit Ion Cannon LOIC DDOS Tool desu string
- [ ] ET DOS Outbound Low Orbit Ion Cannon LOIC Tool Internal User May Be Participating in DDOS desu string
- [ ] ET DOS IBM Tivoli Endpoint Buffer Overflow Attempt
- [ ] ET DOS Skype FindCountriesByNamePattern property Buffer Overflow Attempt
- [ ] ET DOS Skype FindCountriesByNamePattern property Buffer Overflow Attempt Format String Function Call
- [x] ET DOS LOIC Javascript DDoS Outbound
- [x] ET DOS High Orbit Ion Cannon (HOIC) Attack Inbound Generic Detection Double Spaced UA
- [ ] ET DOS Microsoft Remote Desktop (RDP) Syn then Reset 30 Second DoS Attempt
- [x] ET DOS Microsoft Remote Desktop (RDP) Syn/Ack Outbound Flowbit Set
- [ ] ET DOS Microsoft Remote Desktop (RDP) Session Established Flowbit Set
- [ ] ET DOS Microsoft Remote Desktop Protocol (RDP) maxChannelIds DoS Attempt Negative INT
- [ ] ET DOS Microsoft Remote Desktop Protocol (RDP) maxChannelIds DoS Attempt
- [ ] ET DOS Microsoft Remote Desktop Protocol (RDP) maxChannelIds Integer indef DoS Attempt
- [ ] ET DOS Microsoft Remote Desktop Protocol (RDP) maxChannelIds Negative Integer indef DoS Attempt
- [ ] ET DOS Microsoft Windows 7 ICMPv6 Router Advertisement Flood
- [x] ET DOS DNS Amplification Attack Inbound
- [ ] ET DOS DNS Amplification Attack Outbound
- [x] ET DOS LOIC POST
- [x] ET DOS LOIC GET
- [ ] ET DOS LibuPnP CVE-2012-5958 ST DeviceType Buffer Overflow
- [ ] ET DOS LibuPnP ST UDN Buffer Overflow (CVE-2012-5963)
- [ ] ET DOS LibuPnP CVE-2012-5964 ST URN ServiceType Buffer Overflow
- [ ] ET DOS LibuPnP CVE-2012-5965 ST URN DeviceType Buffer Overflow
- [ ] ET DOS LibuPnP CVE-2012-5961 ST UDN Buffer Overflow
- [ ] ET DOS Miniupnpd M-SEARCH Buffer Overflow (CVE-2013-0229)
- [ ] ET DOS Miniupnpd SoapAction MethodName Buffer Overflow (CVE-2013-0230)
- [ ] ET DOS Squid-3.3.5 DoS

- [x] ET DOS Trojan.BlackRev V1.Botnet HTTP Login POST Flood Traffic Inbound
- [x] ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x02
- [x] ET DOS Possible NTP DDoS Multiple MON_LIST Seq 0 Response Spanning Multiple Packets IMPL 0x02
- [x] ET DOS Possible NTP DDoS Multiple MON_LIST Seq 0 Response Spanning Multiple Packets IMPL 0x03
- [x] ET DOS Likely NTP DDoS In Progress MON_LIST Response to Non-Ephemeral Port IMPL 0x02
- [x] ET DOS Likely NTP DDoS In Progress MON_LIST Response to Non-Ephemeral Port IMPL 0x03
- [x] ET DOS Inbound GoldenEye DoS attack
- [x] ET DOS Possible WordPress Pingback DDoS in Progress (Inbound)
- [x] ET DOS HOIC with booster outbound
- [x] ET DOS HOIC with booster inbound
- [x] ET DOS Likely NTP DDoS In Progress PEER_LIST Response to Non-Ephemeral Port IMPL 0x02
- [x] ET DOS Likely NTP DDoS In Progress PEER_LIST Response to Non-Ephemeral Port IMPL 0x03
- [x] ET DOS Likely NTP DDoS In Progress PEER_LIST_SUM Response to Non-Ephemeral Port IMPL 0x02
- [x] ET DOS Likely NTP DDoS In Progress PEER_LIST_SUM Response to Non-Ephemeral Port IMPL 0x03
- [x] ET DOS Likely NTP DDoS In Progress GET_RESTRICT Response to Non-Ephemeral Port IMPL 0x03
- [x] ET DOS Likely NTP DDoS In Progress GET_RESTRICT Response to Non-Ephemeral Port IMPL 0x02
- [x] ET DOS Possible NTP DDoS Inbound Frequent Un-Authed PEER_LIST Requests IMPL 0x03
- [x] ET DOS Possible NTP DDoS Inbound Frequent Un-Authed PEER_LIST Requests IMPL 0x02
- [x] ET DOS Possible NTP DDoS Inbound Frequent Un-Authed PEER_LIST_SUM Requests IMPL 0x03
- [x] ET DOS Possible NTP DDoS Inbound Frequent Un-Authed PEER_LIST_SUM Requests IMPL 0x02
- [x] ET DOS Possible NTP DDoS Inbound Frequent Un-Authed GET_RESTRICT Requests IMPL 0x03
- [x] ET DOS Possible NTP DDoS Inbound Frequent Un-Authed GET_RESTRICT Requests IMPL 0x02
- [x] ET DOS Likely NTP DDoS In Progress Multiple UNSETTRAP Mode 6 Responses
- [x] ET DOS Possible SSDP Amplification Scan in Progress
- [x] ET DOS Terse HTTP GET Likely LOIC
- [x] ET DOS HTTP GET AAAAAAAA Likely FireFlood
- [x] ET DOS Terse HTTP GET Likely AnonMafiaIC DDoS tool
- [x] ET DOS Terse HTTP GET Likely AnonGhost DDoS tool
- [x] ET DOS Terse HTTP GET Likely GoodBye 5.2 DDoS tool
- [ ] ET DOS Potential Tsunami SYN Flood Denial Of Service Attempt
- [x] ET DOS MC-SQLR Response Outbound Possible DDoS Participation
- [x] ET DOS MC-SQLR Response Inbound Possible DDoS Target
- [x] ET DOS Bittorrent User-Agent inbound - possible DDOS
- [x] ET DOS Possible Sentinal LM Application attack in progress Outbound (Response)
- [x] ET DOS Possible Sentinal LM Amplification attack (Response) Inbound
- [x] ET DOS Possible Sentinal LM Amplification attack (Request) Inbound
- [x] ET DOS Linux/Tsunami DOS User-Agent (x00_-gawa.sa.pilipinas.2015) INBOUND
- [x] ET DOS DNS Amplification Attack Possible Inbound Windows Non-Recursive Root Hint Reserved Port
- [x] ET DOS DNS Amplification Attack Possible Outbound Windows Non-Recursive Root Hint Reserved Port
- [x] ET DOS Microsoft Windows LSASS Remote Memory Corruption (CVE-2017-0004)
- [x] ET DOS Excessive Large Tree Connect Response
- [x] ET DOS SMB Tree_Connect Stack Overflow Attempt (CVE-2017-0016)
- [ ] ET DOS Possible SMBLoris NBSS Length Mem Exhaustion Vuln Inbound
- [x] ET DOS SMBLoris NBSS Length Mem Exhaustion Attempt (PoC Based)
- [x] ET DOS CLDAP Amplification Reflection (PoC based)
- [x] ET DOS Potential CLDAP Amplification Reflection
- [x] ET DOS Possible Memcached DDoS Amplification Query (set)
- [x] ET DOS Possible Memcached DDoS Amplification Response Outbound
- [x] ET DOS Possible Memcached DDoS Amplification Inbound
- [x] ET DOS CallStranger - Attempted UPnP Reflected Amplified TCP with Multiple Callbacks (CVE-2020-12695)
- [x] ET DOS Possible Microsoft Windows HTTP2 Reset Flood Denial of Service Inbound (CVE-2019-9514)
- [ ] ET DOS Possible Apache Traffic Server HTTP2 Settings Flood Denial of Service Inbound (CVE-2019-9515)
- [ ] ET DOS Possible Apache Traffic Server HTTP2 Settings Flood Error Response (CVE-2019-9515)
- [ ] GPL DOS Jolt attack
- [ ] GPL DOS IGMP dos attack

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

- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 1
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 2
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 3
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 4
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 5
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 6
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 7
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 8
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 9
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 10
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 11
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 12
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 13
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 14
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 15
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 16
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 17
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 18
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 19
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 20
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 21
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 22
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 23
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 24
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 25
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 26
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 27
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 28
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 29
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 30
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 31
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 32
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 33
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 34
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 35
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 36
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 37
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 38
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 39
- [x] ET DROP Spamhaus DROP Listed Traffic Inbound group 40

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

- [x] ET DROP Dshield Block Listed Source group 1
- [x] **emerging-exploit.rules** Hide
  - [ ] ET EXPLOIT Cisco Telnet Buffer Overflow
  - [ ] ET EXPLOIT Catalyst SSH protocol mismatch
  - [ ] ET EXPLOIT CVS server heap overflow attempt (target BSD)
  - [ ] ET EXPLOIT CVS server heap overflow attempt (target Linux)
  - [ ] ET EXPLOIT CVS server heap overflow attempt (target Solaris)
  - [ ] ET EXPLOIT Squid NTLM Auth Overflow Exploit
  - [ ] ET EXPLOIT MS-SQL SQL Injection running SQL statements line comment
  - [ ] ET EXPLOIT MS-SQL SQL Injection line comment
  - [ ] ET EXPLOIT MS-SQL heap overflow attempt
  - [ ] ET EXPLOIT MS-SQL DOS attempt (08)
  - [ ] ET EXPLOIT MS-SQL DOS attempt (08) 1 byte
  - [ ] ET EXPLOIT MS-SQL Spike buffer overflow
  - [x] ET EXPLOIT MS-SQL SQL Injection closing string plus line comment
  - [x] ET EXPLOIT Pwdump3e Password Hash Retrieval port 445
  - [x] ET EXPLOIT Pwdump3e pwservice.exe Access port 445
  - [x] ET EXPLOIT Pwdump3e Session Established Reg-Entry port 139
  - [x] ET EXPLOIT Pwdump3e Session Established Reg-Entry port 445
  - [x] ET EXPLOIT Pwdump3e pwservice.exe Access port 139
  - [x] ET EXPLOIT Pwdump3e Password Hash Retrieval port 139
  - [ ] ET EXPLOIT Invalid non-fragmented packet with fragment offset>0
  - [ ] ET EXPLOIT Invalid fragment - ACK reset
  - [ ] ET EXPLOIT Invalid fragment - illegal flags
  - [x] ET EXPLOIT NTDump Session Established Reg-Entry port 139
  - [x] ET EXPLOIT NTDump.exe Service Started port 139
  - [ ] ET EXPLOIT libpng tRNS overflow attempt
  - [ ] ET EXPLOIT libPNG - Width exceeds limit
  - [x] ET EXPLOIT libPNG - Possible integer overflow in allocation in png_handle_sPLT
  - [ ] ET EXPLOIT Adobe Acrobat Reader Malicious URL Null Byte
  - [ ] ET EXPLOIT Possible MS04-032 Windows Metafile (.emf) Heap Overflow Portbind Attempt
  - [ ] ET EXPLOIT MS04-032 Windows Metafile (.emf) Heap Overflow Connectback Attempt
  - [ ] ET EXPLOIT MS04-032 Windows Metafile (.emf) Heap Overflow Exploit
  - [ ] ET EXPLOIT MS04-032 Bad EMF file
  - [ ] ET EXPLOIT Possible ShixxNote buffer-overflow + remote shell attempt
  - [x] ET EXPLOIT NTDump Session Established Reg-Entry port 445
  - [x] ET EXPLOIT NTDump.exe Service Started port 445
  - [x] ET EXPLOIT Exploit MS05-002 Malformed .ANI stack overflow attack
  - [ ] ET EXPLOIT Arkeia full remote access without password or authentication
  - [x] ET EXPLOIT Pwdump4 Session Established GetHash port 139
  - [x] ET EXPLOIT Pwdump4 Session Established GetHash port 445
  - [ ] ET EXPLOIT Solaris TTYPROMPT environment variable set
  - [ ] ET EXPLOIT MS05-021 Exchange Link State - Possible Attack (1)
  - [ ] ET EXPLOIT MS05-021 Exchange Link State - Possible Attack (2)
  - [ ] ET EXPLOIT MS Exchange Link State Routing Chunk (maybe MS05-021)
  - [ ] ET EXPLOIT TCP Reset from MS Exchange after chunked data, probably crashed it (MS05-021)
  - [ ] ET EXPLOIT MySQL MaxDB Buffer Overflow
  - [ ] ET EXPLOIT JamMail Jammail.pl Remote Command Execution Attempt
  - [ ] ET EXPLOIT Possible BackupExec Metasploit Exploit (inbound)
  - [ ] ET EXPLOIT Possible BackupExec Metasploit Exploit (outbound)
  - [ ] ET EXPLOIT Veritas backupexec_agent exploit
  - [ ] ET EXPLOIT NDMP Notify Connect - Possible Backup Exec Remote Agent Recon
  - [ ] ET EXPLOIT Backup Exec Windows Agent Remote File Access - Attempt
  - [ ] ET EXPLOIT Backup Exec Windows Agent Remote File Access - Vulnerable
  - [ ] ET EXPLOIT Incoming Electronic Mail for UNIX Expires Header Buffer Overflow Exploit
  - [ ] ET EXPLOIT Outgoing Electronic Mail for UNIX Expires Header Buffer Overflow Exploit
  - [ ] ET EXPLOIT TAC Attack Directory Traversal
  - [ ] ET EXPLOIT malformed Sack - Snort DoS-by-umid
  - [ ] ET EXPLOIT WMF Exploit
  - [ ] ET EXPLOIT Java runtime.exec() call
  - [ ] ET EXPLOIT Java private function call sun.misc.unsafe
  - [ ] ET EXPLOIT BMP with invalid bfOffBits
  - [ ] ET EXPLOIT MSSQL Hello Overflow Attempt
  - [ ] ET EXPLOIT HP-UX Printer LPD Command Insertion
  - [ ] ET EXPLOIT SYS get_domain_index_metadata Privilege Escalation Attempt
  - [ ] ET EXPLOIT SYS get_domain_index_tables Access
  - [ ] ET EXPLOIT SYS get_v2_domain_index_tables Privilege Escalation Attempt
  - [ ] ET EXPLOIT Symantec Scan Engine Request Password Hash
  - [ ] ET EXPLOIT VNC Possible Vulnerable Server Response
  - [ ] ET EXPLOIT VNC Client response
  - [ ] ET EXPLOIT VNC Server VNC Auth Offer
  - [ ] ET EXPLOIT VNC Authentication Reply
  - [ ] ET EXPLOIT RealVNC Authentication Bypass Attempt
  - [ ] ET EXPLOIT RealVNC Server Authentication Bypass Successful
  - [ ] ET EXPLOIT VNC Server VNC Auth Offer - No Challenge string
  - [ ] ET EXPLOIT VNC Good Authentication Reply
  - [ ] ET EXPLOIT VNC Multiple Authentication Failures
  - [ ] ET EXPLOIT VNC Server Not Requiring Authentication (case 2)
  - [ ] ET EXPLOIT VNC Server Not Requiring Authentication
  - [ ] ET EXPLOIT UPnP DLink M-Search Overflow Attempt
  - [ ] ET EXPLOIT DOS Microsoft Windows SRV.SYS MAILSLOT
  - [ ] ET EXPLOIT Linksys WRT54g Authentication Bypass Attempt
  - [ ] ET EXPLOIT Novell HttpStk Remote Code Execution Attempt /nds
  - [ ] ET EXPLOIT Novell HttpStk Remote Code Execution Attempt /dhost
  - [ ] ET EXPLOIT Novell HttpStk Remote Code Execution Attempt /dhost (linewrap)
  - [ ] ET EXPLOIT Novell HttpStk Remote Code Execution Attempt /nds (linewrap)
  - [ ] ET EXPLOIT FTP .message file write
  - [ ] ET EXPLOIT ProFTPD .message file overflow attempt
  - [ ] ET EXPLOIT TFTP Invalid Mode in file Get
  - [ ] ET EXPLOIT TFTP Invalid Mode in file Put
  - [ ] ET EXPLOIT Symantec Remote Management RTVScan Exploit
  - [ ] ET EXPLOIT GuppY error.php POST Arbitrary Remote Code Execution
  - [ ] ET EXPLOIT CA BrightStor ARCserve Mobile Backup LGSERVER.EXE Heap Corruption
  - [ ] ET EXPLOIT Computer Associates Brightstor ARCServer Backup RPC Server (Catirpc.dll) DoS
  - [ ] ET EXPLOIT Computer Associates Mobile Backup Service LGSERVER.EXE Stack Overflow
  - [ ] ET EXPLOIT Computer Associates BrightStor ARCserve Backup for Laptops LGServer.exe DoS
  - [ ] ET EXPLOIT US-ASCII Obfuscated script
  - [ ] ET EXPLOIT US-ASCII Obfuscated VBScript download file
  - [ ] ET EXPLOIT US-ASCII Obfuscated VBScript execute command
  - [ ] ET EXPLOIT US-ASCII Obfuscated VBScript
  - [ ] ET EXPLOIT Solaris telnet USER environment vuln Attack inbound
  - [ ] ET EXPLOIT Solaris telnet USER environment vuln Attack outbound

- [ ] ET EXPLOIT Trend Micro Web Interface Auth Bypass Vulnerable Cookie Attempt
- [ ] ET EXPLOIT CA Brightstor ARCServe caloggerd DoS
- [ ] ET EXPLOIT TrendMicro ServerProtect Exploit possible worma(little-endian DCERPC Request)
- [ ] ET EXPLOIT Now SMS/MMS Gateway SMPP BOF Vulnerability
- [ ] ET EXPLOIT ExtremeZ-IP File and Print Server Multiple Vulnerabilities - tcp
- [ ] ET EXPLOIT Zilab Chat and Instant Messaging User Info BoF Vulnerability
- [ ] ET EXPLOIT MDAEMON (Post Auth) Remote Root IMAP FETCH Command Universal Exploit
- [x] ET EXPLOIT PWDump4 Password dumping exe copied to victim
- [ ] ET EXPLOIT Foofus.net Password dumping dll injection
- [x] ET EXPLOIT SQL sp_configure attempt
- [ ] ET EXPLOIT GuildFTPd CWD and LIST Command Heap Overflow - POC-2
- [ ] ET EXPLOIT Possible IIS FTP Exploit attempt - Large SITE command
- [ ] ET EXPLOIT Siemens Gigaset SE361 WLAN Data Flood Denial of Service Vulnerability
- [ ] ET EXPLOIT xp_fileexist access
- [x] ET EXPLOIT xp_readerrorlogs access
- [x] ET EXPLOIT Possible Oracle Database Text Component ctxsys.drvxtabc.create_tables Remote SQL Injection Attempt
- [ ] ET EXPLOIT Xerox WorkCentre PJL Daemon Buffer Overflow Attempt
- [ ] ET EXPLOIT Possible SpamAssassin Milter Plugin Remote Arbitrary Command Injection Attempt
- [ ] ET EXPLOIT Possible Sendmail SpamAssassin Milter Plugin Remote Arbitrary Command Injection Attempt
- [ ] ET EXPLOIT M3U File Request Flowbit Set
- [ ] ET EXPLOIT HP OpenView Network Node Manager OvJavaLocale Cookie Value Buffer Overflow Attempt
- [ ] ET EXPLOIT Possible Etrust Secure Transaction Platform Identification and Entitlements Server File Disclosure Attempt
- [ ] ET EXPLOIT Neosploit Exploit Pack Activity Observed
- [ ] ET EXPLOIT Driveby Bredolab - client exploited by acrobat
- [ ] ET EXPLOIT JAR served from /tmp/ could be Phoenix Exploit Kit
- [ ] ET EXPLOIT JDownloader Webinterface Source Code Disclosure
- [ ] ET EXPLOIT HP LaserJet PLJ Interface Directory Traversal
- [ ] ET EXPLOIT Oracle Virtual Server Agent Command Injection Attempt
- [ ] ET EXPLOIT Wireshark ENTTEC DMX Data Processing Code Execution Attempt 1
- [ ] ET EXPLOIT Microsoft Windows Common Control Library Heap Buffer Overflow
- [ ] ET EXPLOIT Unknown Exploit Pack URL Detected
- [ ] ET EXPLOIT RetroGuard Obfuscated JAR likely part of hostile exploit kit
- [ ] ET EXPLOIT Java Exploit io.exe download served
- [ ] ET EXPLOIT Java Exploit Attempt Request for .id from octal host
- [ ] ET EXPLOIT HP OpenView NNM snmpviewer.exe CGI Stack Buffer Overflow 1
- [ ] ET EXPLOIT Unknown Exploit Pack Binary Load Request
- [ ] ET EXPLOIT Java Exploit Attempt applet via file URI param
- [ ] ET EXPLOIT Possible CVE-2011-2110 Flash Exploit Attempt
- [ ] ET EXPLOIT Possible CVE-2011-2110 Flash Exploit Attempt Embedded in Web Page
- [ ] ET EXPLOIT 2Wire Password Reset Vulnerability via POST
- [ ] ET EXPLOIT VSFTPD Backdoor User Login Smiley
- [ ] ET EXPLOIT Phoenix Java MIDI Exploit Received By Vulnerable Client
- [ ] ET EXPLOIT Computer Associates Brightstor ARCServe Backup Mediasvr.exe Remote Exploit
- [ ] ET EXPLOIT CA Brightstor ARCServe Mediasvr DoS
- [ ] ET EXPLOIT Now SMS/MMS Gateway HTTP BOF Vulnerability
- [ ] ET EXPLOIT ExtremeZ-IP File and Print Server Multiple Vulnerabilities - udp
- [ ] ET EXPLOIT Zilab Chat and Instant Messaging Heap Overflow Vulnerability
- [ ] ET EXPLOIT Borland VisiBroker Smart Agent Heap Overflow
- [ ] ET EXPLOIT SecurityGateway 1.0.1 Remote Buffer Overflow
- [x] ET EXPLOIT Pwdump6 Session Established test file created on victim
- [x] ET EXPLOIT SQL sp_configure - configuration change
- [ ] ET EXPLOIT GuildFTPd CWD and LIST Command Heap Overflow - POC-1
- [ ] ET EXPLOIT VLC web interface buffer overflow attempt
- [ ] ET EXPLOIT IIS FTP Exploit - NLST Globbing Exploit
- [ ] ET EXPLOIT xp_servicecontrol access
- [x] ET EXPLOIT xp_enumerrorlogs access
- [x] ET EXPLOIT xp_enumdsn access
- [ ] ET EXPLOIT HP Open View Data Protector Buffer Overflow Attempt
- [ ] ET EXPLOIT GsecDump executed
- [ ] ET EXPLOIT Possible Foxit PDF Reader Authentication Bypass Attempt
- [ ] ET EXPLOIT Possible Novell Groupwise Internet Agent CREATE Verb Stack Overflow Attempt
- [ ] ET EXPLOIT Possible VLC Media Player M3U File FTP URL Processing Stack Buffer Overflow Attempt
- [ ] ET EXPLOIT Possible Microsoft Office Word 2007 sprmCMajority Buffer Overflow Attempt
- [ ] ET EXPLOIT Successful Etrust Secure Transaction Platform Identification and Entitlements Server File Disclosure Attempt
- [x] ET EXPLOIT Linksys WAP54G debug.cgi Shell Access as Gemtek
- [ ] ET EXPLOIT PDF served from /tmp/ could be Phoenix Exploit Kit
- [ ] ET EXPLOIT VMware Tools Update OS Command Injection Attempt
- [ ] ET EXPLOIT VMware 2 Web Server Directory Traversal
- [ ] ET EXPLOIT Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference (CVE-2009-3103)
- [ ] ET EXPLOIT D-Link bsc_wlan.php Security Bypass
- [ ] ET EXPLOIT Wireshark ENTTEC DMX Data Processing Code Execution Attempt 2
- [x] ET EXPLOIT Lexmark Printer RDYMSG Cross Site Scripting Attempt
- [ ] ET EXPLOIT Compressed Adobe Flash File Embedded in XLS FILE Caution - Could be Exploit
- [ ] ET EXPLOIT Phoenix Java Exploit Attempt Request for .class from octal host
- [ ] ET EXPLOIT Adobe Flash SWF File Embedded in XLS FILE Caution - Could be Exploit
- [ ] ET EXPLOIT Java Exploit Attempt Request for hostile binary
- [ ] ET EXPLOIT HP OpenView NNM snmpviewer.exe CGI Stack Buffer Overflow 2
- [ ] ET EXPLOIT RXS-3211 IP Camera Password Information Disclosure Attempt
- [ ] ET EXPLOIT Eleonore Exploit Pack exemple.com Request
- [ ] ET EXPLOIT Java Exploit Attempt applet via file URI setAttribute
- [ ] ET EXPLOIT 2Wire Password Reset Vulnerability via GET
- [ ] ET EXPLOIT FreeBSD OpenSSH 3.5p1 possible vulnerable server
- [ ] ET EXPLOIT HP OpenView Network Node Manager Toolbar.exe CGI Buffer Overflow Attempt
- [ ] ET EXPLOIT Phoenix Java MIDI Exploit Received

- [ ] ET EXPLOIT Likely Generic Java Exploit Attempt Request for Java to decimal host
- [ ] ET EXPLOIT Possible BSNL Router DNS Change Attempt
- [ ] ET EXPLOIT Dadong Java Exploit Requested
- [ ] ET EXPLOIT Java Rhino Exploit Attempt - evilcode.class
- [ ] ET EXPLOIT RuggedCom Banner with MAC (SET)
- [x] ET EXPLOIT php with eval/gzinflate/base64_decode possible webshell
- [ ] ET EXPLOIT Base64 - Java Exploit Requested - /1Digit
- [ ] ET EXPLOIT Unknown - Java Exploit Requested - 13-14Alpha.jar
- [ ] ET EXPLOIT Potential RoaringBeast ProFTPd Exploit Specific config files upload
- [ ] ET EXPLOIT Potential RoaringBeast ProFTPd Exploit Specific (CHMOD 777)
- [x] ET EXPLOIT Access To mm-forms-community upload dir (Outbound)
- [ ] ET EXPLOIT Scalaxy Java Exploit 10/11/12
- [ ] ET EXPLOIT MySQL Stack based buffer overrun Exploit Specific
- [ ] ET EXPLOIT MySQL (Linux) Database Privilege Elevation (Exploit Specific)
- [x] ET EXPLOIT MySQL Server for Windows Remote SYSTEM Level Exploit (Stuxnet Technique)
- [x] ET EXPLOIT Metasploit -Java Atomic Exploit Downloaded
- [ ] ET EXPLOIT Metasploit CVE-2012-4792 EIP in URI IE 8
- [ ] ET EXPLOIT Possible Internet Explorer Use-After-Free Inbound (CVE-2012-4792)
- [ ] ET EXPLOIT Possible CVE-2013-0156 Ruby On Rails XML POST to Disallowed Type SYMBOL
- [x] ET EXPLOIT Adobe PDF Zero Day Trojan.666 Payload libarhlp32.dll Second Stage Download POST
- [ ] ET EXPLOIT Successful Compromise svchost.jpg Beacon - Java Zeroday
- [x] ET EXPLOIT Metasploit mstime_malloc no-spray
- [x] ET EXPLOIT Apache Struts Possible OGNL Java Exec In URI
- [x] ET EXPLOIT Apache Struts Possible OGNL AllowStaticMethodAccess in URI
- [x] ET EXPLOIT Apache Struts Possible OGNL Java WriteFile in client_body
- [x] ET EXPLOIT Possible 2012-1533 altjvm RCE via JNLP command injection
- [x] ET EXPLOIT SolusVM 1.13.03 SQL injection
- [ ] ET EXPLOIT SolusVM WHMCS CURL Multi-part Boundary Issue
- [ ] ET EXPLOIT Potential Internet Explorer Use After Free CVE-2013-3163 Exploit URI Struct 1
- [x] ET EXPLOIT Apache Struts Possible OGNL Java ProcessBuilder in client body
- [x] ET EXPLOIT Wscript Shell Run Attempt - Likely Hostile
- [ ] ET EXPLOIT Possible MHTML CVE-2012-0158 Vulnerable CLSID+b64 Office Doc Magic 2
- [ ] ET EXPLOIT Sakura - Java Exploit Recieved - Atomic
- [ ] ET EXPLOIT Possible Java CVE-2013-1488 java.sql.Drivers Service Object in JAR
- [ ] ET EXPLOIT Fredcot campaign php5-cgi initial exploit
- [ ] ET EXPLOIT Microsoft Outlook/Crypto API X.509 oid id-pe-authorityInfoAccessSyntax design bug allow blind HTTP requests attempt
- [x] ET EXPLOIT Zollard PHP Exploit UA
- [x] ET EXPLOIT Zollard PHP Exploit Telnet Outbound
- [x] ET EXPLOIT Zollard PHP Exploit UA Outbound
- [x] ET EXPLOIT Metasploit Plugin-Detect Posting Data 2
- [x] ET EXPLOIT Metasploit 2013-3346
- [x] ET EXPLOIT MMCS service (Big Endian)
- [ ] ET EXPLOIT Hostile _dsgweed.class JAR exploit
- [ ] ET EXPLOIT Crimepack Java exploit attempt(2)
- [ ] ET EXPLOIT Obfuscated Base64 in Javascript probably Scalaxy exploit kit
- [ ] ET EXPLOIT Microsoft RDP Server targetParams Exploit Attempt
- [ ] ET EXPLOIT Java Atomic Reference Exploit Attempt Metasploit Specific (CVE-2012-0507)
- [ ] ET EXPLOIT RuggedCom factory account backdoor
- [ ] ET EXPLOIT RedKit - Java Exploit Requested - 5 digit jar
- [ ] ET EXPLOIT Generic - PDF with NEW PDF EXPLOIT
- [ ] ET EXPLOIT Incognito - Java Exploit Requested - /gotit.php by Java Client
- [ ] ET EXPLOIT Potential RoaringBeast ProFTPd Exploit nsswitch.conf Upload
- [x] ET EXPLOIT Possible Metasploit Java Exploit
- [x] ET EXPLOIT Access To mm-forms-community upload dir (Inbound)
- [ ] ET EXPLOIT Java Exploit Campaign SetAttribute Java Applet
- [ ] ET EXPLOIT MySQL Heap based buffer overrun Exploit Specific
- [x] ET EXPLOIT MySQL Server for Windows Remote SYSTEM Level Exploit (Stuxnet Techique DUMP INTO executable)
- [ ] ET EXPLOIT Embedded Open Type Font file .eot seeing at Cool Exploit Kit
- [ ] ET EXPLOIT Escaped Unicode Char in Location CVE-2012-4792 EIP (Exploit Specific replace)
- [ ] ET EXPLOIT EIP in URI M1 (CVE-2012-4792)
- [ ] ET EXPLOIT Possible CVE-2013-0156 Ruby On Rails XML POST to Disallowed Type YAML
- [ ] ET EXPLOIT Metasploit Landing Page (CVE-2013-0422)
- [x] ET EXPLOIT Adobe PDF Zero Day Trojan.666 Payload libarext32.dll Second Stage Download POST
- [x] ET EXPLOIT Metasploit js_property_spray sprayHeap
- [x] ET EXPLOIT Exim/Dovecot Possible MAIL FROM Command Execution
- [x] ET EXPLOIT Apache Struts Possible OGNL AllowStaticMethodAccess in client body
- [x] ET EXPLOIT Apache Struts Possible OGNL Java Exec in client body
- [x] ET EXPLOIT Apache Struts Possible OGNL Java WriteFile in URI
- [ ] ET EXPLOIT Javadoc API Redirect CVE-2013-1571
- [x] ET EXPLOIT SolusVM 1.13.03 Access to solusvmc-node setuid bin
- [x] ET EXPLOIT IPMI Cipher 0 Authentication mode set
- [x] ET EXPLOIT Apache Struts Possible OGNL Java ProcessBuilder URI
- [ ] ET EXPLOIT DRIVEBY Rawin - Java Exploit -dubspace.jar
- [ ] ET EXPLOIT Possible MHTML CVE-2012-0158 Vulnerable CLSID+b64 Office Doc Magic 1
- [ ] ET EXPLOIT Possible MHTML CVE-2012-0158 Vulnerable CLSID+b64 Office Doc Magic 3
- [ ] ET EXPLOIT Metasploit Exploit Specific Function Naming
- [ ] ET EXPLOIT Possible Metasploit Java CVE-2013-2465 Class Name Sub Algo
- [ ] ET EXPLOIT Possible CVE-2013-3906 CnC Checkin
- [x] ET EXPLOIT JavaX Toolkit Posting Plugin-Detect Data
- [x] ET EXPLOIT Zollard PHP Exploit Telnet Inbound
- [x] ET EXPLOIT Metasploit Browser Exploit Server Plugin Detect
- [x] ET EXPLOIT Metasploit Plugin-Detect Posting Data 1
- [x] ET EXPLOIT Metasploit Plugin-Detect Posting Data 3
- [x] ET EXPLOIT MMCS service (Little Endian)
- [x] ET EXPLOIT Netgear passwordrecovered.cgi attempt
- [x] ET EXPLOIT Linksys Auth Bypass fw_sys_up.cgi

- [x] ET EXPLOIT Linksys Auth Bypass override.cgi
- [x] ET EXPLOIT Linksys Auth Bypass switch_boot.cgi
- [x] ET EXPLOIT Possible ZyXELs ZynOS Configuration Download Attempt (Contains Passwords)
- [x] ET EXPLOIT Joomla 3.2.1 SQL injection attempt
- [ ] ET EXPLOIT Possible CVE-2014-1761 Inbound SMTP 2
- [ ] ET EXPLOIT Possible CVE-2014-1761 Inbound SMTP 4
- [ ] ET EXPLOIT Possible CVE-2014-1761 Inbound SMTP 6
- [x] ET EXPLOIT Malformed HeartBeat Request
- [x] ET EXPLOIT Malformed HeartBeat Request method 2
- [x] ET EXPLOIT TLS HeartBeat Request (Client Initiated) fb set
- [x] ET EXPLOIT Possible OpenSSL HeartBleed Large HeartBeat Response (Server Init Vuln Client)
- [x] ET EXPLOIT Possible OpenSSL HeartBleed Large HeartBeat Response from Common SSL Port (Outbound from Client)
- [x] ET EXPLOIT Possible TLS HeartBleed Unencrypted Request Method 3 (Inbound to Common SSL Port)
- [ ] ET EXPLOIT Fiesta Flash Exploit Download
- [x] ET EXPLOIT Metasploit Various Java Exploit Common Class name
- [x] ET EXPLOIT SUSPICIOUS DTLS 1.0 Fragmented Client Hello Possible CVE-2014-0195
- [x] ET EXPLOIT Supermicro BMC Password Disclosure 1
- [x] ET EXPLOIT Supermicro BMC Password Disclosure 3
- [x] ET EXPLOIT Metasploit FireFox WebIDL Privileged Javascript Injection
- [x] ET EXPLOIT F5 BIG-IP rsync cmi authorized_keys access attempt
- [x] ET EXPLOIT F5 BIG-IP rsync cmi authorized_keys successful upload
- [x] ET EXPLOIT Possible CVE-2014-6271 exploit attempt via malicious DHCP ACK
- [x] ET EXPLOIT Possible CVE-2014-6271 Attempt Against SIP Proxy
- [x] ET EXPLOIT Possible OpenVPN CVE-2014-6271 attempt
- [x] ET EXPLOIT Possible Pure-FTPd CVE-2014-6271 attempt
- [x] ET EXPLOIT Possible CVE-2014-6271 malicious DNS response
- [ ] ET EXPLOIT SSL excessive fatal alerts (possible POODLE attack against server)
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 2
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 4
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 6
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 8
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 10
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 12
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 14
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 16
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 18
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 20
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 22
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 24
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 26
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 28
- [x] ET EXPLOIT Linksys Auth Bypass share_editor.cgi
- [x] ET EXPLOIT Linksys Failed Upgrade BackDoor Access (Server Response)
- [ ] ET EXPLOIT CritX/SafePack/FlashPack CVE-2013-2551
- [x] ET EXPLOIT Joomla 3.2.1 SQL injection attempt 2
- [ ] ET EXPLOIT Possible CVE-2014-1761 Inbound SMTP 3
- [ ] ET EXPLOIT Possible CVE-2014-1761 Inbound SMTP 5
- [ ] ET EXPLOIT Possible CVE-2014-1761 Inbound SMTP 1
- [x] ET EXPLOIT Malformed HeartBeat Response
- [x] ET EXPLOIT TLS HeartBeat Request (Server Initiated) fb set
- [x] ET EXPLOIT Possible OpenSSL HeartBleed Large HeartBeat Response (Client Init Vuln Server)
- [x] ET EXPLOIT Possible OpenSSL HeartBleed Large HeartBeat Response from Common SSL Port (Outbound from Server)
- [x] ET EXPLOIT Possible TLS HeartBleed Unencrypted Request Method 4 (Inbound to Common SSL Port)
- [ ] ET EXPLOIT Fiesta PDF Exploit Download
- [ ] ET EXPLOIT Common Bad Actor Indicators Used in Various Targeted 0-day Attacks
- [ ] ET EXPLOIT SUSPICIOUS DTLS Pre 1.0 Fragmented Client Hello Possible CVE-2014-0195
- [ ] ET EXPLOIT SUSPICIOUS DTLS 1.2 Fragmented Client Hello Possible CVE-2014-0195
- [x] ET EXPLOIT Supermicro BMC Password Disclosure 2
- [x] ET EXPLOIT Supermicro BMC Password Disclosure 4
- [x] ET EXPLOIT F5 BIG-IP rsync cmi access attempt
- [x] ET EXPLOIT F5 BIG-IP rsync cmi authorized_keys successful exfiltration
- [x] ET EXPLOIT Metasploit Random Base CharCode JS Encoded String
- [x] ET EXPLOIT Possible CVE-2014-6271 Attempt Against SIP Proxy
- [x] ET EXPLOIT Possible Qmail CVE-2014-6271 Mail From attempt
- [x] ET EXPLOIT Possible OpenVPN CVE-2014-6271 attempt
- [x] ET EXPLOIT Possible Postfix CVE-2014-6271 attempt
- [x] ET EXPLOIT Possible CVE-2014-6271 exploit attempt via malicious DNS
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 1
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 3
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 5
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 7
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 9
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 11
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 13
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 15
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 17
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 19
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 21
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 23
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 25
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 27
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 29

- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 30
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 31
- [x] ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCODE 32
- [x] ET EXPLOIT Possible Malicious NAT-PMP Response to External Network
- [x] ET EXPLOIT Possible Malicious NAT-PMP Response Successful TCP Map to External Network
- [x] ET EXPLOIT Possible Malicious NAT-PMP Response Successful UDP Map to External Network
- [ ] ET EXPLOIT Fiesta Java Exploit/Payload URI Struct
- [ ] ET EXPLOIT Fiesta SilverLight 4.x Exploit URI Struct
- [ ] ET EXPLOIT Possible HanJuan Flash Exploit
- [x] ET EXPLOIT Belkin N750 Buffer Overflow Attempt
- [x] ET EXPLOIT Possible Internet Explorer VBscript failure to handle error case information disclosure CVE-2014-6332 Common Function Name
- [ ] ET EXPLOIT Possible Sweet Orange CVE-2014-6332 Payload Request
- [ ] ET EXPLOIT FlashPack Flash Exploit Nov 20 2014
- [ ] ET EXPLOIT Magnitude Flash Exploit (IE)
- [x] ET EXPLOIT D-Link IP Camera Vulnerable HTTP Request (CVE-2013-1599)
- [x] ET EXPLOIT D-Link IP Camera Vulnerable HTTP Request (CVE-2013-1600)
- [x] ET EXPLOIT D-Link IP Camera Vulnerable HTTP Request (CVE-2013-1601)
- [ ] ET EXPLOIT Possible PYKEK Priv Esc in-use
- [x] ET EXPLOIT QNAP Shellshock CVE-2014-6271
- [x] ET EXPLOIT QNAP Shellshock script retrieval
- [x] ET EXPLOIT Possible GoldenPac Priv Esc in-use
- [ ] ET EXPLOIT Possible CVE-2014-6332 Arrays with Offset Dec 23
- [x] ET EXPLOIT Possible Misfortune Cookie - SET
- [x] ET EXPLOIT Possible Misfortune Cookie RomPager Server banner
- [ ] ET EXPLOIT CVE-2015-0235 Exim Buffer Overflow Attempt (HELO)
- [ ] ET EXPLOIT CVE-2015-0235 Exim Buffer Overflow Attempt (EHLO)
- [x] ET EXPLOIT Possible CVE-2014-6332 DECS2
- [x] ET EXPLOIT Possible dlink-DSL2640B DNS Change Attempt
- [x] ET EXPLOIT Possible ShuttleTech 915WM DNS Change Attempt
- [x] ET EXPLOIT Generic ADSL Router DNS Change GET Request
- [x] ET EXPLOIT Generic ADSL Router DNS Change POST Request
- [x] ET EXPLOIT Seagate Business NAS Unauthenticated Remote Command Execution
- [x] ET EXPLOIT PCMan FTP Server 2.0.7 Remote Command Execution
- [x] ET EXPLOIT D-Link and TRENDnet ncc2 Service Vulnerability (ping.ccp) 2015-1187
- [x] ET EXPLOIT D-Link and TRENDnet ncc2 Service Vulnerability (fwupdate.cpp) 2015-1187
- [ ] ET EXPLOIT FREAK Weak Export Suite From Server (CVE-2015-0204)
- [ ] ET EXPLOIT FREAK Weak Export Suite From Server (CVE-2015-0204)
- [ ] ET EXPLOIT FREAK Weak Export Suite From Server (CVE-2015-0204)
- [ ] ET EXPLOIT FREAK Weak Export Suite From Server (CVE-2015-0204)
- [x] ET EXPLOIT FREAK Weak Export Suite From Server (CVE-2015-0204)
- [ ] ET EXPLOIT FREAK Weak Export Suite From Server (CVE-2015-0204)
- [ ] ET EXPLOIT FREAK Weak Export Suite From Server (CVE-2015-0204)
- [ ] ET EXPLOIT FREAK Weak Export Suite From Server (CVE-2015-0204)
- [ ] ET EXPLOIT FREAK Weak Export Suite From Server (CVE-2015-0204)
- [ ] ET EXPLOIT FREAK Weak Export Suite From Server (CVE-2015-0204)
- [ ] ET EXPLOIT FREAK Weak Export Suite From Server (CVE-2015-0204)
- [ ] ET EXPLOIT FREAK Weak Export Suite From Server (CVE-2015-0204)
- [x] ET EXPLOIT Metasploit Plugin-Detect Posting Data 4
- [x] ET EXPLOIT Metasploit Plugin-Detect Posting Data 5
- [x] ET EXPLOIT Metasploit Plugin-Detect Posting Data 6
- [x] ET EXPLOIT Metasploit Plugin-Detect Posting Data 7
- [x] ET EXPLOIT Metasploit Browser Exploit Server Plugin Detect 2
- [x] ET EXPLOIT TP-LINK TL-WR340G Router DNS Change GET Request
- [x] ET EXPLOIT Belkin Wireless G Router DNS Change POST Request
- [x] ET EXPLOIT Linksys WRT54GL Router DNS Change POST Request
- [x] ET EXPLOIT Netgear WNDR Router DNS Change POST Request
- [x] ET EXPLOIT Motorola SBG900 Router DNS Change GET Request
- [x] ET EXPLOIT ASUS RT N56U Router DNS Change GET Request 1
- [x] ET EXPLOIT ASUS RT N56U Router DNS Change GET Request 2
- [x] ET EXPLOIT FritzBox RCE POST Request
- [x] ET EXPLOIT FritzBox RCE GET Request
- [x] ET EXPLOIT ASUS RT N56U Router DNS Change GET Request 3
- [x] ET EXPLOIT TP-LINK Known Malicious Router DNS Change GET Request
- [x] ET EXPLOIT D-link DI604 Known Malicious Router DNS Change GET Request
- [x] ET EXPLOIT Netgear DGN1000B Router DNS Change GET Request
- [x] ET EXPLOIT Belkin G F5D7230-4 Router DNS Change GET Request
- [x] ET EXPLOIT Tenda ADSL2/2+ Router DNS Change GET Request
- [x] ET EXPLOIT Known Malicious Router DNS Change GET Request
- [x] ET EXPLOIT TP-LINK TL-WR841N Router DNS Change GET Request
- [x] ET EXPLOIT Linksys WRT54GL DNS Change GET Request
- [x] ET EXPLOIT TP-LINK TL-WR750N DNS Change GET Request
- [x] ET EXPLOIT D-Link Devices Home Network Administration Protocol Command Execution
- [x] ET EXPLOIT Possible Redirect to SMB exploit attempt - 302
- [x] ET EXPLOIT Possible Redirect to SMB exploit attempt - 301
- [x] ET EXPLOIT Possible Redirect to SMB exploit attempt - 307
- [x] ET EXPLOIT Possible Redirect to SMB exploit attempt - 303
- [x] ET EXPLOIT WNR2000v4 HTTP POST RCE Attempt Via Timestamp Discovery
- [ ] ET EXPLOIT Logjam Weak DH/DHE Export Suite From Server
- [ ] ET EXPLOIT Logjam Weak DH/DHE Export Suite From Server
- [x] ET EXPLOIT Possible Elasticsearch CVE-2015-1427 Exploit Campaign SSL Certificate
- [x] ET EXPLOIT Targeted Attack from APT Actor Delivering HT SWF Exploit RIP
- [x] ET EXPLOIT AirLive RCI HTTP Request
- [x] ET EXPLOIT Possible BIND9 DoS CVE-2015-5477 M1
- [x] ET EXPLOIT Possible BIND9 DoS CVE-2015-5477 M2
- [x] ET EXPLOIT Possible BIND9 DoS CVE-2015-5477 M3
- [x] ET EXPLOIT Possible BIND9 DoS CVE-2015-5477 M4
- [x] ET EXPLOIT HT SWF Exploit RIP
- [x] ET EXPLOIT Possible Firefox PDF.js Same-Origin-Bypass CVE-2015-4495 M1
- [x] ET EXPLOIT Possible Firefox PDF.js Same-Origin-Bypass CVE-2015-4495 M2
- [x] ET EXPLOIT Websense Content Gateway submit_net_debug.cgi cmd_param Param Buffer Overflow Attempt
- [x] ET EXPLOIT HT SWF Exploit RIP M2
- [x] ET EXPLOIT Possible Internet Explorer Memory Corruption Vulnerability (CVE-2015-2444)
- [x] ET EXPLOIT FireEye Appliance Unauthorized File Disclosure
- [x] ET EXPLOIT Possible Android Stagefright MP4 CVE-2015-1538 - Shell
- [x] ET EXPLOIT Possible Android Stagefright MP4 CVE-2015-1538 - ROP
- [x] ET EXPLOIT Possible Android Stagefright MP4 CVE-2015-1538 - STSC
- [x] ET EXPLOIT Netgear Multiple Router Auth Bypass

- [x] ET EXPLOIT Possible Magento Directory Traversal Attempt
- [ ] ET EXPLOIT Possible click2play bypass Oct 19 2015 B64 2
- [x] ET EXPLOIT Serialized Java Object Calling Common Collection Function
- [x] ET EXPLOIT Serialized Java Object Generated by ysoserial
- [x] ET EXPLOIT Serialized Spring Java Object Generated by ysoserial
- [x] ET EXPLOIT Joomla RCE M2 (Serialized PHP in UA)
- [x] ET EXPLOIT Juniper ScreenOS telnet Backdoor Default Password Attempt
- [x] ET EXPLOIT TrendMicro node.js HTTP RCE Exploit Inbound (showSB)
- [x] ET EXPLOIT Possible CVE-2016-0777 Client Sent Roaming Resume Request
- [x] ET EXPLOIT Possible CVE-2016-1287 Invalid Fragment Size Inbound 2
- [x] ET EXPLOIT D-Link DCS-930L Remote Command Execution attempt
- [x] ET EXPLOIT Possible 2015-7547 Malformed Server response
- [x] ET EXPLOIT Possible CVE-2015-7547 Long Response to A lookup
- [x] ET EXPLOIT Possible CVE-2015-7547 Malformed Server Response A/AAAA
- [x] ET EXPLOIT Possible CVE-2015-7547 Large Response to A/AAAA query
- [x] ET EXPLOIT TrendMicro node.js (Remote Debugger)
- [x] ET EXPLOIT Quanta LTE Router UDP Backdoor Activation Attempt
- [x] ET EXPLOIT Quanta LTE Router RDE Exploit Attempt 2 (traceroute)
- [x] ET EXPLOIT Open MGate Device
- [x] ET EXPLOIT Possible Internet Explorer VBscript failure to handle error case information disclosure CVE-2014-6332 Common Construct M2
- [x] ET EXPLOIT Possible CVE-2016-2209 Symantec PowerPoint Parsing Buffer Overflow M1
- [ ] ET EXPLOIT Possible CVE-2016-2211 Symantec Cab Parsing Buffer Overflow
- [x] ET EXPLOIT Possible Symantec Malicious MIME Doc Name Overflow (EICAR) toclient M1
- [x] ET EXPLOIT Possible Symantec Malicious MIME Doc Name Overflow (EICAR) toclient M4
- [x] ET EXPLOIT Possible Symantec Malicious MIME Doc Name Overflow (EICAR) toserver M4
- [x] ET EXPLOIT CVE-2016-0189 Common Construct M2
- [x] ET EXPLOIT Equation Group ExtraBacon Cisco ASA PMCHECK Disable
- [x] ET EXPLOIT Equation Group EGREGIOUSBLUNDER Fortigate Exploit Attempt
- [ ] ET EXPLOIT Possible Challack Tool in use
- [x] ET EXPLOIT CVE-2014-6332 Sep 01 2016 (HFS Actor) M1
- [x] ET EXPLOIT Possible Android Stagefright MP4 (CVE 2016-3861) Set
- [x] ET EXPLOIT Possible MySQL CVE-2016-6662 Attempt
- [x] ET EXPLOIT CVE-2015-2419 As observed in Magnitude EK
- [x] ET EXPLOIT D-Link DSL-2740R Remote DNS Change Attempt
- [ ] ET EXPLOIT Unknown Router Remote DNS Change Attempt
- [x] ET EXPLOIT REDIS Attemted SSH Authorized Key Writing Attempt
- [x] ET EXPLOIT Eir D1000 Modem CWMP Exploit RCE
- [x] ET EXPLOIT Firefox 0-day used against TOR browser Nov 29 2016 M1
- [x] ET EXPLOIT CVE-2016-3210 Exploit Observed ITW M1 Nov 30
- [x] ET EXPLOIT Netgear R7000 Command Injection Exploit
- [x] ET EXPLOIT Possible Microsoft Edge Chakra.dll Type Confusion (CVE-2016-7200 CVE-2016-7201) Observed in SunDown EK 3
- [x] ET EXPLOIT Possible Microsoft Edge Chakra.dll Type Confusion (CVE-2016-7200 CVE-2016-7201) Observed in SunDown EK 2
- [x] ET EXPLOIT Possible Microsoft Edge Chakra.dll Type Confusion (CVE-2016-7200 CVE-2016-7201) B642
- [x] ET EXPLOIT Possible Microsoft RDP Client for Mac RCE
- [ ] ET EXPLOIT Possible Ticketbleed Server Hello (CVE-2016-9244)
- [ ] ET EXPLOIT Possible click2play bypass Oct 19 2015 B64 1
- [ ] ET EXPLOIT Possible click2play bypass Oct 19 2015 B64 3
- [x] ET EXPLOIT Serialized Java Object Calling Common Collection Function
- [x] ET EXPLOIT Serialized Groovy Java Object Generated by ysoserial
- [x] ET EXPLOIT Joomla RCE (JDatabaseDriverMysqli)
- [x] ET EXPLOIT Joomla RCE M3 (Serialized PHP in XFF)
- [x] ET EXPLOIT TrendMicro node.js HTTP RCE Exploit Inbound (openUrlInDefaultBrowser)
- [x] ET EXPLOIT Possible CVE-2016-0777 Server Advertises Suspicious Roaming Support
- [x] ET EXPLOIT Possible CVE-2016-1287 Invalid Fragment Size Inbound
- [x] ET EXPLOIT Possible CVE-2016-1287 Invalid Fragment Size Inbound 3
- [x] ET EXPLOIT MS16-009 IE MSHTML Form Element Type Confusion (CVE-2016-0061)
- [x] ET EXPLOIT Possible 2015-7547 PoC Server Response
- [x] ET EXPLOIT Possible CVE-2015-7547 Long Response to AAAA lookup
- [x] ET EXPLOIT Possible CVE-2015-7547 A/AAAA Record Lookup Possible Forced FallBack(fb set)
- [x] ET EXPLOIT FireEye Detection Evasion %temp% attempt - Inbound
- [x] ET EXPLOIT Quanta LTE Router Information Disclosure Exploit Attempt
- [x] ET EXPLOIT Quanta LTE Router RDE Exploit Attempt 1 (ping)
- [x] ET EXPLOIT Dameware DMRC Buffer Overflow Attempt (CVE-2016-2345)
- [x] ET EXPLOIT Linksys Router Unauthenticated Remote Code Execution
- [x] ET EXPLOIT CVE-2016-1287 Public Exploit ShellCode
- [x] ET EXPLOIT Possible CVE-2016-2209 Symantec PowerPoint Parsing Buffer Overflow M2
- [x] ET EXPLOIT Possible Symantec Malicious MIME Doc Name Overflow (EICAR) toclient M2
- [x] ET EXPLOIT Possible Symantec Malicious MIME Doc Name Overflow (EICAR) toserver M3
- [x] ET EXPLOIT Possible Symantec Malicious MIME Doc Name Overflow (EICAR) toclient M3
- [x] ET EXPLOIT CVE-2016-0189 Common Construct M1
- [x] ET EXPLOIT LastPass RCE Attempt
- [x] ET EXPLOIT Equation Group ExtraBacon Cisco ASA AAAADMINAUTH Disable
- [x] ET EXPLOIT CISCO FIREWALL SNMP Buffer Overflow Extrabacon (CVE-2016-6366)
- [ ] ET EXPLOIT RST Flood With Window
- [x] ET EXPLOIT CVE-2014-6332 Sep 01 2016 (HFS Actor) M2
- [x] ET EXPLOIT Possible Android Stagefright MP4 (CVE 2016-3861) ROP
- [x] ET EXPLOIT Possible MySQL cnf overwrite CVE-2016-6662 Attempt
- [x] ET EXPLOIT Possible Cisco IKEv1 Information Disclosure Vulnerability CVE-2016-6415
- [x] ET EXPLOIT COMTREND ADSL Router CT-5367 Remote DNS Change Attempt
- [x] ET EXPLOIT Possible iOS Pegasus Safari Exploit (CVE-2016-4657)
- [x] ET EXPLOIT REDIS Attempted SSH Key Upload
- [x] ET EXPLOIT Eir D1000 Modem CWMP Exploit Retrieving Wifi Key
- [x] ET EXPLOIT Firefox 0-day used against TOR browser Nov 29 2016 M2
- [x] ET EXPLOIT CVE-2016-3210 Exploit Observed ITW M1 Nov 30
- [x] ET EXPLOIT Possible CVE-2016-10033 PHPMailer RCE Attempt
- [x] ET EXPLOIT Possible Microsoft Edge Chakra.dll Type Confusion (CVE-2016-7200 CVE-2016-7201) Observed in SunDown EK 1
- [x] ET EXPLOIT Possible Microsoft Edge Chakra.dll Type Confusion (CVE-2016-7200 CVE-2016-7201) B641
- [x] ET EXPLOIT Possible Microsoft Edge Chakra.dll Type Confusion (CVE-2016-7200 CVE-2016-7201) B643
- [ ] ET EXPLOIT Possible Ticketbleed Client Hello (CVE-2016-9244)
- [x] ET EXPLOIT TP-LINK DNS Change GET Request (DNSChanger EK)

- [x] ET EXPLOIT TP-LINK Password Change GET Request (DNSChanger EK)
- [x] ET EXPLOIT HP Smart Storage Administrator Remote Command Injection
- [x] ET EXPLOIT D-LINK DIR-615 Cross-Site Request Forgery (CVE-2017-7398)
- [x] ET EXPLOIT Possible CVE-2017-0199 HTA Inbound
- [x] ET EXPLOIT Cisco Catalyst Remote Code Execution (CVE-2017-3881)
- [x] ET EXPLOIT Possible Successful ETERNALROMANCE MS17-010 - Windows Executable Observed
- [x] ET EXPLOIT Possible ETERNALCHAMPION MS17-010 Sync Request (set)
- [x] ET EXPLOIT Possible ECLIPSEDWING RPCTOUCH MS08-067
- [x] ET EXPLOIT Possible DOUBLEPULSAR Beacon Response
- [x] ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response
- [x] ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Request (set)
- [x] ET EXPLOIT BlueCoat CAS v1.3.7.1 Report Email Command Injection attempt
- [x] ET EXPLOIT ETERNALBLUE Exploit M2 MS17-010
- [x] ET EXPLOIT NB8-02 - Possible Unauthed RCE via nbbsdtar
- [x] ET EXPLOIT Samba Arbitrary Module Loading Vulnerability (.so file write to share) (CVE-2017-7494)
- [x] ET EXPLOIT Possible $MFT NTFS Device Access in HTTP Response
- [x] ET EXPLOIT Samba Arbitrary Module Loading Vulnerability M2 (NT Create AndX .so) (CVE-2017-7494)
- [x] ET EXPLOIT Possible SharePoint XSS (CVE-2017-8514) Inbound
- [x] ET EXPLOIT Possible ETERNALBLUE Exploit M3 MS17-010
- [x] ET EXPLOIT Possible WINS Server Remote Memory Corruption Vulnerability
- [x] ET EXPLOIT Ubiquiti Networks UniFi Cloud Key Firm v0.6.1 Host Remote Command Execution attempt
- [x] ET EXPLOIT Apache Struts 2 REST Plugin XStream RCE (Runtime.Exec)
- [x] ET EXPLOIT Apache Struts 2 REST Plugin ysoserial Usage (B64) 2
- [x] ET EXPLOIT Apache Struts 2 REST Plugin (B64) 4
- [x] ET EXPLOIT Apache Struts 2 REST Plugin (B64) 6
- [x] ET EXPLOIT Apache Struts 2 REST Plugin (ProcessBuilder)
- [x] ET EXPLOIT CVE-2016-0189 Exploit HFS Actor
- [ ] ET EXPLOIT Possible CVE-2017-8759 Soap File DL
- [ ] ET EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication
- [x] ET EXPLOIT Likely Struts S2-053-CVE-2017-12611 Exploit Attempt M2
- [x] ET EXPLOIT Possible CVE-2017-12629 XXE Exploit Attempt (URI)
- [x] ET EXPLOIT Possible CVE-2017-12629 RCE Exploit Attempt (HTTP GET 2)
- [x] ET EXPLOIT Netgear ReadyNAS Surveillance Unauthenticated Remote Command Execution
- [x] ET EXPLOIT Netgear DGN Remote Command Execution
- [x] ET EXPLOIT AVTECH Authenticated Command Injection in CloudSetup.cgi
- [x] ET EXPLOIT AVTECH Authenticated Command Injection in PwdGrp.cgi
- [x] ET EXPLOIT Actiontec C1000A backdoor account M2
- [x] ET EXPLOIT Actiontec C1000A backdoor account M1
- [x] ET EXPLOIT Possible MeltDown PoC Download In Progress
- [x] ET EXPLOIT Generic ADSL Router DNS Change Request
- [x] ET EXPLOIT MikroTik RouterOS Chimay Red Remote Code Execution Probe
- [x] ET EXPLOIT Apache CouchDB JSON Remote Privesc Attempt (CVE-2017-12636)
- [x] ET EXPLOIT Possible CVE-2018-0171 Exploit (PoC based)
- [x] ET EXPLOIT IBM WebSphere - RCE Java Deserialization
- [x] ET EXPLOIT NETGEAR WNR2000v5 hidden_lang_avi Stack Overflow (CVE-2016-10174)
- [x] ET EXPLOIT TP-Link Archer C2 and Archer C20i Remote Code Execution
- [x] ET EXPLOIT Possible CVE-2017-0199 HTA Inbound M2
- [x] ET EXPLOIT MSXMLHTTP Download of HTA (Observed in CVE-2017-0199)
- [x] ET EXPLOIT Possible ETERNALROMANCE MS17-010
- [x] ET EXPLOIT Possible ETERNALCHAMPION MS17-010 Sync Response
- [x] ET EXPLOIT Possible ECLIPSEDWING MS08-067
- [x] ET EXPLOIT Possible ETERNALBLUE MS17-010 Heap Spray
- [x] ET EXPLOIT Possible ETERNALROMANCE MS17-010 Heap Spray
- [x] ET EXPLOIT Possible EXPLODINGCAN IIS5.0/6.0 Exploit Attempt
- [x] ET EXPLOIT Intel AMT Login Attempt Detected (CVE 2017-5689)
- [x] ET EXPLOIT NB8-01 - Unauthed RCE via bprd
- [x] ET EXPLOIT NB8-04 - Possible Unauthed RCE via whitelist bypass
- [x] ET EXPLOIT Samba Arbitrary Module Loading Vulnerability (NT Create AndX .so) (CVE-2017-7494)
- [x] ET EXPLOIT Win32/Industroyer DDOS Siemens SIPROTEC (CVE-2015-5374)
- [x] ET EXPLOIT HP Printer Attempted Path Traversal via PJL
- [x] ET EXPLOIT CVE-2017-0199 Common Obfus Stage 2 DL
- [x] ET EXPLOIT Suspicious FTP RETR to .hta file possible exploit (CVE-2017-0199)
- [x] ET EXPLOIT SUSPICIOUS Possible CVE-2017-0199 IE7/NoCookie/ Referer HTA dl
- [x] ET EXPLOIT Apache Struts 2 REST Plugin XStream RCE (ProcessBuilder)
- [x] ET EXPLOIT Apache Struts 2 REST Plugin ysoserial Usage (B64) 1
- [x] ET EXPLOIT Apache Struts 2 REST Plugin ysoserial Usage (B64) 3
- [x] ET EXPLOIT Apache Struts 2 REST Plugin (B64) 5
- [x] ET EXPLOIT Apache Struts 2 REST Plugin (Runtime.Exec)
- [x] ET EXPLOIT CVE-2016-0189 Exploit
- [x] ET EXPLOIT Possible CVE-2017-8759 Soap File DL
- [x] ET EXPLOIT Possible CVE-2017-8759 Soap File DL Over FTP
- [x] ET EXPLOIT Likely Struts S2-053-CVE-2017-12611 Exploit Attempt M1
- [x] ET EXPLOIT Possible CVE-2017-12629 RCE Exploit Attempt (HTTP POST)
- [x] ET EXPLOIT Possible CVE-2017-12629 RCE Exploit Attempt (HTTP GET 1)
- [x] ET EXPLOIT D-Link 850L Password Extract Attempt
- [x] ET EXPLOIT Possible Vacron NVR Remote Command Execution
- [x] ET EXPLOIT AVTECH Unauthenticated Command Injection in DVR Devices
- [x] ET EXPLOIT AVTECH Authenticated Command Injection in adcommand.cgi
- [x] ET EXPLOIT Possible Oracle Identity Manager Attempt to Logon with default account
- [x] ET EXPLOIT Exim4 UAF Attempt (BDAT with non-printable chars)
- [x] ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361
- [x] ET EXPLOIT Possible Spectre PoC Download In Progress
- [x] ET EXPLOIT Possible Belkin N600DB Wireless Router Request Forgery Attempt
- [x] ET EXPLOIT [PT Security] Exim <4.90.1 Base64 Overflow RCE (CVE-2018-6789)
- [x] ET EXPLOIT Apache CouchDB JSON Remote Privesc Attempt (CVE-2017-12635)
- [x] ET EXPLOIT Cisco Smart Install Exploitation Tool - Update Ios and Execute

- [x] ET EXPLOIT Cisco Smart Install Exploitation Tool - ChangeConfig
- [x] ET EXPLOIT Cisco Smart Install Exploitation Tool - GetConfig
- [x] ET EXPLOIT HackingTrio UA (Hello, World)
- [x] ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)
- [x] ET EXPLOIT ETERNALBLUE Probe Vulnerable System Response MS17-010
- [x] ET EXPLOIT phpLDAPadmin LDAP Injection
- [x] ET EXPLOIT phpMyAdmin 4.8.1 - Local File Inclusion
- [x] ET EXPLOIT TP-Link Technologies TL-WA850RE Wi-Fi Range Extender - Command Execution
- [x] ET EXPLOIT AsusWRT RT-AC750GF Cross-Site Request Forgery
- [x] ET EXPLOIT Ecessa WANWorx WVR-30 Cross-Site Request Forgery
- [x] ET EXPLOIT Intex Router N-150 Cross-Site Request Forgery
- [x] ET EXPLOIT TP-Link TL-WR840N/TL-WR841N - Authentication Bypass (Add Port Forwarding)
- [x] ET EXPLOIT TP-Link TL-WR840N/TL-WR841N - Authentication Bypass (DMZ enable and Disable)
- [x] ET EXPLOIT TP-Link TL-WR840N/TL-WR841N - Authentication Bypass (Enable Guest Network)
- [x] ET EXPLOIT TP-Link TL-WR840N/TL-WR841N - Authentication Bypass (GET conf.bin)
- [x] ET EXPLOIT TP-Link TL-WR840N/TL-WR841N - Authentication Bypass (Reboot Router)
- [x] ET EXPLOIT TP-Link TL-WR840N/TL-WR841N - Authentication Bypass (WiFi Password Change)
- [x] ET EXPLOIT D-Link DSL-2750B - OS Command Injection
- [x] ET EXPLOIT HP Enterprise VAN SDN Controller Exec Backdoor
- [x] ET EXPLOIT HP Enterprise VAN SDN Controller Install Backdoor
- [x] ET EXPLOIT HP Enterprise VAN SDN Controller Upload Backdoor
- [x] ET EXPLOIT Cisco Adaptive Security Appliance - Path Traversal
- [x] ET EXPLOIT DynoRoot DHCP - Client Command Injection
- [x] ET EXPLOIT CloudMe Sync Buffer Overflow
- [x] ET EXPLOIT VMware NSX SD-WAN Command Injection
- [x] ET EXPLOIT VMware NSX SD-WAN Command Injection 2
- [x] ET EXPLOIT Geutebruck Remote Command Execution
- [x] ET EXPLOIT Nagios XI SQL Injection
- [x] ET EXPLOIT Nagios XI Remote Code Execution 2
- [x] ET EXPLOIT Nagios XI Remote Code Execution
- [x] ET EXPLOIT Nagios XI SQL Injection 2
- [x] ET EXPLOIT Nagios XI Remote Code Execution 3
- [x] ET EXPLOIT Nagios XI Set DB User Root
- [x] ET EXPLOIT Nagios XI Adding Administrative User
- [x] ET EXPLOIT FTPShell client Stack Buffer Overflow
- [ ] ET EXPLOIT Possible ModSecurity 3.0.0 Cross-Site Scripting
- [x] ET EXPLOIT ADB Broadband Authorization Bypass
- [x] ET EXPLOIT Oracle Weblogic Server Deserialization Remote Command Execution
- [x] ET EXPLOIT Exim Internet Mailer Remote Code Execution
- [x] ET EXPLOIT xdebug OS Command Execution
- [x] ET EXPLOIT Generic system shell command to php base64 encoded Remote Code Execution 1
- [x] ET EXPLOIT Generic system shell command to php base64 encoded Remote Code Execution 2
- [x] ET EXPLOIT Generic system shell command to php base64 encoded Remote Code Execution 3
- [x] ET EXPLOIT Generic system shell command to php base64 encoded Remote Code Execution 4
- [x] ET EXPLOIT Generic system shell command to php base64 encoded Remote Code Execution 5
- [x] ET EXPLOIT Generic system shell command to php base64 encoded Remote Code Execution 6
- [x] ET EXPLOIT file_put_contents php base64 encoded Remote Code Execution 1
- [x] ET EXPLOIT file_put_contents php base64 encoded Remote Code Execution 2
- [x] ET EXPLOIT file_put_contents php base64 encoded Remote Code Execution 3
- [x] ET EXPLOIT bin bash base64 encoded Remote Code Execution 1
- [x] ET EXPLOIT bin bash base64 encoded Remote Code Execution 2
- [x] ET EXPLOIT bin bash base64 encoded Remote Code Execution 3
- [x] ET EXPLOIT php script base64 encoded Remote Code Execution 1
- [x] ET EXPLOIT php script base64 encoded Remote Code Execution 2
- [x] ET EXPLOIT php script base64 encoded Remote Code Execution 3
- [x] ET EXPLOIT php script double base64 encoded Remote Code Execution 1
- [x] ET EXPLOIT php script double base64 encoded Remote Code Execution 2
- [x] ET EXPLOIT php script double base64 encoded Remote Code Execution 3
- [x] ET EXPLOIT php script double base64 encoded Remote Code Execution 4
- [x] ET EXPLOIT php script double base64 encoded Remote Code Execution 5
- [x] ET EXPLOIT php script double base64 encoded Remote Code Execution 6
- [x] ET EXPLOIT php script double base64 encoded Remote Code Execution 7
- [x] ET EXPLOIT php script double base64 encoded Remote Code Execution 8
- [x] ET EXPLOIT php script double base64 encoded Remote Code Execution 9
- [x] ET EXPLOIT HID VertX and Edge door controllers command_blink_on Remote Command Execution
- [x] ET EXPLOIT D-Link DIR601 2.02 Credential Disclosure
- [x] ET EXPLOIT IBM QRadar SIEM Unauthenticated Remote Code Execution
- [x] ET EXPLOIT SAP NetWeaver AS JAVA CRM - Log injection Remote Command Execution
- [x] ET EXPLOIT Adobe Coldfusion BlazeDS Java Object Deserialization Remote Code Execution
- [x] ET EXPLOIT Oracle WebLogic - wls-wsat Component Deserialization Remote Code Execution Unix
- [x] ET EXPLOIT Oracle WebLogic - wls-wsat Component Deserialization Remote Code Execution Windows
- [x] ET EXPLOIT Nanopool Claymore Dual Miner Remote Code Execution Linux
- [x] ET EXPLOIT Nanopool Claymore Dual Miner Remote Code Execution Windows
- [x] ET EXPLOIT MVPower DVR Shell UCE MSF Check
- [x] ET EXPLOIT MVPower DVR Shell UCE
- [x] ET EXPLOIT Multiple CCTV-DVR Vendors RCE
- [x] ET EXPLOIT Remote Command Execution via Android Debug Bridge
- [x] ET EXPLOIT Remote Command Execution via Android Debug Bridge 2
- [x] ET EXPLOIT Oracle WebLogic Unrestricted File Upload (CVE-2018-2894)
- [x] ET EXPLOIT Mikrotik Winbox RCE Attempt (CVE-2018-14847)
- [x] ET EXPLOIT SMB Null Pointer Dereference PoC Inbound (CVE-2018-0833)
- [x] ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)
- [x] ET EXPLOIT SonicWall Global Management System - XMLRPC set_time_zone Command Injection (CVE-2018-9866)
- [x] ET EXPLOIT Apache Struts Possible OGNL Java Exec In URI M2

- [x] ET EXPLOIT Apache Struts RCE CVE-2018-11776 POC M1
- [x] ET EXPLOIT Apache Struts RCE CVE-2018-11776 POC M2
- [x] ET EXPLOIT HP Enterprise VAN SDN Controller Root Command Injection (Unix)
- [x] ET EXPLOIT HP Enterprise VAN SDN Controller Root Command Injection (Linux)
- [x] ET EXPLOIT HP Enterprise VAN SDN Controller Upload Backdoor 2
- [x] ET EXPLOIT Ghostscript invalidcheck escape attempt (SMTP)
- [x] ET EXPLOIT Ghostscript invalidcheck escape attempt
- [x] ET EXPLOIT Ghostscript illegal read undefinedfilename attempt (SMTP)
- [x] ET EXPLOIT Ghostscript illegal read undefinedfilename attempt
- [x] ET EXPLOIT Ghostscript illegal delete bindnow attempt (SMTP)
- [x] ET EXPLOIT Ghostscript illegal delete bindnow attempt
- [x] ET EXPLOIT Ghostscript setpattern type confusion attempt (SMTP)
- [x] ET EXPLOIT Ghostscript setpattern type confusion attempt
- [x] ET EXPLOIT Ghostscript LockDistillerParams type confusion attempt (SMTP)
- [x] ET EXPLOIT Ghostscript LockDistillerParams type confusion attempt
- [x] ET EXPLOIT Apache Struts memberAccess and getWriter inbound OGNL injection remote code execution attempt
- [x] ET EXPLOIT Apache Struts memberAccess and opensymphony inbound OGNL injection remote code execution attempt
- [x] ET EXPLOIT Apache Struts getWriter and opensymphony inbound OGNL injection remote code execution attempt
- [x] ET EXPLOIT Linksys E-Series Device RCE Attempt
- [x] ET EXPLOIT Possible Vacron NVR Remote Command Execution M2
- [x] ET EXPLOIT EnGenius EnShare IoT Gigabit Cloud Service RCE
- [x] ET EXPLOIT Zyxel Command Injection RCE (CVE-2017-6884)
- [x] ET EXPLOIT NetGain Enterprise Manager 7.2.562 Ping Command Injection
- [x] ET EXPLOIT NUUO OS Command Injection
- [x] ET EXPLOIT NUUO OS Command Injection M2
- [x] ET EXPLOIT Possible Tor/Noscript JS Bypass
- [x] ET EXPLOIT Possible CVE-2018-4407 - Apple ICMP DoS PoC
- [x] ET EXPLOIT Possible Cisco RV320 RCE Attempt (CVE-2019-1652)
- [x] ET EXPLOIT Possible MicroLogix 1100 PCCC DoS Condition (CVE-2017-7924)
- [x] ET EXPLOIT Nuuo NVR RCE Attempt (CVE-2018-15716)
- [x] ET EXPLOIT Outbound GPON Authentication Bypass Attempt (CVE-2018-10561)
- [x] ET EXPLOIT CVE-2018-8174 Common Construct B64 M1
- [x] ET EXPLOIT CVE-2018-8174 Common Construct B64 M2
- [x] ET EXPLOIT CVE-2018-8174 Common Construct B64 M3
- [x] ET EXPLOIT Possible LG SuperSign EZ CMS 2.5 RCE (CVE-2018-17173)
- [x] ET EXPLOIT Possible WePresent WIPG1000 OS Command Injection
- [x] ET EXPLOIT Possible WePresent WIPG1000 File Inclusion
- [x] ET EXPLOIT Possible ZyXEL P660HN-T v1 RCE (CVE-2017-18368)
- [x] ET EXPLOIT Possible Netgear DGN2200 RCE (CVE-2017-6077)
- [x] ET EXPLOIT Possible Netgear DGN2200 RCE (CVE-2017-6334)
- [x] ET EXPLOIT Possible Linksys WAP54Gv3 Remote Debug Root Shell Exploitation Attempt
- [x] ET EXPLOIT Possible Linksys WRT100/110 RCE Attempt (CVE-2013-3568)
- [x] ET EXPLOIT Possible ZTE ZXV10 H108L Router Root RCE Attempt
- [x] ET EXPLOIT Possible Linksys E1500/E2500 apply.cgi RCE Attempt
- [x] ET EXPLOIT Linksys E-Series Device RCE Attempt Outbound
- [x] ET EXPLOIT Unk.IoT IPCamera Exploit Attempt Inbound
- [x] ET EXPLOIT WinRAR WinAce Containing CVE-2018-20250 Inbound - Path Traversal leading to RCE
- [x] ET EXPLOIT Realtek SDK Miniigd UPnP SOAP Command Execution CVE-2014-8361 - Outbound
- [x] ET EXPLOIT Linksys Smart WiFi Information Disclosure Attempt Inbound
- [x] ET EXPLOIT CyberArk Enterprise Password Vault XXE Injection Attempt
- [x] ET EXPLOIT [NCC GROUP] Possible Bluekeep Inbound RDP Exploitation Attempt (CVE-2019-0708)
- [x] ET EXPLOIT Eir D1000 Remote Command Injection Attempt Inbound
- [x] ET EXPLOIT Eir D1000 Remote Command Injection Attempt Outbound
- [x] ET EXPLOIT Possible Exim 4.87-4.91 RCE Attempt Inbound (CVE-2019-10149)
- [x] ET EXPLOIT Attempted Remote Command Injection Outbound (CVE-2019-3929)
- [x] ET EXPLOIT Attempted Remote Command Injection Inbound (CVE-2019-3929)
- [x] ET EXPLOIT Possible OpenDreamBox Attempted Remote Command Injection Outbound
- [x] ET EXPLOIT Possible OpenDreamBox Attempted Remote Command Injection Inbound
- [x] ET EXPLOIT Attempted Remote Command Injection Outbound (CVE-2018-7841)
- [x] ET EXPLOIT Attempted Remote Command Injection Inbound (CVE-2018-7841)
- [x] ET EXPLOIT Dell KACE Attempted Remote Command Injection Outbound
- [x] ET EXPLOIT Dell KACE Attempted Remote Command Injection Inbound
- [x] ET EXPLOIT Geutebruck Attempted Remote Command Injection Outbound
- [x] ET EXPLOIT Geutebruck Attempted Remote Command Injection Inbound
- [x] ET EXPLOIT Hootoo TripMate Attempted Remote Command Injection Outbound
- [x] ET EXPLOIT Hootoo TripMate Attempted Remote Command Injection Inbound
- [x] ET EXPLOIT Belkin Wemo Enabled Crock-Pot Unauthenticated Command Injection Inbound (CVE-2019-12780)
- [x] ET EXPLOIT Belkin Wemo Enabled Crock-Pot Unauthenticated Command Injection Outbound (CVE-2019-12780)
- [x] ET EXPLOIT MiCasaVerde VeraLite - Remote Code Execution Outbound (CVE-2016-6255)
- [x] ET EXPLOIT MiCasaVerde VeraLite - Remote Code Execution Inbound (CVE-2016-6255)
- [x] ET EXPLOIT FCM-MB40 Attempted Remote Command Execution as Root
- [x] ET EXPLOIT Apache Struts 2 REST Plugin Vulnerability (CVE-2017-9805)
- [x] ET EXPLOIT Tomcat File Upload Payload Request (CVE-2017-12615)
- [x] ET EXPLOIT ThinkPHP Attempted Bypass and Payload Retrieval
- [x] ET EXPLOIT Possible Zoom Client Auto-Join (CVE-2019-13450)
- [x] ET EXPLOIT IE Scripting Engine Memory Corruption Vulnerability M1 (CVE-2019-0752)
- [x] ET EXPLOIT Possible Palo Alto SSL VPN sslmgr Format String Vulnerability (Inbound) (CVE-2019-1579)
- [x] ET EXPLOIT Possible WebShell GIF Upload
- [x] ET EXPLOIT Possible WebShell JPEG Upload
- [ ] ET EXPLOIT Possible VXWORKS Urgent11 RCE Attempt - Urgent Flag
- [ ] ET EXPLOIT Possible VXWORKS Urgent11 RCE Attempt - Illegal Urgent Flag
- [x] ET EXPLOIT Possible Inbound Flash Exploit (CVE-2018-15982)
- [x] ET EXPLOIT Possible Inbound Flash Exploit with Stack-Based wininet
- [x] ET EXPLOIT NETGEAR R7000/R6400 - Command Injection Inbound (CVE-2019-6277)

- [x] ET EXPLOIT NETGEAR R7000/R6400 - Command Injection Outbound (CVE-2019-6277)
- [x] ET EXPLOIT FortiOS SSL VPN - Pre-Auth Messages Payload Buffer Overflow (CVE-2018-13381)
- [x] ET EXPLOIT FortiOS SSL VPN - Remote Code Execution (CVE-2018-13383)
- [x] ET EXPLOIT D-Link Router DNS Changer Exploit Attempt
- [x] ET EXPLOIT DSLink 260E Router DNS Changer Exploit Attempt
- [x] ET EXPLOIT TOTOLINK Router DNS Changer Exploit Attempt
- [x] ET EXPLOIT Possible EXIM RCE Inbound (CVE-2019-15846) M2
- [x] ET EXPLOIT HiSilicon DVR - Buffer Overflow in Builtin Web Server
- [x] ET EXPLOIT HiSilicon DVR - Default Application Backdoor Password
- [x] ET EXPLOIT vBulletin 5.x Unauthenticated Remote Code Execution (CVE-2019-16759) M1
- [x] ET EXPLOIT vBulletin 5.x Unauthenticated Remote Code Execution (CVE-2019-16759) M2
- [x] ET EXPLOIT VMware VeloCloud Authorization Bypass (CVE-2019-5533)
- [x] ET EXPLOIT Observed Orange LiveBox Router Information Leakage Attempt (CVE-2018-20377)
- [x] ET EXPLOIT Yachtcontrol Webservers RCE CVE-2019-17270 (Inbound)
- [x] ET EXPLOIT Technicolor TD5130v2/TD5336 Router RCE CVE-2019-118396/CVE-2017-14127 (Inbound)
- [x] ET EXPLOIT Possible AVCON6 Video Conferencing System RCE (Inbound)
- [x] ET EXPLOIT Enigma Network Management Systems v65.0.0 CVE-2019-16072 (Inbound)
- [x] ET EXPLOIT Possible Sar2HTML plotting tool for Linux servers v3.2.1 (Inbound)
- [x] ET EXPLOIT NetGain Systems Enterprise Manager CVE-2017-16602 (Inbound)
- [x] ET EXPLOIT Citrix NetScaler SD-WAN 9.1.2.26.561201 Devices CVE-2017-6316 (Inbound)
- [x] ET EXPLOIT Thomson Reuters Velocity Analytics Vhayu Analytic Servers 6.94 build 2995 CVE-2013-5912 (Inbound)
- [x] ET EXPLOIT ACTi ASOC 2200 Web Configurators versions <2.6 RCE (Inbound)
- [x] ET EXPLOIT 3Com Office Connect Remote Code Execution (Inbound)
- [x] ET EXPLOIT Barracuda Spam Firewall 3.3.x RCE 2006-4000 (Inbound)
- [x] ET EXPLOIT CCBill Online Payment Systems RCE (Inbound)
- [x] ET EXPLOIT Possible Citrix Application Delivery Controller Arbitrary Code Execution Attempt (CVE-2019-19781)
- [x] ET EXPLOIT Linear eMerge E3 Unauthenticated Command Injection Outbound (CVE-2019-7256)
- [x] ET EXPLOIT Possible Citrix Application Delivery Controller Arbitrary Code Execution Attempt (CVE-2019-19781) M2
- [x] ET EXPLOIT [401TRG] GhostCat LFI Attempt Inbound (CVE-2020-1938)
- [x] ET EXPLOIT Zyxel NAS RCE Attempt Inbound (CVE-2020-9054) M2
- [x] ET EXPLOIT Linksys WRT54G Version 3.1 Command Injection Attempt
- [x] ET EXPLOIT Possible Telerik UI CVE-2019-18935 File Upload Attempt M2
- [x] ET EXPLOIT Multiple DrayTek Products Pre-authentication Remote RCE Inbound (CVE-2020-8515) M1
- [x] ET EXPLOIT Multiple DrayTek Products Pre-authentication Remote RCE Inbound (CVE-2020-8515) M2
- [x] ET EXPLOIT IBM Data Risk Manager Remote Code Execution via NMAP Scan
- [x] ET EXPLOIT IBM Data Risk Manager Authentication Bypass - Password Retrieval
- [x] ET EXPLOIT Possible IBM Data Risk Manager Authentication Bypass - Password Retrieval
- [x] ET EXPLOIT FortiOS SSL VPN - Information Disclosure (CVE-2018-13379)
- [x] ET EXPLOIT FortiOS SSL VPN - Improper Authorization Vulnerability (CVE-2018-13382)
- [x] ET EXPLOIT Pulse Secure SSL VPN - Arbitrary File Read (CVE-2019-11510)
- [x] ET EXPLOIT ARG-W4 ASDL Router DNS Changer Exploit Attempt
- [x] ET EXPLOIT Secutech Router DNS Changer Exploit Attempt
- [x] ET EXPLOIT Possible EXIM RCE Inbound (CVE-2019-15846)
- [x] ET EXPLOIT HiSilicon DVR - Application Credential Disclosure (CVE-2018-9995)
- [x] ET EXPLOIT HiSilicon DVR - Default Telnet Root Password Inbound
- [x] ET EXPLOIT DLink DNS 320 Remote Code Execution (CVE-2019-16057)
- [x] ET EXPLOIT Possible EXIM DoS (CVE-2019-16928)
- [x] ET EXPLOIT vBulletin 5.x Unauthenticated Remote Code Execution (CVE-2019-16759) M3
- [x] ET EXPLOIT Possible rConfig 3.9.2 Remote Code Execution PoC M1 (CVE-2019-16662)
- [x] ET EXPLOIT Yachtcontrol Webservers RCE CVE-2019-17270 (Outbound)
- [x] ET EXPLOIT Technicolor TD5130v2/TD5336 Router RCE CVE-2019-118396/CVE-2017-14127 (Outbound)
- [x] ET EXPLOIT Possible AVCON6 Video Conferencing System RCE (Outbound)
- [x] ET EXPLOIT Enigma Network Management Systems v65.0.0 CVE-2019-16072 (Outbound)
- [x] ET EXPLOIT Possible Sar2HTML plotting tool for Linux servers v3.2.1 (Outbound)
- [x] ET EXPLOIT NetGain Systems Enterprise Manager CVE-2017-16602 (Outbound)
- [x] ET EXPLOIT Citrix NetScaler SD-WAN 9.1.2.26.561201 Devices CVE-2017-6316 (Outbound)
- [x] ET EXPLOIT Thomson Reuters Velocity Analytics Vhayu Analytic Servers 6.94 build 2995 CVE-2013-5912 (Outbound)
- [x] ET EXPLOIT ACTi ASOC 2200 Web Configurators versions <2.6 RCE (Outbound)
- [x] ET EXPLOIT 3Com Office Connect Remote Code Execution (Outbound)
- [x] ET EXPLOIT Barracuda Spam Firewall 3.3.x RCE 2006-4000 (Outbound)
- [x] ET EXPLOIT CCBill Online Payment Systems RCE (Outbound)
- [x] ET EXPLOIT TP-LINK Archer C5 v4 (CVE-2019-7405)
- [x] ET EXPLOIT Linear eMerge E3 Unauthenticated Command Injection Inbound (CVE-2019-7256)
- [x] ET EXPLOIT Netgear DGN1000/DGN2200 Unauthenticated Command Execution Outbound
- [x] ET EXPLOIT Possible Microsoft SQL RCE Attempt (CVE-2020-0618)
- [x] ET EXPLOIT Zyxel NAS RCE Attempt Inbound (CVE-2020-9054) M1
- [x] ET EXPLOIT Zoho ManageEngine Desktop Central RCE Inbound (CVE-2020-10189)
- [x] ET EXPLOIT Possible Telerik UI CVE-2019-18935 File Upload Attempt M1
- [x] ET EXPLOIT Multiple DrayTek Products Pre-authentication Remote RCE Outbound (CVE-2020-8515) M1
- [x] ET EXPLOIT Multiple DrayTek Products Pre-authentication Remote RCE Outbound (CVE-2020-8515) M2
- [x] ET EXPLOIT Netlink GPON Remote Code Execution Attempt (Inbound)
- [x] ET EXPLOIT IBM Data Risk Manager Authentication Bypass - Session ID Assignment (set)
- [x] ET EXPLOIT Possible IBM Data Risk Manager Authentication Bypass - Session ID Assignment
- [x] ET EXPLOIT IBM Data Risk Manager Arbitrary File Download Attempt

- [x] ET EXPLOIT Possible iOS MobileMail OOB Write/Heap Overflow Exploit Email (Inbound)
- [x] ET EXPLOIT Possible iOS MobileMail OOB Write/Heap Overflow Exploit Email (Inbound)
- [x] ET EXPLOIT Possible iOS MobileMail OOB Write/Heap Overflow Exploit Email (Inbound)
- [x] ET EXPLOIT Possible iOS MobileMail OOB Write/Heap Overflow Exploit Email (Inbound)
- [x] ET EXPLOIT Possible SaltStack Authentication Bypass CVE-2020-11651 M2
- [x] ET EXPLOIT Netis E1+ 1.2.32533 - Unauthenticated WiFi Password Leak
- [x] ET EXPLOIT Image Manager 5.2.4 - RCE Attempt
- [x] ET EXPLOIT Possible MPC Sharj 3.11.1 - Arbitrary File Download Attempt
- [x] ET EXPLOIT Possible Oracle WebLogic CVE-2020-2551 Scanning
- [x] ET EXPLOIT QNAP PhotoStation Privilege Escalation Attempt M1 (encrypted token)
- [x] ET EXPLOIT QNAP PhotoStation Privilege Escalation Attempt M2 (plaintext token)
- [x] ET EXPLOIT UCM6202 1.0.18.13 - Remote Command Injection Attempt
- [x] ET EXPLOIT Authenticated QuickBox CE 2.5.5/Pro 2.1.8 RCE Attempt Inbound M1 (CVE-2020-13448)
- [x] ET EXPLOIT Possible WordPress Plugin BBPress 2.5 - Unauthenticated Priv Esc Attempt (CVE-2020-13693)
- [x] ET EXPLOIT Possible Successful VMware Cloud Director RCE Attempt (CVE-2020-3956)
- [x] ET EXPLOIT Attempted Directory Traversal via HTTP Cookie (CVE-2020-9484)
- [x] ET EXPLOIT Multiple Router RCE Routersploit
- [x] ET EXPLOIT Technicolor TD5130.2 - Remote Command Execution
- [x] ET EXPLOIT Fastweb Fastgate 0.00.81 - Remote Code Execution
- [x] ET EXPLOIT Netis WF2419 2.2.36123 - Remote Code Execution CVE-2019-19356
- [x] ET EXPLOIT Wireless IP Camera (P2) WIFICAM Remote Code Execution
- [x] ET EXPLOIT Mi Router 3 Remote Code Execution CVE-2018-13023
- [x] ET EXPLOIT LG SuperSign EZ CMS 2.5 Remote Code Execution CVE-2018-17173
- [x] ET EXPLOIT VMware Spring Cloud Directory Traversal (CVE-2020-5405)
- [x] ET EXPLOIT Centreon 20.04 Authenticated RCE (CVE-2020-12688)
- [x] ET EXPLOIT AnyDesk UDP Discovery Format String (CVE-2020-13160)
- [ ] ET EXPLOIT Possible CVE-2020-11897 IPv6 deprecated RH Type 0 source routing attack
- [ ] ET EXPLOIT Possible CVE-2020-11900 IP-in-IP tunnel Double-Free
- [ ] ET EXPLOIT Possible CVE-2020-11910 anomalous ICMPv4 type 3,code 4 Path MTU Discovery
- [x] ET EXPLOIT F5 TMUI RCE vulnerability CVE-2020-5902 Attempt M1
- [x] ET EXPLOIT Attempted HiSilicon DVR/NVR/IPCam RCE (Inbound)
- [x] ET EXPLOIT Potentially Malicious .cab Inbound (CVE-2020-1300)
- [x] ET EXPLOIT AVTECH Authenticated Command Injection in CloudSetup.cgi (Outbound)
- [x] ET EXPLOIT Possible Windows DNS Integer Overflow Attempt M1 (CVE-2020-1350)
- [x] ET EXPLOIT Possible SAP NetWeaver CVE-2020-6287 Probe
- [x] ET EXPLOIT Possible SAP NetWeaver CVE-2020-6287 Exploit Attempt
- [x] ET EXPLOIT Cisco ASA/Firepower Unauthenticated File Read (CVE-2020-3452) M1
- [x] ET EXPLOIT Possible iOS MobileMail OOB Write/Heap Overflow Exploit Email (Inbound)
- [x] ET EXPLOIT Possible iOS MobileMail OOB Write/Heap Overflow Exploit Email (Inbound)
- [x] ET EXPLOIT Possible iOS MobileMail OOB Write/Heap Overflow Exploit Email (Inbound)
- [x] ET EXPLOIT Possible Saltstack Authentication Bypass CVE-2020-11651 M1
- [x] ET EXPLOIT Online Scheduling System 1.0 - Authentication Bypass Attempt
- [x] ET EXPLOIT NEC SL2100 - Session Enumeration Attempt
- [x] ET EXPLOIT BlogEngine 3.3 - syndication.axd XXE Injection Attempt
- [x] ET EXPLOIT Attempted D-Link ShareCenter (DNS-320/325) RCE (Inbound)
- [x] ET EXPLOIT Complaint Management System 1.0 - Authentication Bypass Attempt
- [x] ET EXPLOIT QNAP PhotoStation Pre-Auth Local File Disclosure Attempt
- [x] ET EXPLOIT QNAP PhotoStation Authenticated Session Tampering Attempt
- [ ] ET EXPLOIT Possible DNS BIND TSIG Denial of Service Attempt (CVE-2020-8617)
- [x] ET EXPLOIT Authenticated QuickBox CE 2.5.5/Pro 2.1.8 RCE Attempt Inbound M2 (CVE-2020-13448)
- [x] ET EXPLOIT Possible VMware Cloud Director RCE Attempt (CVE-2020-3956)
- [x] ET EXPLOIT Possible Zephyr RTOS ICMPv4 Stack Buffer Overflow
- [x] ET EXPLOIT OpenMRS Deserialization Vulnerability CVE-2018-19276
- [x] ET EXPLOIT Edimax Technology EW-7438RPn-v3 Mini 1.27 - Remote Code Execution
- [x] ET EXPLOIT Xfinity Gateway - Remote Code Execution
- [x] ET EXPLOIT Multiple DLink Routers Remote Code Execution CVE-2019-16920
- [x] ET EXPLOIT Cisco AnyConnect Path Traversal Priv Esc (CVE-2020-3153)
- [x] ET EXPLOIT ASUS RT-N56U/RT-AC66U Remote Code Execution
- [x] ET EXPLOIT Mi TV Integration Remote Code Execution CVE-2018-16130
- [x] ET EXPLOIT Possible D-Link Command Injection Attempt Inbound (CVE-2020-13782)
- [x] ET EXPLOIT VMware Spring Cloud Directory Traversal (CVE-2020-5410)
- [ ] ET EXPLOIT GnuTLS Cryptographic Flaw Observed (CVE-2020-13777)
- [ ] ET EXPLOIT Possible CVE-2020-11896/CVE-2020-11898 Fragments inside IP-in-IP tunnel
- [ ] ET EXPLOIT Possible CVE-2020-11899 Multicast out-of-bound read
- [ ] ET EXPLOIT Possible CVE-2020-11902 ICMPv4 parameter problem with tunnel inside
- [ ] ET EXPLOIT Possible CVE-2020-1191 anomalous ICMPv4 Address Mask Reply message (type 18, code 0)
- [x] ET EXPLOIT F5 TMUI RCE vulnerability CVE-2020-5902 Attempt M2
- [x] ET EXPLOIT Attempted HiSilicon DVR/NVR/IPCam RCE (Outbound)
- [x] ET EXPLOIT Possible Authenticated Command Injection Inbound - Comtrend VR-3033 (CVE-2020-10173)
- [x] ET EXPLOIT Possible Windows DNS Integer Overflow Attempt M2 (CVE-2020-1350)
- [x] ET EXPLOIT SAP NetWeaver AS Directory Traversal Attempt Inbound (CVE-2020-6286)
- [x] ET EXPLOIT Possible SAP NetWeaver CVE-2020-6287 Vulnerable Response
- [x] ET EXPLOIT Possible SAP NetWeaver CVE-2020-6287 Exploit Success
- [x] ET EXPLOIT Cisco ASA/Firepower Unauthenticated File Read (CVE-2020-3452) M2

- [x] ET EXPLOIT Cisco ASA/Firepower Unauthenticated File Read (CVE-2020-3452) M3
- [x] ET EXPLOIT Attempted Netgear Buffer Overflow into RCE Inbound M1
- [x] ET EXPLOIT TeamViewer .tvs iFrame Observed (CVE-2020-13699)
- [x] ET EXPLOIT Apache2 Memory Corruption Inbound (CVE-2020-9490)
- [x] ET EXPLOIT vBulletin 5.6.2 widget_tabbedContainer_tab_panel Remote Code Execution (Inbound)
- [x] ET EXPLOIT Possible Zerologon Phase 1/3 - NetrServerReqChallenge with 0x00 Client Challenge (CVE-2020-1472)
- [ ] ET EXPLOIT [401TRG] Possible Zerologon (CVE-2020-1472) M2
- [x] ET EXPLOIT Possible Mida eFramework RCE Attempt Inbound (CVE-2020-15922)
- [x] ET EXPLOIT Qualcomm QCMAP Command Injection Attempt Inbound (CVE-2020-3657)
- [x] ET EXPLOIT Qualcomm QCMAP NULL Pointer Dereference Attempt Inbound (CVE-2020-25858)
- [x] ET EXPLOIT Possible Citrix Authentication Bypass Attempt Inbound (CVE-2020-8193)
- [x] ET EXPLOIT Ruckus vRIoT Command Injection Attempt Inbound (CVE-2020-26878)
- [x] ET EXPLOIT InoERP 0.7.2 Unauthenticated Remote Code Execution (Outbound)
- [x] ET EXPLOIT TikiWiki CMS Authentication Bypass (Forced Blank Admin Pass) Attempt Inbound (CVE-2020-15906)
- [x] ET EXPLOIT OpenMRS Deserialization Vulnerability CVE-2018-19276 M2
- [x] ET EXPLOIT Joomla RCE (JDatabaseDriverMysqli) M2
- [x] ET EXPLOIT Possible SolarWinds Orion API Local File Disclosure (SWNetPerfMon.db) (CVE-2020-10148)
- [x] ET EXPLOIT SaltStack Salt Exploitation Inbound (CVE-2020-16846)
- [x] ET EXPLOIT Microsoft Exchange Server Exploitation (CVE-2020-17141)
- [x] ET EXPLOIT [401TRG] DeDeCMS RFI Attempt
- [x] ET EXPLOIT Possible TerraMaster TOS RCE Inbound (CVE-2020-28188 CVE-2020-35665)
- [x] ET EXPLOIT VisualDoor Sonicwall SSL VPN Exploit Attempt
- [x] ET EXPLOIT Zimbra <8.8.11 - XML External Entity Injection/SSRF Attempt (CVE-2019-9621)
- [x] ET EXPLOIT Possible OpenSMTPD RCE Inbound (CVE-2020-7247)
- [x] ET EXPLOIT Inbound VMware vCenter RCE Attempt M2 (CVE-2021-21972)
- [x] ET EXPLOIT Inbound VMware vCenter RCE Attempt M3 (CVE-2021-21972)
- [x] ET EXPLOIT Inbound Hashicorp Consul RCE via Services API
- [x] ET EXPLOIT ARG-W4 ASDL Router DNS Changer Exploit Attempt M2
- [x] ET EXPLOIT Netgear ProSAFE Plus Unauthenticated RCE Inbound (CVE-2020-26919)
- [x] ET EXPLOIT Possible NSDP (Netgear) Unauthenticated Buffer Overflow (CVE-2020-35232)
- [x] ET EXPLOIT Possible NSDP (Netgear) Unauthenticated Write Access to DHCP Config (CVE-2020-35226)
- [x] ET EXPLOIT Netgear ProSAFE Plus Possible Integer Overflow Attempt Inbound M2 (CVE-2020-35230)
- [x] ET EXPLOIT Possible NSDP (Netgear) Write Command Buffer Overflow Attempt - 0x0005 (CVE-2020-35225)
- [x] ET EXPLOIT VMWare View Planner RCE (CVE-2021-21978) Attempt M2
- [x] ET EXPLOIT ZTE Cable Modem RCE Attempt (CVE-2014-2321)
- [x] ET EXPLOIT Yealink RCE Attempt (CVE-2021-27561)
- [x] ET EXPLOIT [NCC/FOX-IT] Possible F5 BIG-IP/BIG-IQ iControl REST RCE Attempt (CVE-2021-22986)
- [x] ET EXPLOIT DD-WRT UPNP Unauthenticated Buffer Overflow (CVE-2021-27137)
- [x] ET EXPLOIT [401TRG] ZeroShell RCE Inbound (CVE-2019-12725)
- [x] ET EXPLOIT Attempted Netgear Buffer Overflow into RCE Inbound M2
- [x] ET EXPLOIT Possible Pulse Secure VPN RCE Inbound (CVE-2020-8218)
- [x] ET EXPLOIT vBulletin 5.6.2 widget_tabbedContainer_tab_panel Remote Code Execution (Outbound)
- [x] ET EXPLOIT Possible Cisco Jabber RCE Inbound (CVE-2020-3495)
- [x] ET EXPLOIT Possible Zerologon NetrServerAuthenticate with 0x00 Client Credentials (CVE-2020-1472)
- [x] ET EXPLOIT [401TRG] HPDM Backdoor Login
- [x] ET EXPLOIT Possible MobileIron RCE Attempt Inbound (CVE-2020-15505)
- [x] ET EXPLOIT Qualcomm QCMAP Stack-Based Buffer Overflow Attempt Inbound (CVE-2020-3657)
- [x] ET EXPLOIT Possible Jira User Enumeration Attempts (CVE-2020-14181)
- [x] ET EXPLOIT Possible Citrix Information Disclosure Attempt Inbound (CVE-2020-8195)
- [x] ET EXPLOIT Ruckus vRIoT Authentication Bypass Attempt Inbound (CVE-2020-26879)
- [x] ET EXPLOIT InoERP 0.7.2 Unauthenticated Remote Code Execution (Inbound)
- [x] ET EXPLOIT Nexus Repository Manager EL Injection to RCE Inbound (CVE-2020-10204)
- [x] ET EXPLOIT 401TRG Liferay RCE (CVE-2020-7961)
- [x] ET EXPLOIT Possible SolarWinds Orion API Local File Disclosure (web.config) (CVE-2020-10148)
- [x] ET EXPLOIT Silver Peak Unity Orchestrator Exploitation Inbound (CVE-2020-12146)
- [x] ET EXPLOIT Microsoft Exchange Server Exploitation Inbound (CVE-2020-17132)
- [ ] ET EXPLOIT Possible NTFS Index Attribute Corruption Vulnerability
- [x] ET EXPLOIT Oracle WebLogic JNDI Injection RCE Attempt (CVE-2021-2109)
- [x] ET EXPLOIT Possible Zend Framework Exploit (CVE-2021-3007)
- [x] ET EXPLOIT Suspected SAP EEM SOLMAN RCE (CVE-2020-6207)
- [x] ET EXPLOIT PHP-CGI Query String Parameter Vuln Inbound (CVE-2012-2311)
- [x] ET EXPLOIT Inbound VMware vCenter RCE Attempt M1 (CVE-2021-21972)
- [x] ET EXPLOIT Inbound VMware vCenter RCE Attempt with Untrusted SSH Key Upload (CVE-2021-21972)
- [x] ET EXPLOIT Inbound VMware vCenter RCE Attempt M4 (CVE-2021-21972)
- [x] ET EXPLOIT DNS Change Attempt (Unknown Device)
- [x] ET EXPLOIT D-Link DI-804HV DNS Changer Exploit Attempt
- [x] ET EXPLOIT Possible NSDP (Netgear) Remote Authentication Bypass with Factory Reset (CVE-2020-35231)
- [x] ET EXPLOIT Netgear ProSAFE Plus Stored XSS Inbound (CVE-2020-35228)
- [x] ET EXPLOIT Netgear ProSAFE Plus Possible Integer Overflow Attempt Inbound M1 (CVE-2020-35230)
- [x] ET EXPLOIT Possible NSDP (Netgear) Write Command Buffer Overflow Attempt - 0x0003 (CVE-2020-35225)
- [x] ET EXPLOIT Possible NSDP (Netgear) Write Command Buffer Overflow Attempt - 0x000a (CVE-2020-35225)
- [x] ET EXPLOIT VMWare View Planner RCE (CVE-2021-21978) Attempt M1
- [x] ET EXPLOIT F5 BIG-IP iControl REST Unauthenticated RCE Inbound (CVE-2021-22986)
- [x] ET EXPLOIT Possible F5 BIG-IP Infoleak and Out-of-Bounds Write Inbound (CVE-2021-22991)
- [x] ET EXPLOIT Possible Vantage Velocity Field Unit RCE Inbound (CVE-2020-9020)
- [ ] ET EXPLOIT Windows DNS Server RCE Attempt Inbound (CVE-2021-26877)

- [x] ET EXPLOIT Windows DNS Server RCE Attempt Inbound (CVE-2021-26897)
- [x] ET EXPLOIT Possible Zyxel Authentication Bypass Inbound (CVE-2021-3297)
- [x] ET EXPLOIT Mitsubishi Electric smartRTU RCE Inbound (CVE-2019-14931)
- [x] ET EXPLOIT Klog Server Command Injection Inbound (CVE-2021-3317)
- [x] ET EXPLOIT Advantech iView RCE Setup via Config Overwrite Inbound (CVE-2021-22652)
- [x] ET EXPLOIT ZBL EPON ONU Broadband Router Remote Privilege Escalation Inbound M2
- [x] ET EXPLOIT Possible Local Active Directory Federation Services (AD FS) Replication Attempt
- [x] ET EXPLOIT Exim receive_msg Integer Overflow Attempt Inbound M1 (CVE-2020-28020)
- [x] ET EXPLOIT Exim New-Line Injection into Spool Header File Inbound M1 (CVE-2020-28021)
- [x] ET EXPLOIT Exim New-Line Injection into Spool Header File Inbound - Information Disclosure Attempt (CVE-2020-28021)
- [x] ET EXPLOIT [FIREEYE] Suspicious Pulse Secure HTTP Request (CVE-2021-22893) M1
- [x] ET EXPLOIT [FIREEYE] Suspicious Pulse Secure HTTP Request (CVE-2021-22893) M3
- [x] ET EXPLOIT QNAP MusicStation Pre-Auth RCE Inbound (CVE-2020-36197)
- [x] ET EXPLOIT Laravel Remote Code Execution (CVE-2021-3129) Inbound - Attempt to clear logs
- [x] ET EXPLOIT Laravel Remote Code Execution (CVE-2021-3129) Outbound - Attempt to clear logs
- [x] ET EXPLOIT Cisco RV320/RV325 Command Injection Attempt Inbound (CVE-2019-1652)
- [x] ET EXPLOIT Successful Cisco RV320/RV325 Config Disclosure (CVE-2019-1653)
- [x] ET EXPLOIT Successful Cisco RV320/RV325 Debug Dump Disclosure (CVE-2019-1653)
- [x] ET EXPLOIT Solr DataImport Handler RCE (CVE-2019-0193)
- [x] ET EXPLOIT Jboss RCE (CVE-2017-12149)
- [x] ET EXPLOIT ForgeRock Access Manager RCE (CVE-2021-35464)
- [x] ET EXPLOIT Unknown Vulnerability Exploit Attempt (Possible Mirai Activity)
- [x] ET EXPLOIT OptiLink ONT1GEW GPON RCE Outbound
- [x] ET EXPLOIT Cisco HyperFlex HX RCE Outbound (CVE-2021-1498)
- [x] ET EXPLOIT Trenda Router AC11 RCE Outbound (CVE-2021-31755)
- [x] ET EXPLOIT UDP Technology Firmware (IP Cam) - certmngr.cgi RCE via Command Injection Attempt Inbound (CVE-2021-33544)
- [x] ET EXPLOIT UDP Technology Firmware (IP Cam) - factory.cgi RCE via Command Injection Attempt Inbound (CVE-2021-33544)
- [x] ET EXPLOIT UDP Technology Firmware (IP Cam) - language.cgi RCE via Command Injection Attempt Inbound (CVE-2021-33544)
- [x] ET EXPLOIT UDP Technology Firmware (IP Cam) - oem.cgi RCE via Command Injection Attempt Inbound (CVE-2021-33544)
- [x] ET EXPLOIT UDP Technology Firmware (IP Cam) - simple_reclistjs.cgi RCE via Command Injection Attempt Inbound (CVE-2021-33544)
- [x] ET EXPLOIT UDP Technology Firmware (IP Cam) - testcmd.cgi RCE via Command Injection Attempt Inbound (CVE-2021-33544)
- [x] ET EXPLOIT UDP Technology Firmware (IP Cam) - tmpapp.cgi RCE via Command Injection Attempt Inbound (CVE-2021-33544)
- [x] ET EXPLOIT UDP Technology Firmware (IP Cam) - Auth Bypass Attempt Inbound (CVE-2021-33543)
- [x] ET EXPLOIT UDP Technology Firmware (IP Cam) - Possible Stack Buffer Overflow Attempt Inbound (Multiple CVE IDs)
- [x] ET EXPLOIT [ConnectWise CRU] Potential Sonicwall SMA Authentication Bypass (management) (CVE-2021-20016)
- [x] ET EXPLOIT [ConnectWise CRU] Potential Sonicwall SMA User-Level Authentication Bypass (portal) (CVE-2021-20016)
- [ ] ET EXPLOIT Possible OpenSSL TLSv1.2 DoS Inbound (CVE-2021-3449)
- [x] ET EXPLOIT Trend Micro IWSVA Unauthenticated Command Injection Inbound (CVE-2020-8466)
- [x] ET EXPLOIT Mitsubishi Electric smartRTU RCE Outbound (CVE-2019-14931)
- [x] ET EXPLOIT ScadaBR RCE with JSP Shell Inbound (CVE-2021-26828)
- [x] ET EXPLOIT ZBL EPON ONU Broadband Router Remote Privilege Escalation Inbound M1
- [x] ET EXPLOIT ZBL EPON ONU Broadband Router Remote Privilege Escalation - Responding with Superuser Credentials
- [x] ET EXPLOIT Microsoft Exchange RCE Setup Inbound (CVE-2021-28482)
- [x] ET EXPLOIT Exim receive_msg Integer Overflow Attempt Inbound M2 (CVE-2020-28020)
- [x] ET EXPLOIT Exim New-Line Injection into Spool Header File Inbound M2 (CVE-2020-28021)
- [x] ET EXPLOIT Exim Stack Exhaustion via BDAT Error Inbound (CVE-2020-28019)
- [x] ET EXPLOIT [FIREEYE] Suspicious Pulse Secure HTTP Request (CVE-2021-22893) M2
- [x] ET EXPLOIT Windows HTTP Protocol Stack UAF/RCE (CVE-2021-31166), http.sys DOS (CVE-2022-21907) Inbound
- [x] ET EXPLOIT Possible SolarWinds Orion RCE Inbound (CVE-2021-31474)
- [x] ET EXPLOIT Laravel Remote Code Execution (CVE-2021-3129) Inbound - Payload Execution Attempt
- [x] ET EXPLOIT Laravel Remote Code Execution (CVE-2021-3129) Outbound - Payload Execution Attempt
- [x] ET EXPLOIT Cisco RV320/RV325 Config Disclosure Attempt Inbound (CVE-2019-1653)
- [x] ET EXPLOIT Cisco RV320/RV325 Debug Dump Disclosure Attempt Inbound (CVE-2019-1653)
- [x] ET EXPLOIT Mongo-Express RCE Inbound (CVE-2019-10758)
- [x] ET EXPLOIT XXL-Job RCE
- [x] ET EXPLOIT Atlassian Jira Unauth User Enumeration Attempt (CVE-2020-36289)
- [x] ET EXPLOIT Unknown Command Injection Attempt Inbound (Possible Mirai Activity)
- [x] ET EXPLOIT OptiLink ONT1GEW GPON RCE Inbound
- [x] ET EXPLOIT Cisco HyperFlex HX RCE Inbound (CVE-2021-1498)
- [x] ET EXPLOIT Trenda Router AC11 RCE Inbound (CVE-2021-31755)
- [x] ET EXPLOIT UDP Technology Firmware (IP Cam) - certmngr.cgi RCE via Command Injection Attempt Outbound (CVE-2021-33544)
- [x] ET EXPLOIT UDP Technology Firmware (IP Cam) - factory.cgi RCE via Command Injection Attempt Outbound (CVE-2021-33544)
- [x] ET EXPLOIT UDP Technology Firmware (IP Cam) - language.cgi RCE via Command Injection Attempt Outbound (CVE-2021-33544)
- [x] ET EXPLOIT UDP Technology Firmware (IP Cam) - oem.cgi RCE via Command Injection Attempt Outbound (CVE-2021-33544)
- [x] ET EXPLOIT UDP Technology Firmware (IP Cam) - simple_reclistjs.cgi RCE via Command Injection Attempt Outbound (CVE-2021-33544)
- [x] ET EXPLOIT UDP Technology Firmware (IP Cam) - testcmd.cgi RCE via Command Injection Attempt Outbound (CVE-2021-33544)
- [x] ET EXPLOIT UDP Technology Firmware (IP Cam) - tmpapp.cgi RCE via Command Injection Attempt Outbound (CVE-2021-33544)
- [x] ET EXPLOIT UDP Technology Firmware (IP Cam) - Auth Bypass Attempt Outbound (CVE-2021-33543)
- [x] ET EXPLOIT UDP Technology Firmware (IP Cam) - Possible Stack Buffer Overflow Attempt Outbound (Multiple CVE IDs)
- [x] ET EXPLOIT IE MSHTML Out-of-Bounds Write Inbound (CVE-2021-33742)
- [x] ET EXPLOIT [ConnectWise CRU] Potential Sonicwall SMA User-Level Authentication Bypass (sslvpnclient) (CVE-2021-20016)
- [x] ET EXPLOIT [ConnectWise CRU] Potential Sonicwall SRA SQLi (CVE-2019-7481)

- [x] ET EXPLOIT Stored XSS Vulnerability CVE-2021-31250 M1
- [x] ET EXPLOIT Stored XSS Vulnerability CVE-2021-31250 M2
- [x] ET EXPLOIT Stored XSS Vulnerability CVE-2021-31250 M3
- [x] ET EXPLOIT Stored XSS Vulnerability CVE-2021-31250 M4
- [x] ET EXPLOIT Stored XSS and Webpass IoT devices CVE-2021-31643
- [x] ET EXPLOIT CHIYU IoT Devices - Denial of Service
- [x] ET EXPLOIT Cisco Data Center Network Manager Authentication Bypass Inbound (CVE-2019-15976)
- [x] ET EXPLOIT Cisco Data Center Network Manager Information Disclosure Inbound
- [x] ET EXPLOIT Cisco Data Center Network Manager SQL Injection Inbound (CVE-2019-15984)
- [x] ET EXPLOIT Cisco Data Center Network Manager Directory Traversal Inbound (CVE-2019-15980)
- [x] ET EXPLOIT Possible Cisco Data Center Network Manager - Log Retrieval (CVE-2019-1622)
- [x] ET EXPLOIT Possible Cisco Data Center Network Manager - Authenticated File Upload (CVE-2019-1620)
- [x] ET EXPLOIT Possible Cisco Data Center Network Manager - Unauthenticated File Upload (CVE-2019-1620)
- [x] ET EXPLOIT Possible CloudMe Sync Stack-based Buffer Overflow Inbound (CVE-2018-6892)
- [ ] ET EXPLOIT Possible Dovecot Memory Corruption Inbound (CVE-2019-11500)
- [x] ET EXPLOIT LibreOffice pydoc RCE Inbound (CVE-2018-16858)
- [x] ET EXPLOIT Sunhillo SureLine Unauthenticated OS Command Injection Inbound (CVE-2021-36380)
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (BeanShell1/Click1/CommonsCollections1/CommonsCollections4) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (BeanShell1/Click1/CommonsCollections1/CommonsCollections4) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (BeanShell1/Click1/CommonsCollections1/CommonsCollections4) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (Clojure1) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (Clojure1) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (Clojure1) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections1/CommonsCollections3) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections1/CommonsCollections3) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections1/CommonsCollections3) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections5/MozillaRhino1/Vaadin) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections5/MozillaRhino1/Vaadin) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections5/MozillaRhino1/Vaadin) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections6) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections6) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections6) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections7) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections7) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (CommonsCollections7) M3
- [ ] ET EXPLOIT ysoserial Payload in HTTP URI (Groovy1) M1
- [ ] ET EXPLOIT ysoserial Payload in HTTP URI (Groovy1) M2
- [ ] ET EXPLOIT ysoserial Payload in HTTP URI (Groovy1) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (Hibernate1/Hibernate2/JSON1/Myfaces1/ROME/URLDNS) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (Hibernate1/Hibernate2/JSON1/Myfaces1/ROME/URLDNS) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (Hibernate1/Hibernate2/JSON1/Myfaces1/ROME/URLDNS) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (JavassistWeld1) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (JavassistWeld1) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (JavassistWeld1) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (JBossInterceptors1) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (JBossInterceptors1) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (JBossInterceptors1) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (Jdk7u21) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (Jdk7u21) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (Jdk7u21) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (JRMPClient) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (JRMPClient) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (JRMPClient) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (MozillaRhino2) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (MozillaRhino2) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (MozillaRhino2) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (Spring1/Spring2) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (Spring1/Spring2) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP URI (Spring1/Spring2) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (BeanShell1/Click1/CommonsCollections1/CommonsCollections4) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (BeanShell1/Click1/CommonsCollections1/CommonsCollections4) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (BeanShell1/Click1/CommonsCollections1/CommonsCollections4) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (Clojure1) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (Clojure1) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (Clojure1) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections1/CommonsCollections3) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections1/CommonsCollections3) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections1/CommonsCollections3) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections5/MozillaRhino1/Vaadin) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections5/MozillaRhino1/Vaadin) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections5/MozillaRhino1/Vaadin) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections6) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections6) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections6) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections7) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections7) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (CommonsCollections7) M3
- [ ] ET EXPLOIT ysoserial Payload in HTTP Header (Groovy1) M1
- [ ] ET EXPLOIT ysoserial Payload in HTTP Header (Groovy1) M2
- [ ] ET EXPLOIT ysoserial Payload in HTTP Header (Groovy1) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (Hibernate1/Hibernate2/JSON1/Myfaces1/ROME/URLDNS) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (Hibernate1/Hibernate2/JSON1/Myfaces1/ROME/URLDNS) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (Hibernate1/Hibernate2/JSON1/Myfaces1/ROME/URLDNS) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (JavassistWeld1) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (JavassistWeld1) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (JavassistWeld1) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (JBossInterceptors1) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (JBossInterceptors1) M2

- [x] ET EXPLOIT ysoserial Payload in HTTP Header (JBossInterceptors1) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (Jdk7u21) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (Jdk7u21) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (Jdk7u21) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (JRMPClient) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (JRMPClient) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (JRMPClient) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (MozillaRhino2) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (MozillaRhino2) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (MozillaRhino2) M3
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (Spring1/Spring2) M1
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (Spring1/Spring2) M2
- [x] ET EXPLOIT ysoserial Payload in HTTP Header (Spring1/Spring2) M3
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (BeanShell1/Click1/CommonsCollections1/CommonsCollections4) M1
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (BeanShell1/Click1/CommonsCollections1/CommonsCollections4) M2
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (BeanShell1/Click1/CommonsCollections1/CommonsCollections4) M3
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Clojure1) M1
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Clojure1) M2
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Clojure1) M3
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (CommonsCollections1/CommonsCollections3) M1
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (CommonsCollections1/CommonsCollections3) M2
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (CommonsCollections1/CommonsCollections3) M3
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (CommonsCollections5/MozillaRhino1/Vaadin) M1
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (CommonsCollections5/MozillaRhino1/Vaadin) M2
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (CommonsCollections5/MozillaRhino1/Vaadin) M3
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (CommonsCollections6) M1
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (CommonsCollections6) M2
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (CommonsCollections6) M3
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (CommonsCollections7) M1
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (CommonsCollections7) M2
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (CommonsCollections7) M3
- [ ] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Groovy1) M1
- [ ] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Groovy1) M2
- [ ] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Groovy1) M3
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Hibernate1/Hibernate2/JSON1/Myfaces1/ROME/URLDNS) M1
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Hibernate1/Hibernate2/JSON1/Myfaces1/ROME/URLDNS) M2
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Hibernate1/Hibernate2/JSON1/Myfaces1/ROME/URLDNS) M3
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (JavassistWeld1) M1
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (JavassistWeld1) M2
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (JavassistWeld1) M3
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (JBossInterceptors1) M1
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (JBossInterceptors1) M2
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (JBossInterceptors1) M3
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Jdk7u21) M1
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Jdk7u21) M2
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Jdk7u21) M3
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (JRMPClient) M1
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (JRMPClient) M2
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (JRMPClient) M3
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (MozillaRhino2) M1
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (MozillaRhino2) M2
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (MozillaRhino2) M3
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Spring1/Spring2) M1
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Spring1/Spring2) M2
- [x] ET EXPLOIT HTTP POST Request With ysoserial In Request Body (Spring1/Spring2) M3
- [x] ET EXPLOIT Monitorr 1.7.6m RCE Exploit Attempt
- [x] ET EXPLOIT Jenkins Plugin Script RCE Exploit Attempt (CVE-2019-1003001)
- [x] ET EXPLOIT Apache Ambari Default Credentials Attempt
- [x] ET EXPLOIT Jitsi Meet Plugin XSS Attempt (CVE-2021-26812)
- [x] ET EXPLOIT GraphQL Introspection Query Attempt
- [x] ET EXPLOIT JCK Editor 6.4.4 SQLi Attempt (CVE-2018-17254)
- [x] ET EXPLOIT TIBCO Data Virtualization <= 8.3 RCE Attempt (CVE-2016-2510)
- [x] ET EXPLOIT Smart Google Code Inserter < 3.5 Auth Bypass (CVE-2018-3810)
- [x] ET EXPLOIT Smart Google Code Inserter < 3.5 SQLi (CVE-2018-3811)
- [x] ET EXPLOIT rConfig < 3.9.7 SQLi (CVE-2020-10546)
- [x] ET EXPLOIT phpMyAdmin setup.php Local File Include
- [x] ET EXPLOIT Apache Cocoon <= 2.1.x LFI (CVE-2020-11991)
- [x] ET EXPLOIT Paypal Pro < 1.1.65 SQLi (CVE-2020-14092)
- [x] ET EXPLOIT [PwnedPiper] Exploitation Attempt - Small Malformed Translogic Packet (Multiple CVEs)
- [x] ET EXPLOIT [PwnedPiper] Exploitation Attempt - Large Malformed Translogic Packet (CVE-2021-37164)
- [x] ET EXPLOIT Microsoft Exchange Pre-Auth Path Confusion M1 (CVE-2021-31207)
- [x] ET EXPLOIT Microsoft Exchange Pre-Auth Path Confusion M2 (CVE-2021-31207)
- [x] ET EXPLOIT Vulnerable Microsoft Exchange Server Response (CVE-2021-31207)
- [x] ET EXPLOIT Possible Microsoft Exchange RCE Inbound M1 (CVE-2021-34473)
- [x] ET EXPLOIT Microsoft Exchange SUID Disclosure via SSRF Inbound M1 (CVE-2021-31207)
- [x] ET EXPLOIT Possible Microsoft Exchange RCE Inbound M2 (CVE-2021-34473)

- [x] ET EXPLOIT Possible Microsoft Exchange RCE with Python PSRP Client UA Inbound (CVE-2021-34473)
- [x] ET EXPLOIT Fortinet FortiWeb OS Command Injection Inbound M1 (CVE-2021-22123)
- [x] ET EXPLOIT Possible Pulse Secure VPN RCE Chain Stage 1 Inbound - Request Config Backup (CVE-2020-8260)
- [x] ET EXPLOIT Possible Pulse Secure VPN RCE Chain Stage 3 Inbound - Execute Mal Config Trigger (CVE-2020-8260)
- [x] ET EXPLOIT Possible Microsoft Exchange ProxyLogon Activity - OABVirtualDirectory SetObject (CVE-2021-27065)
- [x] ET EXPLOIT vCenter Server RCE Chain Final Stage Inbound (CVE-2021-21985)
- [x] ET EXPLOIT Genexis PLATINUM 4410 Command Injection Inbound (CVE-2021-29003)
- [x] ET EXPLOIT Microsoft Edge Chakra - InjectJsBuiltInLibraryCode Use-After-Free Inbound (CVE-2019-0568)
- [x] ET EXPLOIT Microsoft Edge Chakra - InlineArrayPush Type Confusion Inbound M1 (CVE-2018-8617)
- [x] ET EXPLOIT Prestashop Orderfiles Module Arbitrary File Upload
- [x] ET EXPLOIT Microsoft Exchange - Information Disclosure flowbit set (CVE-2021-33766)
- [x] ET EXPLOIT Microsoft Exchange - InboxRules.svc Access Observed Following Successful ProxyToken Attack
- [x] ET EXPLOIT Possible Realtek SDK - formWlSiteSurvey Stack Buffer Overflow Inbound (CVE-2021-35393)
- [x] ET EXPLOIT Realtek SDK - Command Injection Inbound (CVE-2021-35395)
- [x] ET EXPLOIT Possible Realtek SDK - formWlanMultipleAP Stack Buffer Overflow Inbound (CVE-2021-35393)
- [x] ET EXPLOIT TOTOLINK Router Cross-site Scripting CVE-2021-34228 (boafrm) M1
- [x] ET EXPLOIT TOTOLINK Router Cross-site Scripting CVE-2021-34228 (boafrm) M3
- [x] ET EXPLOIT WebSVN 2.6.0 OS Command Injection Inbound (CVE-2021-32305)
- [x] ET EXPLOIT Possible JNBridge Java Deserialization Attempt M1
- [x] ET EXPLOIT Possible JNBridge Java Deserialization Attempt M2
- [x] ET EXPLOIT Possible JNBridge Java Deserialization Attempt M3
- [x] ET EXPLOIT Possible Mirai Infection Attempt via OS Command Injection Inbound (CVE-2021-32305)
- [x] ET EXPLOIT Possible SolarWinds Serv-U SSH RCE Inbound M2 (CVE-2021-35211)
- [x] ET EXPLOIT Possible ImageMagick Malformed SVG Upload Leading to RCE
- [x] ET EXPLOIT PiHole Web Interface Regex Escape Leading to RCE Inbound M2 (CVE-2021-32706)
- [x] ET EXPLOIT Microsoft OMI RCE Exploit Attempt (CVE-2021-38647) M2
- [x] ET EXPLOIT Netgear Seventh Inferno Vulnerability (fake packet upload)
- [x] ET EXPLOIT JBOSS Deserialization Attempt Inbound (CVE-2017-7504)
- [x] ET EXPLOIT Cisco ASA XSS Attempt (CVE-2020-3580)
- [x] ET EXPLOIT Fortinet FortiOS/FortiProxy SSL VPN Web Portal Path Traversal (CVE-2018-13379)
- [x] ET EXPLOIT Nagios XI Post-Auth Path Traversal (CVE-2021-37343)
- [x] ET EXPLOIT VMware vCenter RCE Exploitation Attempt M2 (CVE-2021-22005)
- [x] ET EXPLOIT Cisco HyperFlex OS Command Injection M2 (CVE-2021-1497)
- [x] ET EXPLOIT Apache HTTP Server 2.4.49 - Path Traversal Attempt (CVE-2021-41773) M1
- [x] ET EXPLOIT Apache HTTP Server 2.4.49 - Path Traversal Attempt (CVE-2021-41773) M3
- [x] ET EXPLOIT Possible Atlassian Confluence Pre-Authorization Arbitrary File Read Attempt (seraph-config.xml) (CVE-2021-26085)
- [ ] ET EXPLOIT Microsoft Windows VBScript Engine VbsErase Memory Corruption (CVE-2019-0667)
- [x] ET EXPLOIT Fortinet FortiWeb OS Command Injection Inbound M2 (CVE-2021-22123)
- [x] ET EXPLOIT Possible Pulse Secure VPN RCE Chain Stage 2 Inbound - Upload Malicious Config (CVE-2020-8260)
- [x] ET EXPLOIT Pulse Secure VPN RCE Chain Stage 3 Inbound - Execute Mal Config Trigger, PoC Based (CVE-2020-8260)
- [x] ET EXPLOIT vCenter Server RCE Chain Initial Stage Inbound (CVE-2021-21985)
- [x] ET EXPLOIT eMerge E3 Command Injection Inbound (CVE-2019-7256)
- [x] ET EXPLOIT Unknown Target Application Command Injection Inbound
- [ ] ET EXPLOIT Use-After-Free in QuickTimePluginReplacement (CVE-2021-1879)
- [x] ET EXPLOIT Microsoft Edge Chakra - NewScObjectNoCtor InitProtoType Confusion Inbound (CVE-2019-0567)
- [x] ET EXPLOIT Prestashop Supercheckout Module Arbitrary File Upload
- [x] ET EXPLOIT Microsoft Exchange - Successful msExchEcpCanary Disclosure (CVE-2021-33766)
- [x] ET EXPLOIT Possible Realtek SDK - formRebootCheck/formWsc Stack Buffer Overflow Inbound (CVE-2021-35392)
- [x] ET EXPLOIT Realtek SDK - Command Execution/Backdoor Access Inbound (CVE-2021-35395)
- [x] ET EXPLOIT Possible Realtek SDK - formStaticDHCP Stack Buffer Overflow Inbound (CVE-2021-35393)
- [x] ET EXPLOIT Possible Realtek SDK - Stack Buffer Overflow via UPnP SUBSCRIBE Callback Header Inbound (CVE-2021-35393)
- [x] ET EXPLOIT TOTOLINK Router Cross-site Scripting CVE-2021-34228 (boafrm) M2
- [x] ET EXPLOIT TOTOLINK Router Cross-site Scripting CVE-2021-34228 (boafrm) M4
- [x] ET EXPLOIT Possible JNBridge Java Deserialization Attempt (Wide) M1
- [x] ET EXPLOIT Possible JNBridge Java Deserialization Attempt (Wide) M2
- [x] ET EXPLOIT Possible JNBridge Java Deserialization Attempt (Wide) M3
- [x] ET EXPLOIT Possible Mirai Infection Attempt via OS Command Injection Outbound (CVE-2021-32305)
- [x] ET EXPLOIT Possible SolarWinds Serv-U SSH RCE Inbound M1 (CVE-2021-35211)
- [x] ET EXPLOIT Cisco HyperFlex HX Data Platform Pre-Auth RCE Inbound (CVE-2021-1499)
- [x] ET EXPLOIT PiHole Web Interface Regex Escape Leading to RCE Inbound M1 (CVE-2021-32706)
- [x] ET EXPLOIT Microsoft OMI RCE Exploit Attempt (CVE-2021-38647) M1
- [x] ET EXPLOIT Netgear Seventh Inferno CVE-2021-41314 (new line injection)
- [x] ET EXPLOIT Netgear Seventh Inferno Vulnerability (post-auth shell injection)
- [x] ET EXPLOIT WP Download From Files Plugin <= 1.48 Arbitrary File Upload Attempt
- [x] ET EXPLOIT Microsoft Edge Chakra - InlineArrayPush Type Confusion Inbound M2 (CVE-2018-8617)
- [x] ET EXPLOIT Pulse Secure Post-Auth OS Command Injection (CVE-2019-11539)
- [x] ET EXPLOIT Possible Citrix ShareFile RCE Inbound (CVE-2021-22941)
- [x] ET EXPLOIT Cisco HyperFlex OS Command Injection M1 (CVE-2021-1497)
- [x] ET EXPLOIT File Sharing Wizard 1.5.0 - SEH Overflow Inbound (CVE-2019-16724)
- [x] ET EXPLOIT Apache HTTP Server 2.4.49 - Path Traversal Attempt (CVE-2021-41773) M2
- [x] ET EXPLOIT Possible Atlassian Confluence Pre-Authorization Arbitrary File Read Attempt (web.xml) (CVE-2021-26085)
- [x] ET EXPLOIT Possible Atlassian Confluence Pre-Authorization Arbitrary File Read Attempt (pom.properties) (CVE-2021-26085)

- [x] ET EXPLOIT Possible Atlassian Confluence Pre-Authorization Arbitrary File Read Attempt (pom.xml) (CVE-2021-26085)
- [x] ET EXPLOIT Possible EyesOfNetwork Remote File Upload with PHP WebShell Inbound (CVE-2021-27513)
- [x] ET EXPLOIT RUIJIE NBR/RGNBR Command Injection Attempt Inbound M2
- [x] ET EXPLOIT Apache HTTP Server - Path Traversal Attempt (CVE-2021-42013) M2
- [ ] ET EXPLOIT Oracle BI Publisher Authentication Bypass (CVE-2019-2616)
- [x] ET EXPLOIT Discourse SNS Webhook RCE Inbound (CVE-2021-41163)
- [x] ET EXPLOIT Amcrest Camera and NVR Buffer Overflow Attempt (CVE-2020-5735)
- [x] ET EXPLOIT Apache Solr RCE via Velocity Template M2 (CVE-2019-17558)
- [x] ET EXPLOIT Confluence Server Path Traversal Vulnerability (CVE-2019-3398)
- [x] ET EXPLOIT Cisco ASA and Firepower Path Traversal Vulnerability M2 (CVE-2020-3452)
- [x] ET EXPLOIT PHP Melody v3.0 SQL Injection Attempt
- [x] ET EXPLOIT Cisco RV320/RV325 RCE (CVE-2019-1653)
- [x] ET EXPLOIT D-Link DIR-825 R1 Web Interface RCE (CVE-2020-29557)
- [x] ET EXPLOIT EyesOfNetwork Cookie SQLi (CVE-2020-9465)
- [x] ET EXPLOIT EyesOfNetwork Autodiscover Command Injection (CVE-2020-8654)
- [x] ET EXPLOIT GoCD Authentication Bypass URI Path - add-on
- [ ] ET EXPLOIT Vanguard v2.1 (Search) POST Inject Web Vulnerability
- [x] ET EXPLOIT ManageEngine AdSelfService Plus - Arbritrary File Upload Attempt (CVE-2021-40539)
- [x] ET EXPLOIT ManageEngine AdSelfService Plus - Possible Code Execution via openSSLTool (CVE-2021-40539)
- [x] ET EXPLOIT Possible Engineers Online Portal System Webshell Upload (CVE-2021-42669)
- [x] ET EXPLOIT Possible Gitlab CE/EE Image Parser RCE Inbound (CVE-2021-22205)
- [ ] ET EXPLOIT Ultimate POS 4.4 Cross-Site Scripting (XSS) - Outbound
- [x] ET EXPLOIT Guangzhou 1GE ONU OS Command Execution (CVE-2020-8958)
- [x] ET EXPLOIT Possible Tenda OS Command Injection (CVE-2020-10987) (POST)
- [x] ET EXPLOIT Kaseya VSA ManagedITSync SQL Injection (CVE-2017-18362)
- [x] ET EXPLOIT UPnP UUID Password Change Exploit Attempt Inbound - R6700V3 PoC Gadgets (CVE-2021-34991)
- [x] ET EXPLOIT .NET Framework Remote Code Execution Injection (CVE-2020-1147)
- [x] ET EXPLOIT Microsoft Exchange Create User Configuration - xbit set 2 (CVE-2021-42321)
- [x] ET EXPLOIT Possible FatPipe Unrestricted File Upload
- [x] ET EXPLOIT Nagios XI <= 5.6.5 Privesc (CVE-2019-15949)
- [x] ET EXPLOIT Possible Edgewater Networks Edgemarc Blind Command Injection Attempt (CVE-2017-6079)
- [x] ET EXPLOIT [CISA AA21-336A] Zoho ManageEngine ServiceDesk Possible Exploitation Activity (CVE-2021-44077)
- [x] ET EXPLOIT VMware vCenter Unauthorized File Read Inbound
- [x] ET EXPLOIT NodeBB Path Traversal (CVE-2021-43788)
- [x] ET EXPLOIT MS-Officecmd Remote Code Execution Attempt
- [x] ET EXPLOIT Hikvision IP Camera RCE Attempt (CVE-2021-36260)
- [x] ET EXPLOIT Apache log4j RCE Attempt (http rmi) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (tcp rmi) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (udp rmi) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (tcp dns) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (udp ldaps) (CVE-2021-44228)
- [x] ET EXPLOIT Aviatrix Controller Unrestricted File Upload with Path Traversal Inbound (CVE-2021-40870)
- [x] ET EXPLOIT RUIJIE NBR/RGNBR Command Injection Attempt Inbound M1
- [x] ET EXPLOIT Apache HTTP Server - Path Traversal Attempt (CVE-2021-42013) M1
- [x] ET EXPLOIT Apache HTTP Server - Path Traversal Attempt (Unassigned CVE)
- [x] ET EXPLOIT TerraMaster TOS RCE via OS Command Injection Inbound (CVE-2020-28188)
- [x] ET EXPLOIT Possible Apache Shiro 1.2.4 Cookie RememberME Deserial RCE (CVE-2016-4437)
- [x] ET EXPLOIT Apache Solr RCE via Velocity Template M1 (CVE-2019-17558)
- [x] ET EXPLOIT Furukawa Electric ConsciusMAP 2.8.1 Java Deserialization Remote Code Execution (CVE-2020-12133)
- [x] ET EXPLOIT Cisco ASA and Firepower Path Traversal Vulnerability M1 (CVE-2020-3452)
- [x] ET EXPLOIT PHP Melody v3.0 SQL Injection Attempt
- [x] ET EXPLOIT Cisco IP Phones Web Server Vulnerability (CVE-2020-3161)
- [x] ET EXPLOIT Citrix App Delivery Controller and Citrix Gateway M1 (CVE-2019-19781)
- [x] ET EXPLOIT DotNetNuke 9.2-9.2.2 Cookie Deserialization Exploit (CVE-2018-15811)
- [x] ET EXPLOIT EyesOfNetwork Generate API Key SQLi (CVE-2020-8656)
- [x] ET EXPLOIT IBM Data Risk Manager Arbitrary File Download (CVE-2020-4430)
- [x] ET EXPLOIT GoCD Authentication Bypass Successful Leak
- [x] ET EXPLOIT ManageEngine AdSelfService Plus - Authentication Bypass Attempt (CVE-2021-40539)
- [x] ET EXPLOIT ManageEngine AdSelfService Plus - .jsp WebShell Upload Attempt (CVE-2021-40539)
- [x] ET EXPLOIT Possible MovableTypePoC RCE Inbound (CVE-2021-20837)
- [x] ET EXPLOIT Possible Engineers Online Portal System Access Control Bypass (CVE-2021-42671)
- [x] ET EXPLOIT Attempted IDSVSE IP Camera RCE
- [ ] ET EXPLOIT Ultimate POS 4.4 Cross-Site Scripting (XSS) - Inbound
- [x] ET EXPLOIT Tenda OS Command Injection (CVE-2020-10987) (GET)
- [x] ET EXPLOIT D-Link HNAP SOAPAction Command Injection (CVE-2015-2051)
- [x] ET EXPLOIT UPnP UUID Password Change Exploit Attempt Inbound - XR300 PoC Gadgets (CVE-2021-34991)
- [x] ET EXPLOIT .NET Framework Remote Code Execution Injection (CVE-2020-0646)
- [x] ET EXPLOIT Microsoft Exchange Delete User Configuration - xbit set 1 (CVE-2021-42321)
- [x] ET EXPLOIT Possible Microsoft Exchange Server Remote Code Execution Inbound (CVE-2021-42321)
- [x] ET EXPLOIT FatPipe Unrestricted File Upload
- [x] ET EXPLOIT Apache HTTP Server SSRF (CVE-2021-40438)
- [x] ET EXPLOIT Netgear DGN Remote Code Execution
- [x] ET EXPLOIT IE Scripting Engine Memory Corruption Vulnerability M2 (CVE-2019-0752)
- [x] ET EXPLOIT VMware vCenter SSRF Inbound
- [ ] ET EXPLOIT Exiftool RCE Inbound (CVE-2021-22204)
- [x] ET EXPLOIT Grafana 8.x Path Traversal (CVE-2021-43798)
- [x] ET EXPLOIT Apache log4j RCE Attempt (http ldap) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (tcp ldap) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (udp ldap) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (udp dns) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (http dns) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (tcp ldaps) (CVE-2021-44228)

- [x] ET EXPLOIT Apache log4j RCE Attempt (http ldaps) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt - lower/upper UDP Bypass M1 (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (tcp iiop) (CVE-2021-44228)
- [ ] ET EXPLOIT Apache log4j RCE Attempt - 2021/12/13 Obfuscation Observed (udp) (CVE-2021-44228)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt - 2021/12/12 Obfuscation Observed M2 (udp) (CVE-2021-44228)
- [x] ET EXPLOIT TP-Link TL-WR840N EU v5 RCE Attempt (CVE-2021-41653)
- [x] ET EXPLOIT Apache log4j RCE Attempt - lower/upper TCP Bypass M2 (CVE-2021-44228)
- [ ] ET EXPLOIT Apache log4j RCE Attempt - 2021/12/12 Obfuscation Observed (tcp) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt - Nested lower (tcp) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt - Nested upper (tcp) (CVE-2021-44228)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt (tcp nis) (CVE-2021-44228)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt (tcp nds) (CVE-2021-44228)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt (tcp corba) (CVE-2021-44228)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt - Base64 jndi (tcp) (CVE-2021-44228)
- [x] ET EXPLOIT AjaxPro RCE Attempt (CVE-2021-23758)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt - Base64 jndi (tcp) (Outbound) (CVE-2021-44228)
- [ ] ET EXPLOIT Apache log4j RCE Attempt (http ldap) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (tcp ldap) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (udp ldap) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (udp dns) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (http dns) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (tcp ldaps) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Oracle Coherence Deserialization RCE (CVE-2020-2555)
- [x] ET EXPLOIT Apache log4j RCE Attempt - lower/upper UDP Bypass M1 (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (tcp iiop) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt (udp corba) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt (udp nds) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt (udp nis) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt - Nested upper (udp) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt - Nested lower (udp) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt - lower/upper UDP Bypass M2 (Outbound) (CVE-2021-44228)
- [ ] ET EXPLOIT Apache log4j RCE Attempt - 2021/12/13 Obfuscation Observed (udp) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt - 2021/12/13 Obfuscation Observed (tcp) (Outbound) (CVE-2021-44228)
- [ ] ET EXPLOIT Apache log4j RCE Attempt - 2021/12/12 Obfuscation Observed (udp) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt - lower/upper TCP Bypass M1 (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (udp iiop) (CVE-2021-44228)
- [ ] ET EXPLOIT Apache log4j RCE Attempt - 2021/12/13 Obfuscation Observed (tcp) (CVE-2021-44228)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt - 2021/12/12 Obfuscation Observed M2 (tcp) (CVE-2021-44228)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt - 2021/12/13 Obfuscation Observed (tcp) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt - AWS Access Key Disclosure (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt - lower/upper UDP Bypass M2 (CVE-2021-44228)
- [ ] ET EXPLOIT Apache log4j RCE Attempt - 2021/12/12 Obfuscation Observed (udp) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt - Nested lower (udp) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt - Nested upper (udp) (CVE-2021-44228)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt (udp nis) (CVE-2021-44228)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt (udp nds) (CVE-2021-44228)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt (udp corba) (CVE-2021-44228)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt - Base64 jndi (udp) (CVE-2021-44228)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt - Base64 jndi (udp) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Apache Obfuscated log4j RCE Attempt (tcp ldap) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (http rmi) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (tcp rmi) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (udp rmi) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (tcp dns) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (udp ldaps) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (http ldaps) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt - lower/upper TCP Bypass M1 (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt - 2021/12/12 Obfuscation Observed M2 (tcp) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt (udp iiop) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt (tcp corba) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt (tcp nds) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt (tcp nis) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt - Nested upper (tcp) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt - Nested lower (tcp) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt - lower/upper TCP Bypass M2 (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt - 2021/12/12 Obfuscation Observed M2 (udp) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Apache log4j RCE Attempt - AWS Access Key Disclosure (Outbound) (CVE-2021-44228)
- [ ] ET EXPLOIT Apache log4j RCE Attempt - 2021/12/12 Obfuscation Observed (tcp) (Outbound) (CVE-2021-44228)

- [ ] ET EXPLOIT Apache log4j RCE Attempt - 2021/12/13 Obfuscation Observed (tcp) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT Possible Joomla RCE (CVE-2011-5148)
- [x] ET EXPLOIT Qianxin Netcom NGFW Command Injection
- [x] ET EXPLOIT SonicWall SMA 100 Series - Possible Heap-Based Overflow Activity (CVE-2021-20043)
- [x] ET EXPLOIT OctoberCMS Auth Bypass Inbound M1 trigger_reset (CVE-2021-32648)
- [x] ET EXPLOIT Zoho ManagedEngine Desktop Central Authentication Bypass - File Upload Attempt (CVE-2021-44515)
- [ ] ET EXPLOIT GitLab Unauthenticated Remote ExifTool Command Injection (CVE-2021-24563)
- [x] ET EXPLOIT SolarWinds Web Help Desk Hard Coded Credentials Request (CVE-2021-35232)
- [x] ET EXPLOIT NodeJS System Information Library Command Injection Attempt (CVE-2021-21315)
- [x] ET EXPLOIT SonicWall SMA Stack-Based Buffer Overflow CVE-2021-20038 M1
- [x] ET EXPLOIT SonicWall SMA Authenticated Command Injection Attempt CVE-2021-20039
- [x] ET EXPLOIT Nagios XI OS Command Injection (CVE-2021-25297 & CVE-2021-25298)
- [x] ET EXPLOIT Apache Spark RPC - Unauthenticated RegisterApplication Request - RCE Attempt (CVE-2020-9480)
- [x] ET EXPLOIT Apache Struts RCE Attempt (CVE-2020-17530)
- [x] ET EXPLOIT Cisco REST API Container for Cisco IOS XE Software Authentication Bypass - Successful Exploit (CVE-2019-12643)
- [x] ET EXPLOIT Oracle WebLogic IIOP JNDI Injection (CVE-2020-14841)
- [x] ET EXPLOIT MetInfo 7.0 SQL Injection (CVE-2019-17418)
- [x] ET EXPLOIT Possible Apache Airflow DAG Example RCE Attempt - Create DAG (CVE-2020-11978)
- [x] ET EXPLOIT Citrix SD-WAN Unauthenticated RCE (CVE-2020-8271)
- [x] ET EXPLOIT VMware SD-WAN Orchestrator Path Traversal (CVE-2020-4000)
- [x] ET EXPLOIT Cisco Security Manager Path Traversal - athena (CVE-2020-27130)
- [x] ET EXPLOIT Possible Citrix Application Delivery Controller Arbitrary Code Execution Attempt (CVE-2019-19781) M4
- [x] ET EXPLOIT Citrix Application Delivery Controller Arbitrary Code Execution Attempt Scanner Attempt - Server Response (CVE-2019-19781)
- [x] ET EXPLOIT Cisco SD-WAN vManage Software Directory Traversal (CVE-2020-26073)
- [x] ET EXPLOIT Possible SAP ICM MPI Desynchronization Scanning Activity (CVE-2022-22536) M1
- [x] ET EXPLOIT Possible Moxa MxView RCE Attempt (CVE-2021-38454)
- [x] ET EXPLOIT Zerologon Phase 2/3 - NetrServerAuthenticate2 Request with 0x00 Client Challenge and Sign and Seal Disabled (CVE-2020-1472) M1
- [x] ET EXPLOIT Zerologon Phase 2/3 - NetrServerAuthenticate3 Request with 0x00 Client Challenge and Sign and Seal Disabled (CVE-2020-1472) M1
- [x] ET EXPLOIT Zerologon Phase 3/3 - Malicious NetrServerPasswordSet2 (CVE-2020-1472)
- [x] ET EXPLOIT Apache APISIX Admin API Authentication Bypass (CVE-2022-24112) M1
- [x] ET EXPLOIT Extensis Portfolio Unrestricted File Upload (CVE-2022-24252)
- [x] ET EXPLOIT CreateService via SMB to Reset-ComputerMachinePassword - Observed Post Zerologon Activity
- [x] ET EXPLOIT Linux/Attempted Hosts File Exfil
- [x] ET EXPLOIT Possible Apache log4j Uncontrolled Recursion Lookup (CVE-2021-45105)
- [x] ET EXPLOIT Possible ELEFANTE/ElephantBeetle WebShell Access Inbound
- [x] ET EXPLOIT SonicWall SMA 100 Series - Unauthenticated File Upload Path Traversal (CVE-2021-20040)
- [ ] ET EXPLOIT Windows Defender POWERLIKS Detection Bypass
- [x] ET EXPLOIT OctoberCMS Auth Bypass Inbound M2 set_password (CVE-2021-32648)
- [x] ET EXPLOIT Zoho ManagedEngine Desktop Central Authentication Bypass - Administrator Password Reset Attempt (CVE-2021-44515)
- [x] ET EXPLOIT Sonicwall Unauthenticated Stack-Based Buffer Overflow (CVE-2021-20038)
- [x] ET EXPLOIT Citrix ShareFile Storage Zones Controller RCE Attempt (CVE-2021-22941)
- [x] ET EXPLOIT Possible vRealize Operations Manager API SSRF Attempt (CVE-2021-21975)
- [x] ET EXPLOIT SonicWall SMA Stack-Based Buffer Overflow CVE-2021-20038 M2
- [x] ET EXPLOIT Nagios XI OS Command Injection (CVE-2021-25296)
- [x] ET EXPLOIT Apache Spark RPC - Unauthenticated RegisterApplication Request (CVE-2020-9480)
- [x] ET EXPLOIT Possible Apache ShardingSphere RCE Attempt (CVE-2020-1947) (PoC Based)
- [x] ET EXPLOIT Possible Cisco REST API Container for Cisco IOS XE Software Authentication Bypass Attempt (CVE-2019-12643)
- [x] ET EXPLOIT Cisco REST API Container for Cisco IOS XE Software Authentication Bypass - Token Usage (CVE-2019-12643)
- [x] ET EXPLOIT Sangoma Asterisk Originate AMI RCE (CVE-2019-18610) (PoC Based)
- [x] ET EXPLOIT MetInfo 7.0 SQL Injection (CVE-2019-16997)
- [x] ET EXPLOIT Possible Apache Airflow DAG Example RCE Attempt - Unpause (CVE-2020-11978)
- [x] ET EXPLOIT VMware SD-WAN Orchestrator Authentication Bypass (CVE-2020-4001)
- [x] ET EXPLOIT VMware SD-WAN Orchestrator SQL Injection (CVE-2020-3984)
- [x] ET EXPLOIT Cisco Security Manager Path Traversal - cwhp (CVE-2020-27130)
- [x] ET EXPLOIT Citrix Application Delivery Controller Arbitrary Code Execution Attempt Scanner Attempt (CVE-2019-19781)
- [x] ET EXPLOIT Cisco Viptela vManage Directory Traversal (CVE-2020-27128)
- [x] ET EXPLOIT Possible Microsoft Exchange Server OWA GetWacUrl Information Disclosure Attempt (CVE-2020-17143)
- [x] ET EXPLOIT Possible SAP ICM MPI Desynchronization Scanning Activity (CVE-2022-22536) M2
- [x] ET EXPLOIT Oracle Weblogic Server Deserialization RCE T3 (CVE-2015-4852)
- [x] ET EXPLOIT Zerologon Phase 2/3 - NetrServerAuthenticate2 Request with 0x00 Client Challenge and Sign and Seal Disabled (CVE-2020-1472) M2
- [x] ET EXPLOIT Zerologon Phase 2/3 - NetrServerAuthenticate3 Request with 0x00 Client Challenge and Sign and Seal Disabled (CVE-2020-1472) M2
- [x] ET EXPLOIT Zerologon Phase 3/3 - NetrLogonSamLogonWithFlags Request with 0x00 Client Credentials (CVE-2020-1472)
- [x] ET EXPLOIT Apache APISIX Admin API Authentication Bypass (CVE-2022-24112) M2
- [x] ET EXPLOIT TOTOLINK Realtek SDK RCE (CVE-2019-19824)
- [x] ET EXPLOIT Suspicious SVCCTL CreateService Command via SMB - Observed Zerologon Post Compromise Activity
- [x] ET EXPLOIT Zabbix v5.4.0 - 5.4.8 SSO/SALM Auth Bypass (CVE-2022-23131) M1

- [x] ET EXPLOIT Zabbix v5.4.0 - 5.4.8 SSO/SALM Auth Bypass (CVE-2022-23131) M2
- [x] ET EXPLOIT VMware Spring Cloud Gateway Code Injection (CVE-2022-22947) (set)
- [x] ET EXPLOIT Extreme Networks ExtremeWireless Aerohive HiveOS and IQ Engine (Log Poisoning) (CVE-2020-16152) M1
- [x] ET EXPLOIT Azure Automation Authentication Bypass
- [x] ET EXPLOIT Netgear R6260 Mini_httpd Buffer Overflow Attempt - Possible RCE (CVE-2021-34979)
- [x] ET EXPLOIT TerraMaster TOS Unauthenticated Command Injection Inbound M1 (CVE-2022-24989)
- [x] ET EXPLOIT TerraMaster TOS Information Leak Inbound (CVE-2022-24990)
- [x] ET EXPLOIT WatchGuard CVE-2022-26318 RCE Attempt M2
- [x] ET EXPLOIT Microsoft Exchange SUID Disclosure via SSRF Inbound M2 (CVE-2021-31207)
- [x] ET EXPLOIT Possible Microsoft Exchange Mailbox Enumeration Inbound (CVE-2021-34473)
- [x] ET EXPLOIT Possible SpringCore RCE/Spring4Shell Stage 1 Pattern Set Inbound (CVE-2022-22965)
- [x] ET EXPLOIT Possible SpringCore RCE/Spring4Shell Stage 3 Directory Set Inbound (CVE-2022-22965)
- [x] ET EXPLOIT Possible SpringCore RCE/Spring4Shell Inbound (CVE-2022-22965)
- [x] ET EXPLOIT Redis RCE Attempt (CVE-2022-0543) M1
- [x] ET EXPLOIT Possible Redis RCE Attempt - Dynamic Importing of liblua (CVE-2022-0543)
- [x] ET EXPLOIT Totolink - Command Injection Attempt Inbound (CVE-2022-26186)
- [x] ET EXPLOIT D-Link - RCE Attempt Inbound (CVE-2021-45382)
- [x] ET EXPLOIT Gitlab Login Attempt with hard-coded password (CVE-2022-1162)
- [x] ET EXPLOIT VMWare Server-side Template Injection RCE (CVE-2022-22954)
- [x] ET EXPLOIT Possible OpenSSL Infinite Loop Inducing Cert Inbound via TCP (CVE-2022-0778)
- [x] ET EXPLOIT Possible NGINX Reference LDAP Query Injection Attack
- [x] ET EXPLOIT SEOWON INTECH SLC-130/SLR-120S RCE Inbound M2 (CVE-2020-17456)
- [x] ET EXPLOIT D-Link DWR Command Injection Inbound (CVE-2018-10823)
- [ ] ET EXPLOIT Razer Sila Router - Command Injection Attempt Inbound (No CVE)
- [x] ET EXPLOIT Shenzhen TVT DVR/NVR/IPC WebUI RCE ADD Attempt
- [x] ET EXPLOIT Shenzhen TVT DVR/NVR/IPC Stack Overflow in Base64 Authorization Mechanism M1
- [x] ET EXPLOIT Shenzhen TVT DVR/NVR/IPC Hardcoded Credential ConfigSyncProc Login Attempt
- [x] ET EXPLOIT Shenzhen TVT DVR/NVR/IPC Hardcoded WebUI Login Attempt M2
- [x] ET EXPLOIT [ConnectWise CRU] Java ECDSA (Psychic) TLS Signature (CVE-2022-21449)
- [ ] ET EXPLOIT [ConnectWise CRU] Java ECDSA (Psychic) Signed JWT Bypass (CVE-2022-21449)
- [x] ET EXPLOIT dotCMS Arbitrary File Upload Attempt (CVE-2022-26352) M1
- [x] ET EXPLOIT F5 BIG-IP iControl REST Authentication Bypass (CVE-2022-1388) M1
- [x] ET EXPLOIT Sophos Firewall Authentication Bypass (CVE-2022-1040)
- [x] ET EXPLOIT Sophos Firewall Authentication Bypass (CVE-2022-1040) Server Response M2
- [x] ET EXPLOIT [Rapid7] Zyxel ZTP setWanPortSt mtu Parameter Exploit Attempt (CVE-2022-30525)
- [x] ET EXPLOIT Zabbix v5.4.0 - 5.4.8 SSO/SALM Auth Bypass (CVE-2022-23131) M3
- [x] ET EXPLOIT VMware Spring Cloud Gateway Code Injection (CVE-2022-22947)
- [x] ET EXPLOIT Extreme Networks ExtremeWireless Aerohive HiveOS and IQ Engine (LFI) (CVE-2020-16152) M2
- [x] ET EXPLOIT Possible Oracle Access Manager RCE Attempt (CVE-2021-35587)
- [x] ET EXPLOIT TP-LINK TL-WR840N RCE Inbound (CVE-2022-25064)
- [x] ET EXPLOIT TerraMaster TOS Unauthenticated Command Injection Inbound M2 (CVE-2022-24989)
- [x] ET EXPLOIT WatchGuard CVE-2022-26318 RCE Attempt M1
- [x] ET EXPLOIT Possible WatchGuard CVE-2022-26318 RCE Attempt M3
- [x] ET EXPLOIT Possible Microsoft Exchange RCE Inbound M3 (CVE-2021-34473)
- [x] ET EXPLOIT Possible Spring Cloud Connector RCE Inbound (CVE-2022-22963)
- [x] ET EXPLOIT Possible SpringCore RCE/Spring4Shell Stage 2 Suffix Set Inbound (CVE-2022-22965)
- [x] ET EXPLOIT Possible SpringCore RCE/Spring4Shell Stage 4 Prefix Set Inbound (CVE-2022-22965)
- [x] ET EXPLOIT NetGear R6700v3 upnpd Buffer Overflow Inbound (CVE-2022-27643)
- [x] ET EXPLOIT Redis RCE Attempt (CVE-2022-0543) M2
- [x] ET EXPLOIT Totolink - Command Injection Attempt Inbound (CVE-2022-26210)
- [x] ET EXPLOIT Totolink - Command Injection Attempt Inbound (CVE-2022-25075)
- [x] ET EXPLOIT Gitlab Login Attempt with hard-coded password (CVE-2022-1162)
- [x] ET EXPLOIT VMWare Server-side Template Injection RCE (CVE-2022-22954)
- [x] ET EXPLOIT VMWare Server-side Template Injection RCE (CVE-2022-22954)
- [x] ET EXPLOIT Possible OpenSSL Infinite Loop Inducing Cert Inbound via UDP (CVE-2022-0778)
- [x] ET EXPLOIT SEOWON INTECH SLC-130/SLR-120S RCE Inbound M1 (CVE-2020-17456)
- [x] ET EXPLOIT SEOWON INTECH SLC-130 RCE Inbound (No CVE)
- [x] ET EXPLOIT iRZ Mobile Router RCE Inbound M1 (CVE-2022-27226)
- [ ] ET EXPLOIT Razer Sila Router - LFI Attempt Inbound (No CVE)
- [x] ET EXPLOIT Shenzhen TVT DVR/NVR/IPC Hardcoded WebUI Login Attempt M1
- [x] ET EXPLOIT Shenzhen TVT DVR/NVR/IPC Stack Overflow in Base64 Authorization Mechanism M2
- [x] ET EXPLOIT Shenzhen TVT DVR/NVR/IPC Hardcoded Credential ConfigSyncProc System Details Request
- [x] ET EXPLOIT Shenzhen TVT DVR/NVR/IPC ConfigSyncProc RCE Attempt
- [ ] ET EXPLOIT WSO2 Server RCE (CVE-2022-29464)
- [x] ET EXPLOIT Possible VMware Workspace ONE Access RCE via Server-Side Template Injection Inbound (CVE-2022-22954)
- [x] ET EXPLOIT dotCMS Arbitrary File Upload Attempt (CVE-2022-26352) M2
- [x] ET EXPLOIT F5 BIG-IP iControl REST Authentication Bypass Server Response (CVE-2022-1388)
- [x] ET EXPLOIT Sophos Firewall Authentication Bypass (CVE-2022-1040) Server Response M1
- [x] ET EXPLOIT F5 BIG-IP iControl REST Authentication Bypass Attempt (CVE-2022-1388) M2
- [x] ET EXPLOIT Attempted ThinkPHP < 5.2.x RCE Inbound (CVE-2018-20062)

- [x] ET EXPLOIT Attempted ThinkPHP < 5.2.x RCE Outbound (CVE-2018-20062)
- [x] ET EXPLOIT Default Apache CouchDB Erlang Cookie Observed (CVE-2022-24706)
- [x] ET EXPLOIT Potential External VMware vRealize Automation Authentication Bypass Vulnerability
- [x] ET EXPLOIT WordPress Plugin video-synchro-pdf 1.7.4 - Local File Inclusion
- [x] ET EXPLOIT Local File Inclusion with Shell Execution via proc/self/environ
- [x] ET EXPLOIT Adobe ColdFusion 11 - LDAP Java Object Deserialization RCE (POST) CVE-2018-15957
- [x] ET EXPLOIT Zyxel NWA-1100-NH Command Injection Attempt (CVE-2021-4039)
- [x] ET EXPLOIT WordPress Plugin cab-fare-calculator 1.0.3 - Local File Inclusion
- [x] ET EXPLOIT Fuel CMS 1.4.1 RCE (CVE-2018-16763)
- [x] ET EXPLOIT Zhone ZNID GPON 2426A < S3.0.501 RCE (CVE-2014-9118) M2
- [x] ET EXPLOIT Bonitasoft Authorization Bypass M1 (CVE-2022-25237)
- [x] ET EXPLOIT Bonitasoft Authorization Bypass and RCE Upload M2 (CVE-2022-25237)
- [x] ET EXPLOIT Possible Zimbra Autodiscover Servlet XXE (CVE-2019-9670)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt - HTTP URI Obfuscation (CVE-2021-44228) (Inbound)
- [x] ET EXPLOIT Possible Microsoft Support Diagnostic Tool Exploitation Inbound (CVE-2022-30190)
- [x] ET EXPLOIT Possible ManageEngine ADAudit Plus Directory Traversal Leading to Deserialization
- [x] ET EXPLOIT Attempted VMware Authentication Bypass (CVE-2022-31656)
- [x] ET EXPLOIT Possible Zimbra RCE Attempt Inbound (CVE-2022-27925)
- [x] ET EXPLOIT Realtek eCos RSDK/MSDK Stack-based Buffer Overflow Attempt Inbound (CVE-2022-27255)
- [x] ET EXPLOIT Jira Server/Data Center 8.4.0 Remote File Read Attempt (CVE-2021-26086) M2
- [x] ET EXPLOIT Possible SAP NetWeaver SQL Injection Attempt Inbound (CVE-2016-2386)
- [x] ET EXPLOIT NetGear WNR2000v5 Buffer Overflow Attempt Inbound (CVE-2017-6862)
- [x] ET EXPLOIT D-Link Remote Code Execution Attempt (CVE-2022-28958)
- [x] ET EXPLOIT Dataprobe iBoot-PDU Pre-Auth Remote Code Execution Attempt via git-update.php (CVE-2022-3184) M1
- [ ] ET EXPLOIT Possible Zoho ManageEngine RCE Attempt Inbound (CVE-2022-35405)
- [x] ET EXPLOIT ZKBioSecurity SQL Injection Attempt (CVE-2022-36635)
- [x] ET EXPLOIT Possible Zimbra Arbitrary File Upload (CVE-2022-41352) M2
- [x] ET EXPLOIT Possible Zimbra Arbitrary File Upload (CVE-2022-41352) M3
- [x] ET EXPLOIT Possible Zimbra Arbitrary File Upload (CVE-2022-41352) M5
- [x] ET EXPLOIT Possible Zimbra Arbitrary File Upload (CVE-2022-41352) M8
- [x] ET EXPLOIT Possible Zimbra Arbitrary File Upload (CVE-2022-30333) M2
- [x] ET EXPLOIT Possible Apache Text4shell RCE Attempt Script Prefix (CVE-2022-42889) (Outbound)
- [x] ET EXPLOIT Possible Apache Text4shell RCE Attempt DNS Prefix (CVE-2022-42889) (Outbound)
- [x] ET EXPLOIT Possible Apache Text4shell RCE Attempt URL Prefix (CVE-2022-42889) (Outbound)
- [x] ET EXPLOIT Possible Apache Text4shell RCE Attempt JEXL Path (CVE-2022-42889) (Outbound)
- [x] ET EXPLOIT SolarView Compact Command Injection Inbound (CVE-2022-29303)
- [x] ET EXPLOIT Telesquare SDT-CW3B1 1.1.0 - OS Command Injection (CVE-2021-46422)
- [x] ET EXPLOIT Possible Microsoft Support Diagnostic Tool Exploitation Inbound (CVE-2022-30190)
- [x] ET EXPLOIT DBltek GoIP GoIP-1 GSM Gateway - Local File Inclusion
- [x] ET EXPLOIT Adobe ColdFusion 11 - LDAP Java Object Deserialization RCE (GET) CVE-2018-15957
- [x] ET EXPLOIT Scriptcase 9.7 Arbitrary File Upload Attempt
- [x] ET EXPLOIT Kramer VIAware Remote Code Execution (CVE-2021-35064 CVE-2021-36356)
- [x] ET EXPLOIT Archeevo 5.0 - Local File Inclusion
- [x] ET EXPLOIT Zhone ZNID GPON 2426A < S3.0.501 RCE (CVE-2014-9118) M1
- [x] ET EXPLOIT Bonitasoft Successful Default User Login Attempt (Possible Staging for CVE-2022-25237)
- [x] ET EXPLOIT Bonitasoft Authorization Bypass M2 (CVE-2022-25237)
- [x] ET EXPLOIT Bonitasoft Authorization Bypass and RCE Upload M1 (CVE-2022-25237)
- [ ] ET EXPLOIT Apache Tommcat/JBoss RCE Inbound (CVE-2013-4810)
- [x] ET EXPLOIT Possible Apache log4j RCE Attempt - HTTP URI Obfuscation (CVE-2021-44228) (Outbound)
- [x] ET EXPLOIT Attempted Mitel MiVoice Connect Data Validation RCE Inbound (CVE-2022-29499)
- [x] ET EXPLOIT Possible ManageEngine ADAudit Plus XXE (CVE-2022-28219)
- [x] ET EXPLOIT Possible Zavio IP Camera OS Command Injection Attempt Inbound (CVE-2013-2568)
- [x] ET EXPLOIT Attempted Schneider Electric SpaceLogic C-Bus Home Controller 5200WHC2 Remote Code Execution (CVE-2022-34753)
- [x] ET EXPLOIT Jira Server/Data Center 8.4.0 Remote File Read Attempt (CVE-2021-26086) M1
- [x] ET EXPLOIT PAN-OS OS Command Injecton Attempt Inbound (CVE-2020-2038)
- [x] ET EXPLOIT QNAP Photo Station Path Traversal Attempt Inbound (CVE-2019-7195)
- [ ] ET EXPLOIT D-Link Remote Code Execution Attempt (CVE-2022-26258)
- [x] ET EXPLOIT Atlassian Bitbucket CVE-2022-36804 Exploit Attempt
- [x] ET EXPLOIT Dataprobe iBoot-PDU Pre-Auth Remote Code Execution Attempt via git-update.php (CVE-2022-3184) M2
- [x] ET EXPLOIT Microsoft Exchange Remote Code Execution Attempt (CVE-2022-41040, CVE-2022-41082)
- [x] ET EXPLOIT Possible Zimbra Arbitrary File Upload (CVE-2022-41352) M1
- [x] ET EXPLOIT Possible Zimbra Arbitrary File Upload (CVE-2022-41352) M4
- [x] ET EXPLOIT Possible Zimbra Arbitrary File Upload (CVE-2022-41352) M6
- [x] ET EXPLOIT Possible Zimbra Arbitrary File Upload (CVE-2022-41352) M7
- [x] ET EXPLOIT Possible Zimbra Arbitrary File Upload (CVE-2022-30333) M1
- [x] ET EXPLOIT Possible Apache Text4shell RCE Attempt Script Prefix (CVE-2022-42889) (Inbound)
- [x] ET EXPLOIT Possible Apache Text4shell RCE Attempt DNS Prefix (CVE-2022-42889) (Inbound)
- [x] ET EXPLOIT Possible Apache Text4shell RCE Attempt URL Prefix (CVE-2022-42889) (Inbound)
- [x] ET EXPLOIT Possible Apache Text4shell RCE Attempt JEXL Path (CVE-2022-42889) (Inbound)
- [x] ET EXPLOIT Possible VMWare NSX Manager Remote Code Execution Exploit Attempt (CVE-2021-39144)

- [x] ET EXPLOIT Possible OpenSSL Punycode Email Address Buffer Overflow Attempt Inbound (CVE-2022-3602)
- [x] ET EXPLOIT GL iNet MTN300n Command Injection Attempt Inbound (CVE-2022-31898)
- [x] ET EXPLOIT Xiongmai/HiSilicon DVR - Request for Product Details Possible CVE-2017-7577 Exploit Attempt
- [x] ET EXPLOIT Xiongmai/HiSilicon DVR - OpenTelnet Inbound - Possilbe CVE-2020-22253 Attempt
- [x] ET EXPLOIT Xiongmai/HiSilicon DVR - Successful Telnet Opening - Successful CVE-2020-22253 Attempt
- [x] ET EXPLOIT Redfish Exploitation Attempt (CVE-2022-40259)
- [x] ET EXPLOIT Observed Mirai/Gafgyt Post Brute Force Activity (GET)
- [x] ET EXPLOIT Possible Cacti Unauthenticated RCE Inbound M1 (CVE-2022-46169)
- [x] ET EXPLOIT TIBCO JasperReports Directory Traversal Attempt (CVE-2018-18809)
- [x] ET EXPLOIT SugarCRM Auth Bypass Attempt 2022-12-31
- [x] ET EXPLOIT CentOS Control Web Panel Pre-Auth Remote Code Execution (CVE-2022-44877)
- [x] ET EXPLOIT ManageEngine Unauthenticated RCE Attempt M2 (CVE-2022-47966)
- [x] ET EXPLOIT Realtek SDK - Command Execution/Backdoor Access Inbound (CVE-2021-35394)
- [x] ET EXPLOIT Possible Oracle E-Business RCE Attempt Inbound M1 (CVE-2022-21587)
- [x] ET EXPLOIT Possible Oracle E-Business RCE Attempt Inbound M3 (CVE-2022-21587)
- [x] ET EXPLOIT VMWare ESXi 6.7.0 OpenSLP Remote Code Execution Attempt - Directory Agent Advertisement Heap Overflow (CVE-2021-21974)
- [x] ET EXPLOIT Possible ImageMagick (7.1.0-49) DOS PNG Observed Inbound (CVE-2022-44267)
- [x] ET EXPLOIT Fortra MFT Deserialization Remote Code Execution Attempt (CVE-2023-0669) M1
- [x] ET EXPLOIT Fortra MFT Deserialization Remote Code Execution Attempt (CVE-2023-0669) M3
- [x] ET EXPLOIT Sunlogin Sunflower Simplified 1.0.1.43315 Directory Traversal Attempt (CVE-2022-48323)
- [x] ET EXPLOIT Razer Sila Router - Command Injection Attempt Inbound (wget) (No CVE)
- [x] ET EXPLOIT Razer Sila Router - Command Injection Attempt Inbound (find) (No CVE)
- [x] ET EXPLOIT Razer Sila Router - LFI Attempt Inbound (passwd) (No CVE)
- [x] ET EXPLOIT pfBlockerNG HTTP Host Header Remote Code Execution Attempt (CVE-2022-31814)
- [x] ET EXPLOIT Possible Microsoft Outlook Elevation of Privilege Payload Observed M2 (CVE-2023-23397)
- [x] ET EXPLOIT Possible Microsoft Outlook Elevation of Privilege Payload Observed M4 (CVE-2023-23397)
- [x] ET EXPLOIT Possible Microsoft Outlook Elevation of Privilege Payload Observed M6 (CVE-2023-23397)
- [x] ET EXPLOIT Possible Microsoft Outlook Elevation of Privilege Payload Observed M8 (CVE-2023-23397)
- [x] ET EXPLOIT Apache log4j RCE Attempt (http) (Inbound) (CVE-2021-44228)
- [x] ET EXPLOIT ManageEngine Unauthenticated RCE Attempt M10 (CVE-2022-47966)
- [x] ET EXPLOIT ManageEngine Unauthenticated RCE Attempt M12 (CVE-2022-47966)
- [x] ET EXPLOIT Suspected cPanel XSS Exploit Activity (CVE-2023-29489)
- [x] ET EXPLOIT Ruckus Wireless Admin Remote Code Execution Attempt (CVE 2023-25717)
- [x] ET EXPLOIT Fortigate VPN - Repeated GET Requests to /remote/hostcheck_validate (CVE-2023-27997)
- [x] ET EXPLOIT Fortigate VPN - Repeated POST Requests to /remote/hostcheck_validate (CVE-2023-27997) M2
- [x] ET EXPLOIT Possible OpenSSL Punycode Email Address Buffer Overflow Attempt Outbound (CVE-2022-3602)
- [x] ET EXPLOIT D-Link Related Command Injection Attempt Inbound (CVE-2013-7471)
- [x] ET EXPLOIT Xiongmai/HiSilicon DVR - Request for User Details - Possible CVE-2017-7577 Exploit Attempt
- [x] ET EXPLOIT Xiongmai/HiSilicon DVR - Successful Auth - Possilbe CVE-2020-22253 Attempt
- [x] ET EXPLOIT Xiongmai/HiSilicon DVR - RTSP Buffer Overflow Attempt - CVE-2022-26259
- [x] ET EXPLOIT Redfish API User Enumeration Attempt (CVE-2022-2827)
- [x] ET EXPLOIT Microsoft Exchange Remote Code Execution Attempt - OWASSRF (CVE-2022-41040, CVE-2022-41082)
- [x] ET EXPLOIT Possible Cacti Unauthenticated RCE Inbound M2 (CVE-2022-46169)
- [x] ET EXPLOIT TIBCO JasperReports Authenticated Arbitrary File Read Attempt (CVE-2018-5430)
- [x] ET EXPLOIT SugarCRM PHP Shell Upload Attempt
- [x] ET EXPLOIT ManageEngine Unauthenticated RCE Attempt M1 (CVE-2022-47966)
- [x] ET EXPLOIT Lexmark Malicious File Upload Detected
- [x] ET EXPLOIT D-Link webupg Remote Code Execution Attempt Inbound (CVE 2021-46441, 2021-46442)
- [x] ET EXPLOIT Possible Oracle E-Business RCE Attempt Inbound M2 (CVE-2022-21587)
- [x] ET EXPLOIT Possible Oracle E-Business RCE Attempt Inbound M4 (CVE-2022-21587)
- [x] ET EXPLOIT Possible ImageMagick (7.1.0-49) DOS PNG Upload Attempt (CVE-2022-44267)
- [x] ET EXPLOIT Possible ImageMagick (7.1.0-49) Arbitrary Remote Leak PNG Upload Attempt (CVE-2022-44268)
- [x] ET EXPLOIT Fortra MFT Deserialization Remote Code Execution Attempt (CVE-2023-0669) M2
- [x] ET EXPLOIT GitLab Pre-Auth RCE Detected (CVE-2021-22205)
- [x] ET EXPLOIT Fortinet FortiNAC - Observed POST .zip with Vulnerable Parameter (CVE-2022-39952)
- [x] ET EXPLOIT Razer Sila Router - Command Injection Attempt Inbound (curl) (No CVE)
- [x] ET EXPLOIT Razer Sila Router - Command Injection Attempt Inbound (sh) (No CVE)
- [x] ET EXPLOIT TP-Link Archer AX21 Unauthenticated Command Injection Inbound (CVE-2023-1389)
- [x] ET EXPLOIT Possible Microsoft Outlook Elevation of Privilege Payload Observed M1 (CVE-2023-23397)
- [x] ET EXPLOIT Possible Microsoft Outlook Elevation of Privilege Payload Observed M3 (CVE-2023-23397)
- [x] ET EXPLOIT Possible Microsoft Outlook Elevation of Privilege Payload Observed M5 (CVE-2023-23397)
- [x] ET EXPLOIT Possible Microsoft Outlook Elevation of Privilege Payload Observed M7 (CVE-2023-23397)
- [x] ET EXPLOIT Apache log4j RCE Attempt (http) (Outbound) (CVE-2021-44228)
- [x] ET EXPLOIT PaperCut MF/NG SetupCompleted Authentication Bypass (CVE-2023-27350)
- [x] ET EXPLOIT ManageEngine Unauthenticated RCE Attempt M11 (CVE-2022-47966)
- [x] ET EXPLOIT Possible Oracle Opera RCE Attempt (CVE-2023-21932)
- [x] ET EXPLOIT Possible Command Injection via User-Agent (PwnAgent) - CVE-2023-24749, CVE-2022-47208
- [x] ET EXPLOIT Possible [401TRG] GhostCat LFI Successful Exploit (CVE-2020-1938)
- [x] ET EXPLOIT Fortigate VPN - Repeated POST Requests to /remote/hostcheck_validate (CVE-2023-27997) M1
- [x] ET EXPLOIT Fortigate VPN - Repeated GET Requests to /remote/logincheck (CVE-2023-27997)

- [x] ET EXPLOIT Fortigate VPN - Repeated POST Requests to /remote/logincheck (CVE-2023-27997)
- [x] ET EXPLOIT Possible Barracuda Email Security Gateway Remote Code Execution Attempt (CVE-2023-2868) M1
- [x] ET EXPLOIT Fortigate VPN - Repeated POST Requests to /remote/error (CVE-2023-27997)
- [x] ET EXPLOIT Possible Storm-0978 CVE-2023-36884 Exploitation Attempt M2
- [x] ET EXPLOIT Possible PaulPrinting CMS Cross-Site Scripting - Inbound
- [x] ET EXPLOIT Junos OS - Unauthenticated Arbitrary File Upload Attempt (CVE-2023-36846 CVE-2023-36847)
- [x] ET EXPLOIT Junos OS - Unauthenticated PHPRC Environmental Variable Modification M1 (CVE-2023-36844 CVE-2023-36845)
- [x] ET EXPLOIT Possible Barracuda Email Security Gateway Remote Code Execution Attempt (CVE-2023-2868) M2
- [x] ET EXPLOIT WS_FTP Reflected XSS Payload Observed M1 (CVE-2022-27665)
- [x] ET EXPLOIT Suspected Exim External Auth Overflow (CVE-2023-4115) set
- [x] ET EXPLOIT JetBrains TeamCity Auth Bypass Attempt (CVE-2023-42793)
- [x] ET EXPLOIT Tenda G103 Command Injection Attempt (CVE-2023-27076)
- [x] ET EXPLOIT DCN DCBI-Netlog-LAB Remote Code Execution Vulnerability Attempt (CVE-2023-26802)
- [x] ET EXPLOIT Cisco IOS XE Web Server Implant Check (CVE-2023-20198) (Inbound) M1
- [ ] ET EXPLOIT Cisco IOS XE Web Server Auth Bypass (CVE-2023-20198) (Inbound) M2
- [ ] ET EXPLOIT Possible Cisco IOS XE Web Server Implant 404 Response (CVE-2023-20198) (Inbound) M1
- [ ] ET EXPLOIT Possible Cisco IOS XE Web Server Implant 404 Response (CVE-2023-20198) (Inbound) M2
- [x] ET EXPLOIT Citrix ADC and NetScaler Gateway Information Disclosure Attempt (CVE-2023-4966)
- [x] ET EXPLOIT Cisco IOS XE Web Server Possible Authentication Bypass Attempt (CVE-2023-20198) (Outbound)
- [x] ET EXPLOIT Cisco IOS XE Web UI Command Injection Vulnerability (CVE-2023-20273)
- [x] ET EXPLOIT F5 BIG-IP - Unauthenticated RCE via AJP Smuggling Request (CVE-2023-46747)
- [x] ET EXPLOIT F5 BIG-IP - Unauthenticated RCE via AJP Smuggling Request - User Deletion (CVE-2023-46747)
- [x] ET EXPLOIT Successful Atlassian Confluence Improper Authentication Validation Exploitation Attempt (CVE-2023-22518)
- [x] ET EXPLOIT D-Link TRENDnet NCC Service Command Injection Attempt (CVE-2015-1187)
- [x] ET EXPLOIT Korenix JetWave formSysCmd Command Injection Attempt (CVE-2016-20017)
- [x] ET EXPLOIT Possible SysAid Traversal Attack (CVE-2023-47246)
- [x] ET EXPLOIT F5 BIG-IP iControl REST Authentication Bypass Attempt (CVE-2022-1388) M3
- [x] ET EXPLOIT Successful Apache ActiveMQ Remote Code Execution (CVE-2023-46604)
- [x] ET EXPLOIT Adobe ColdFusion Deserialization of Untrusted Data (CVE-2023-26360) M2
- [x] ET EXPLOIT ownCloud Information Disclosure Attempt (CVE-2023-49103)
- [x] ET EXPLOIT Successful ownCloud Information Disclosure Attempt (CVE-2023-49103) M2
- [x] ET EXPLOIT Successful ownCloud Remote Improper Authentication Attempt (CVE-2023-49105)
- [x] ET EXPLOIT Sophos Web Appliance Pre-Auth Command Injection Attempt (CVE-2023-1671)
- [x] ET EXPLOIT Inbound Setup Message from SMTP Smuggling Tool
- [x] ET EXPLOIT Inbound Smuggling Message from SMTP Smuggling Tool M2
- [x] ET EXPLOIT Fortigate VPN - Request to /remote/info - Possible CVE-2023-27997 Exploit Attempt
- [x] ET EXPLOIT VMware Aria Operations for Networks RCE Attempt (CVE-2023-20887)
- [x] ET EXPLOIT Possible Storm-0978 CVE-2023-36884 Exploitation Attempt M1
- [x] ET EXPLOIT Possible PaulPrinting CMS Cross-Site Scripting - Inbound
- [x] ET EXPLOIT Javascript Initiating Remote Server Search with Window's Search-MS URI Handler
- [x] ET EXPLOIT Junos OS - Successful Unauthenticated Arbitrary File Upload Attempt (CVE-2023-36846 CVE-2023-36847)
- [x] ET EXPLOIT Junos OS - Unauthenticated PHPRC Environmental Variable Modification M2 (CVE-2023-36844 CVE-2023-36845)
- [x] ET EXPLOIT Potential Adobe Experience Manager (AEM) Dispatcher Bypass Attempt
- [x] ET EXPLOIT WS_FTP .NET Deserialization Exploit Attempt (CVE-2023-40044)
- [x] ET EXPLOIT Suspected Exim External Auth Overflow (CVE-2023-4115)
- [x] ET EXPLOIT JetBrains TeamCity Auth Bypass Successful Attempt (CVE-2023-42793)
- [x] ET EXPLOIT LB-Link Command Injection Attempt (CVE-2023-26801)
- [x] ET EXPLOIT Cisco IOS XE Web Server Implant Check (CVE-2023-20198) (Outbound) M1
- [ ] ET EXPLOIT Cisco IOS XE Web Server Auth Bypass (CVE-2023-20198) (Outbound) M2
- [ ] ET EXPLOIT Possible Cisco IOS XE Web Server Implant 404 Response (CVE-2023-20198) (Outbound) M1
- [ ] ET EXPLOIT Possible Cisco IOS XE Web Server Implant 404 Response (CVE-2023-20198) (Outbound) M2
- [x] ET EXPLOIT Citrix ADC and NetScaler Gateway Information Disclosure Attempt (CVE-2023-4966)
- [x] ET EXPLOIT Citrix ADC and NetScaler Gateway Information Disclosure - Successful Response (CVE-2023-4966)
- [x] ET EXPLOIT Cisco IOS XE Web Server Possible Authentication Bypass Attempt (CVE-2023-20198) (Inbound)
- [x] ET EXPLOIT Apache ActiveMQ Remote Code Execution Attempt (CVE-2023-46604)
- [x] ET EXPLOIT F5 BIG-IP - Unauthenticated RCE via AJP Smuggling Request - User Creation (CVE-2023-46747)
- [x] ET EXPLOIT Possible Atlassian Confluence Improper Authentication Validation Exploitation Attempt set (CVE-2023-22518)
- [x] ET EXPLOIT Cisco IOS XE Web Server Implant Check (CVE-2023-20198) M3
- [x] ET EXPLOIT D-Link DSL-2750B Command Injection Attempt (CVE-2016-20017)
- [x] ET EXPLOIT Totolink Command Injection Attempt (CVE-2020-40475)
- [x] ET EXPLOIT SpringShell/Spring4Shell RCE Attempt (CVE-2022-22965)
- [x] ET EXPLOIT SysAid Traversal Attack (CVE-2023-47246)
- [x] ET EXPLOIT Adobe ColdFusion Deserialization of Untrusted Data (CVE-2023-26360) M1
- [x] ET EXPLOIT Adobe ColdFusion Deserialization of Untrusted Data (CVE-2023-26360) M3
- [x] ET EXPLOIT Successful ownCloud Information Disclosure Attempt (CVE-2023-49103) M1
- [x] ET EXPLOIT ownCloud Remote Improper Authentication Attempt (CVE-2023-49105)
- [x] ET EXPLOIT Suspected WordPress Plugin Royal Elementor RCE (CVE-2023-5360)
- [x] ET EXPLOIT Possible Google Cookie Token Manipulation Activity
- [x] ET EXPLOIT Inbound Smuggling Message from SMTP Smuggling Tool M1
- [x] ET EXPLOIT Atlassian Confluence RCE Attempt Observed (CVE-2023-22527) M1

- [x] ET EXPLOIT Possible Malicious x-sharing-config-url SMTP header observed (CVE-2023-35636)
- [x] ET EXPLOIT Jenkins Unauthenticated RCE Attempt Observed (CVE-2024-23897)
- [x] ET EXPLOIT Atlassian Confluence RCE Attempt Observed (CVE-2023-22527) M2
- [x] ET EXPLOIT Ivanti Connect Secure (9.x,22.x) / Ivanti Policy Secure (9.x,22.x) / Ivanti Neurons for ZTA SSRF Pattern (CVE-2024-21893)
- [x] ET EXPLOIT Ivanti Connect Secure (9.x,22.x) / Ivanti Policy Secure (9.x,22.x) / Ivanti Neurons for ZTA Command Injection via SSRF (CVE-2024-21887)
- [x] ET EXPLOIT CVE-2024-25600 Bricks Exploitation Attempt
- [ ] GPL EXPLOIT Redhat 7.0 lprd overflow
- [ ] GPL EXPLOIT ntpdx overflow attempt
- [ ] GPL EXPLOIT x86 Linux mountd overflow
- [ ] GPL EXPLOIT bootp x86 linux overflow
- [ ] GPL EXPLOIT ttdbserv solaris overflow
- [ ] GPL EXPLOIT ttdbserv Solaris overflow
- [ ] GPL EXPLOIT EXPLOIT statdx
- [x] GPL EXPLOIT rsh froot
- [x] GPL EXPLOIT rsh bin
- [x] GPL EXPLOIT sp_start_job - program execution
- [ ] GPL EXPLOIT sp_adduser database user creation
- [x] GPL EXPLOIT xp_cmdshell - program execution
- [x] GPL EXPLOIT xp_sprintf possible buffer overflow
- [ ] GPL EXPLOIT php.cgi access
- [ ] GPL EXPLOIT formmail access
- [x] GPL EXPLOIT administrators.pwd access
- [x] GPL EXPLOIT Alternate Data streams ASP file access attempt
- [x] GPL EXPLOIT .cnf access
- [x] GPL EXPLOIT unicode directory traversal attempt
- [x] GPL EXPLOIT unicode directory traversal attempt
- [x] GPL EXPLOIT .htr access
- [x] GPL EXPLOIT cmd? access
- [x] GPL EXPLOIT fpcount access
- [x] GPL EXPLOIT iisadmpwd attempt
- [x] GPL EXPLOIT site/iisamples access
- [x] GPL EXPLOIT xp_filelist attempt
- [ ] GPL EXPLOIT Tomcat server exploit access
- [x] GPL EXPLOIT ISAPI .ida access
- [x] GPL EXPLOIT ISAPI .ida attempt
- [x] GPL EXPLOIT ISAPI .idq attempt
- [x] GPL EXPLOIT ISAPI .idq access
- [x] GPL EXPLOIT CodeRed v2 root.exe access
- [ ] GPL EXPLOIT AIX pdnsd overflow
- [ ] GPL EXPLOIT ssh CRC32 overflow
- [x] GPL EXPLOIT echo command attempt
- [ ] GPL EXPLOIT tftp command attempt
- [ ] GPL EXPLOIT CDE dtspcd exploit attempt
- [x] GPL EXPLOIT /msadc/samples/ access
- [x] GPL EXPLOIT iissamples access
- [x] GPL EXPLOIT /iisadmpwd/aexp2.htr access
- [ ] GPL EXPLOIT formmail arbitrary command execution attempt
- [x] GPL EXPLOIT cmd32.exe access
- [ ] GPL EXPLOIT cachefsd buffer overflow attempt
- [x] GPL EXPLOIT xp_cmdshell program execution 445
- [ ] GPL EXPLOIT apache chunked encoding memory corruption exploit attempt
- [ ] GPL EXPLOIT LPD dvips remote command execution attempt
- [ ] GPL EXPLOIT SSH server banner overflow
- [x] GPL EXPLOIT kadmind buffer overflow attempt
- [x] GPL EXPLOIT kadmind buffer overflow attempt
- [x] GPL EXPLOIT kadmind buffer overflow attempt
- [x] GPL EXPLOIT kadmind buffer overflow attempt
- [ ] GPL EXPLOIT kadmind buffer overflow attempt 2
- [ ] GPL EXPLOIT kadmind buffer overflow attempt 3
- [ ] GPL EXPLOIT successful kadmind buffer overflow attempt
- [ ] GPL EXPLOIT successful kadmind buffer overflow attempt
- [ ] GPL EXPLOIT xfs overflow attempt
- [ ] GPL EXPLOIT bootp hostname format string attempt
- [x] GPL EXPLOIT rsyncd module list access
- [ ] GPL EXPLOIT WEBDAV exploit attempt
- [ ] GPL EXPLOIT portmap proxy integer overflow attempt UDP
- [ ] GPL EXPLOIT rexec username overflow attempt
- [x] GPL EXPLOIT Microsoft cmd.exe banner
- [ ] GPL EXPLOIT CVS non-relative path access attempt
- [ ] GPL EXPLOIT ISAKMP first payload certificate request length overflow attempt
- [ ] GPL EXPLOIT ISAKMP second payload certificate request length overflow attempt
- [ ] GPL EXPLOIT ISAKMP forth payload certificate request length overflow attempt
- [ ] GPL EXPLOIT ISAKMP fifth payload certificate request length overflow attempt
- [x] GPL EXPLOIT NTLM ASN.1 vulnerability scan attempt
- [ ] GPL EXPLOIT ISAKMP delete hash with empty hash attempt
- [ ] GPL EXPLOIT ISAKMP initial contact notification without SPI attempt
- [ ] GPL EXPLOIT ISAKMP second payload initial contact notification without SPI attempt
- [ ] GPL EXPLOIT IGMP IGAP account overflow attempt
- [ ] GPL EXPLOIT IGMP IGAP message overflow attempt
- [ ] GPL EXPLOIT EIGRP prefix length overflow attempt
- [ ] GPL EXPLOIT ISAKMP invalid identification payload attempt
- [ ] GPL EXPLOIT Oracle Web Cache HEAD overflow attempt
- [ ] GPL EXPLOIT Oracle Web Cache PUT overflow attempt
- [ ] GPL EXPLOIT Oracle Web Cache POST overflow attempt
- [ ] GPL EXPLOIT Oracle Web Cache TRACE overflow attempt
- [ ] GPL EXPLOIT Oracle Web Cache DELETE overflow attempt
- [ ] GPL EXPLOIT Oracle Web Cache LOCK overflow attempt
- [ ] GPL EXPLOIT Oracle Web Cache MKCOL overflow attempt
- [ ] GPL EXPLOIT Oracle Web Cache COPY overflow attempt
- [ ] GPL EXPLOIT Oracle Web Cache MOVE overflow attempt
- [x] GPL EXPLOIT .cmd executable file parsing attack
- [ ] GPL EXPLOIT WINS name query overflow attempt TCP
- [x] GPL EXPLOIT login buffer non-evasive overflow attempt
- [ ] GPL EXPLOIT Arkeia client backup system info probe
- [x] GPL EXPLOIT WEB-MISC JBoss RMI class download service directory listing attempt

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

- [ ] ET EXPLOIT_KIT Possible Malicious Applet Access (justexploit kit)
- [ ] ET EXPLOIT_KIT Exploit kit download payload likely Hiloti Gozi FakeAV etc
- [ ] ET EXPLOIT_KIT Exploit kit attack activity likely hostile
- [ ] ET EXPLOIT_KIT Phoenix Exploit Kit Facebook phishing page payload could be ZeuS
- [ ] ET EXPLOIT_KIT Phoenix Exploit Kit pdfopen.pdf
- [ ] ET EXPLOIT_KIT Phoenix Exploit Kit pdfswf.pdf
- [ ] ET EXPLOIT_KIT Phoenix Exploit Kit - libtiff.pdf
- [x] ET EXPLOIT_KIT Phoenix Exploit Kit VBscript download
- [ ] ET EXPLOIT_KIT Phoenix Exploit Kit - Admin Login Page Detected Outbound
- [x] ET EXPLOIT_KIT phoenix exploit kit - admin login page detected

- [ ] ET EXPLOIT_KIT DRIVEBY SEO Exploit Kit request for PDF exploit
- [ ] ET EXPLOIT_KIT DRIVEBY SEO Exploit Kit request for Java and PDF exploits
- [ ] ET EXPLOIT_KIT SEO Exploit Kit - Landing Page
- [x] ET EXPLOIT_KIT exploit kit x/load/svchost.exe
- [ ] ET EXPLOIT_KIT Java Exploit Kit Success Check-in Executable Download Likely
- [ ] ET EXPLOIT_KIT Phoenix Exploit Kit Newplayer.pdf
- [ ] ET EXPLOIT_KIT Phoenix Exploit Kit Geticon.pdf
- [ ] ET EXPLOIT_KIT Exploit kit mario.jar
- [ ] ET EXPLOIT_KIT Java/PDF Exploit kit initial landing
- [ ] ET EXPLOIT_KIT Likely EgyPack Exploit kit landing page (EGYPACK_CRYPT)
- [ ] ET EXPLOIT_KIT Obfuscated Javascript Often Used in Drivebys
- [ ] ET EXPLOIT_KIT DRIVEBY ACH - Redirection
- [ ] ET EXPLOIT_KIT Driveby Generic Java Exploit Attempt 2
- [ ] ET EXPLOIT_KIT Exploit kit worms.jar
- [ ] ET EXPLOIT_KIT Unknown Exploit Kit Java requesting malicious JAR
- [ ] ET EXPLOIT_KIT Unknown Exploit Kit request for pdf_err__Error__Unspecified
- [ ] ET EXPLOIT_KIT Unknown Java Exploit Kit lo.class
- [ ] ET EXPLOIT_KIT Unknown Java Exploit Kit applet landing
- [ ] ET EXPLOIT_KIT Saturn Exploit Kit probable Java exploit request
- [ ] ET EXPLOIT_KIT Incognito Exploit Kit Java request to showthread.php?t=
- [ ] ET EXPLOIT_KIT Neosploit Java Exploit Kit request to /? plus hex 32
- [ ] ET EXPLOIT_KIT Probable Scalaxy exploit kit Java or PDF exploit request
- [ ] ET EXPLOIT_KIT DRIVEBY Generic Java Rhino Scripting Engine Exploit Previously Requested org.class
- [ ] ET EXPLOIT_KIT DRIVEBY Generic Java Rhino Scripting Engine Exploit Previously Requested net.class
- [x] ET EXPLOIT_KIT Document.write Long Backslash UTF-16 Encoded Content - Exploit Kit Behavior Flowbit Set
- [ ] ET EXPLOIT_KIT Exploit Kit Delivering Office File to Client
- [x] ET EXPLOIT_KIT Sakura Exploit Kit Landing Page Request
- [ ] ET EXPLOIT_KIT Known Malicious Link Leading to Exploit Kits (t.php?id=is1)
- [ ] ET EXPLOIT_KIT Yang Pack Exploit Kit Landing Page Known JavaScript Function Detected
- [ ] ET EXPLOIT_KIT CUTE-IE.html CutePack Exploit Kit Landing Page Request
- [ ] ET EXPLOIT_KIT CUTE-IE.html CutePack Exploit Kit Iframe for Landing Page Detected
- [x] ET EXPLOIT_KIT DRIVEBY Java Rhino Scripting Engine Exploit Downloaded
- [x] ET EXPLOIT_KIT DRIVEBY Incognito Payload Download /load/*exe
- [ ] ET EXPLOIT_KIT DRIVEBY Incognito libtiff PDF Exploit Recieved
- [x] ET EXPLOIT_KIT DRIVEBY EgyPack Exploit Kit Cookie Set
- [ ] ET EXPLOIT_KIT DRIVEBY Unknown - news=1 in http_cookie
- [x] ET EXPLOIT_KIT Possible Dynamic Dns Exploit Pack Java exploit
- [ ] ET EXPLOIT_KIT Malicious TDS /indigo?
- [x] ET EXPLOIT_KIT TDS Sutra - request in.cgi
- [x] ET EXPLOIT_KIT TDS Sutra - page redirecting to a SutraTDS
- [x] ET EXPLOIT_KIT TDS Sutra - redirect received
- [x] ET EXPLOIT_KIT TDS Sutra - page redirecting to a SutraTDS
- [ ] ET EXPLOIT_KIT Unkown exploit kit version check
- [x] ET EXPLOIT_KIT TDS Sutra - cookie set RULEZ
- [x] ET EXPLOIT_KIT Incognito Exploit Kit PDF request to images.php?t=81118
- [ ] ET EXPLOIT_KIT DRIVEBY SEO Exploit Kit request for Java exploit
- [ ] ET EXPLOIT_KIT Fragus Exploit Kit Landing
- [ ] ET EXPLOIT_KIT SEO Exploit Kit - client exploited
- [ ] ET EXPLOIT_KIT Phoenix-style Exploit Kit Java Request with semicolon in URI
- [x] ET EXPLOIT_KIT Incognito Exploit Kit Checkin
- [ ] ET EXPLOIT_KIT Phoenix Exploit Kit Printf.pdf
- [ ] ET EXPLOIT_KIT Phoenix Exploit Kit All.pdf
- [ ] ET EXPLOIT_KIT Java/PDF Exploit kit from /Home/games/ initial landing
- [ ] ET EXPLOIT_KIT Driveby Exploit Kit Browser Progress Checkin - Binary Likely Previously Downloaded
- [ ] ET EXPLOIT_KIT EgyPack Exploit Kit Post-Infection Request
- [x] ET EXPLOIT_KIT Redirection to driveby Page Home index.php
- [ ] ET EXPLOIT_KIT Driveby Generic Java Exploit Attempt
- [ ] ET EXPLOIT_KIT Unknown Exploit Kit Landing Response Malicious JavaScript
- [ ] ET EXPLOIT_KIT Unknown Exploit Kit reporting Java and PDF state
- [ ] ET EXPLOIT_KIT Unknown Exploit Kit Java requesting malicious EXE
- [ ] ET EXPLOIT_KIT Unknown Java Exploit Kit x.jar?o=
- [ ] ET EXPLOIT_KIT Unknown Java Exploit Kit lo2.jar
- [ ] ET EXPLOIT_KIT Saturn Exploit Kit binary download request
- [ ] ET EXPLOIT_KIT Saturn Exploit Kit probable Java MIDI exploit request
- [ ] ET EXPLOIT_KIT Jupiter Exploit Kit Landing Page with Malicious Java Applets
- [ ] ET EXPLOIT_KIT Probable Scalaxy exploit kit secondary request
- [ ] ET EXPLOIT_KIT DRIVEBY Generic Java Rhino Scripting Engine Exploit Previously Requested com.class
- [ ] ET EXPLOIT_KIT DRIVEBY Generic Java Rhino Scripting Engine Exploit Previously Requested edu.class
- [ ] ET EXPLOIT_KIT DRIVEBY Generic Java Exploit Obfuscated With Allatori
- [ ] ET EXPLOIT_KIT Excessive new Array With Newline - Exploit Kit Behavior Flowbit Set
- [ ] ET EXPLOIT_KIT Unknown Java Exploit Version Check with hidden applet
- [x] ET EXPLOIT_KIT Sakura Exploit Kit Binary Load Request
- [ ] ET EXPLOIT_KIT DRIVEBY Unknown Landing Page Received
- [ ] ET EXPLOIT_KIT Exploit Kit Exploiting IEPeers
- [ ] ET EXPLOIT_KIT CutePack Exploit Kit JavaScript Variable Detected
- [ ] ET EXPLOIT_KIT CutePack Exploit Kit Landing Page Detected
- [x] ET EXPLOIT_KIT DRIVEBY Java Atomic Exploit Downloaded
- [ ] ET EXPLOIT_KIT DRIVEBY Incognito libtiff PDF Exploit Requested
- [x] ET EXPLOIT_KIT Likely Scalaxy Exploit Kit URL template download
- [x] ET EXPLOIT_KIT DRIVEBY EgyPack Exploit Kit Cookie Present
- [x] ET EXPLOIT_KIT Possible Dynamic DNS Exploit Pack Landing Page /de/sN
- [x] ET EXPLOIT_KIT Exploit Kit Delivering JAR Archive to Client
- [x] ET EXPLOIT_KIT TDS Sutra - redirect received
- [x] ET EXPLOIT_KIT TDS Sutra - cookie set
- [x] ET EXPLOIT_KIT TDS Sutra - HTTP header redirecting to a SutraTDS
- [x] ET EXPLOIT_KIT TDS Sutra - cookie set
- [ ] ET EXPLOIT_KIT Unkown exploit kit jar download
- [x] ET EXPLOIT_KIT Incognito Exploit Kit Java request to images.php?t=
- [x] ET EXPLOIT_KIT TDS Sutra - cookie is set RULEZ
- [ ] ET EXPLOIT_KIT Incognito Exploit Kit payload request to images.php?t=N

- [ ] ET EXPLOIT_KIT Incognito Exploit Kit landing page request to images.php?t=4xxxxxxx
- [ ] ET EXPLOIT_KIT Unkown exploit kit payload download
- [x] ET EXPLOIT_KIT Bleeding Life 2 GPLed Exploit Pack exploit request
- [x] ET EXPLOIT_KIT Bleeding Life 2 GPLed Exploit Pack payload download
- [ ] ET EXPLOIT_KIT Incognito/RedKit Exploit Kit vulnerable Java payload request to /1digit.html
- [x] ET EXPLOIT_KIT Fragus Exploit jar Download
- [x] ET EXPLOIT_KIT Sakura Exploit Kit Version 1.1 Archive Request
- [ ] ET EXPLOIT_KIT Sakura Exploit Kit Version 1.1 Applet Value lxxt
- [x] ET EXPLOIT_KIT Redirect to driveby sid=mix
- [ ] ET EXPLOIT_KIT NuclearPack - JAR Naming Algorithm
- [ ] ET EXPLOIT_KIT DRIVEBY Incognito Landing Page Requested .php?showtopic=6digit
- [x] ET EXPLOIT_KIT DRIVEBY Incognito Payload Requested /getfile.php by Java Client
- [ ] ET EXPLOIT_KIT NuclearPack Java exploit binary get request
- [x] ET EXPLOIT_KIT g01pack exploit pack /mix/ payload
- [ ] ET EXPLOIT_KIT Possible Unknown TDS /rem2.html
- [x] ET EXPLOIT_KIT DoSWF Flash Encryption (Used in KaiXin Exploit Kit)
- [x] ET EXPLOIT_KIT Sutra TDS /simmetry
- [ ] ET EXPLOIT_KIT DRIVEBY SPL - Java Exploit Requested .jar Naming Pattern
- [ ] ET EXPLOIT_KIT Unknown Exploit Kit seen with O1/O2.class /form
- [ ] ET EXPLOIT_KIT Unknown Exploit Kit redirect
- [ ] ET EXPLOIT_KIT Unknown Java Exploit Kit Payload Download Request - Sep 04 2012
- [x] ET EXPLOIT_KIT Probable Sakura exploit kit landing page with obfuscated URLs
- [ ] ET EXPLOIT_KIT Unknown Java Exploit Kit with fast-flux like behavior hostile java archive - Sep 05 2012
- [ ] ET EXPLOIT_KIT NeoSploit - Obfuscated Payload Requested
- [x] ET EXPLOIT_KIT NeoSploit - Version Enumerated - Java
- [x] ET EXPLOIT_KIT DRIVEBY Generic - 8Char.JAR Naming Algorithm
- [ ] ET EXPLOIT_KIT pamdql Exploit Kit 09/25/12 Sending Jar
- [x] ET EXPLOIT_KIT Sakura exploit kit exploit download request /nano.php
- [ ] ET EXPLOIT_KIT pamdql obfuscated javascript --- padding
- [x] ET EXPLOIT_KIT Unknown Java Exploit Kit 32-32 byte hex initial landing
- [ ] ET EXPLOIT_KIT BegOp Exploit Kit Payload
- [x] ET EXPLOIT_KIT BegOpEK - TDS - icon.php
- [ ] ET EXPLOIT_KIT g01pack Exploit Kit .homeip. Landing Page
- [ ] ET EXPLOIT_KIT Unknown Exploit Kit Landing Page
- [x] ET EXPLOIT_KIT NeoSploit Jar with three-letter class names
- [x] ET EXPLOIT_KIT Sakura/RedKit obfuscated URL
- [ ] ET EXPLOIT_KIT Cool Exploit Kit Requesting Payload
- [x] ET EXPLOIT_KIT KaiXin Exploit Kit Landing Page parseInt Javascript Replace
- [x] ET EXPLOIT_KIT CritXPack - No Java URI - Dot.class
- [ ] ET EXPLOIT_KIT Magnitude EK (formerly Popads) Java Exploit Kit 32 byte hex with trailing digit java payload request
- [ ] ET EXPLOIT_KIT Possible TDS Exploit Kit /flow redirect at .ru domain
- [ ] ET EXPLOIT_KIT Possible Glazunov Java exploit request /9-10-/4-5-digit
- [ ] ET EXPLOIT_KIT RedKit Exploit Kit Java Request to Recent jar (1)
- [ ] ET EXPLOIT_KIT RedKit Exploit Kit Vulnerable Java Payload Request URI (1)
- [x] ET EXPLOIT_KIT Unkown exploit kit pdf download
- [x] ET EXPLOIT_KIT DRIVEBY Generic - Redirection to Kit - BrowserDetect with var stopit
- [x] ET EXPLOIT_KIT Bleeding Life 2 GPLed Exploit Pack payload request (exploit successful!)
- [ ] ET EXPLOIT_KIT Redkit Java Exploit request to /24842.jar
- [ ] ET EXPLOIT_KIT Nuclear/Safe/CritX/FlashPack - Java Request - 32char hex-ascii
- [x] ET EXPLOIT_KIT Wordpress timthumb look-alike domain list RFI
- [x] ET EXPLOIT_KIT Possible Sakura Exploit Kit Version 1.1 document.write Fake 404 - Landing Page
- [x] ET EXPLOIT_KIT Likely TDS redirecting to exploit kit
- [ ] ET EXPLOIT_KIT Request to malicious SutraTDS - lonly= in cookie
- [x] ET EXPLOIT_KIT NuclearPack - Landing Page Received - applet archive=32CharHex
- [ ] ET EXPLOIT_KIT DRIVEBY Incognito Landing Page Received applet and flowbit
- [x] ET EXPLOIT_KIT - Landing Page Requested - 15Alpha1Digit.php
- [ ] ET EXPLOIT_KIT g01pack exploit pack /mix/ Java exploit
- [x] ET EXPLOIT_KIT Possible Unknown TDS /top2.html
- [x] ET EXPLOIT_KIT Yszz JS/Encryption (Used in KaiXin Exploit Kit)
- [ ] ET EXPLOIT_KIT KaiXin Exploit Kit Java Class
- [x] ET EXPLOIT_KIT DRIVEBY SPL - Java Exploit Requested - /spl_data/
- [x] ET EXPLOIT_KIT DRIVEBY SPL - Landing Page Received
- [ ] ET EXPLOIT_KIT Unknown Exploit Kit seen with O1/O2.class /search
- [x] ET EXPLOIT_KIT SimpleTDS go.php (sid)
- [ ] ET EXPLOIT_KIT Sakura exploit kit exploit download request /view.php
- [ ] ET EXPLOIT_KIT Unknown Java Exploit Kit with fast-flux like behavior static initial landing - Sep 05 2012
- [ ] ET EXPLOIT_KIT DRIVEBY NeoSploit - Java Exploit Requested
- [ ] ET EXPLOIT_KIT NeoSploit - PDF Exploit Requested
- [ ] ET EXPLOIT_KIT NeoSploit - Version Enumerated - null
- [x] ET EXPLOIT_KIT SSL Cert Used In Unknown Exploit Kit (ashburn)
- [ ] ET EXPLOIT_KIT Sakura exploit kit exploit download request /sarah.php
- [x] ET EXPLOIT_KIT Probable Sakura Java applet with obfuscated URL Sep 21 2012
- [ ] ET EXPLOIT_KIT g01pack Exploit Kit Landing Page (2)
- [ ] ET EXPLOIT_KIT Magnitude EK (formerly Popads) Other Java Exploit Kit 32-32 byte hex hostile jar
- [x] ET EXPLOIT_KIT BegOpEK - Landing Page
- [ ] ET EXPLOIT_KIT Scalaxy Secondary Landing Page 10/11/12
- [ ] ET EXPLOIT_KIT g01pack Exploit Kit .homelinux. Landing Page
- [ ] ET EXPLOIT_KIT Unknown Exploit Kit Landing Page
- [ ] ET EXPLOIT_KIT Metasploit CVE-2012-1723 Path (Seen in Unknown EK) 10/29/12
- [ ] ET EXPLOIT_KIT Self-Signed SSL Cert Used in Conjunction with Neosploit
- [x] ET EXPLOIT_KIT KaiXin Exploit Kit Landing Page NOP String
- [x] ET EXPLOIT_KIT CritXPack Landing Page
- [x] ET EXPLOIT_KIT CirtXPack - No Java URI - /a.Test
- [x] ET EXPLOIT_KIT CoolEK - Landing Page - FlashExploit
- [ ] ET EXPLOIT_KIT Magnitude EK (formerly Popads) - Landing Page - Java ClassID and 32HexChar.jar
- [x] ET EXPLOIT_KIT Possible Glazunov Java payload request /5-digit
- [ ] ET EXPLOIT_KIT RedKit Exploit Kit Java Request to Recent jar (2)
- [ ] ET EXPLOIT_KIT RedKit Exploit Kit vulnerable Java Payload Request to URI (2)

- [ ] ET EXPLOIT_KIT Nuclear Exploit Kit HTTP Off-port Landing Page Request
- [ ] ET EXPLOIT_KIT CrimeBoss - Java Exploit - Recent Jar (1)
- [ ] ET EXPLOIT_KIT Crimeboss - Java Exploit - Recent Jar (3)
- [ ] ET EXPLOIT_KIT CrimeBoss - Stats Java On
- [ ] ET EXPLOIT_KIT Propack Recent Jar (1)
- [ ] ET EXPLOIT_KIT PDF /FlateDecode and PDF version 1.1 (seen in pamdql EK)
- [x] ET EXPLOIT_KIT CritXPack Jar Request
- [ ] ET EXPLOIT_KIT CritXPack Payload Request
- [ ] ET EXPLOIT_KIT Zuponcic EK Payload Request
- [ ] ET EXPLOIT_KIT Sibhost Status Check
- [ ] ET EXPLOIT_KIT CritXPack - Landing Page
- [x] ET EXPLOIT_KIT Zuponcic Hostile JavaScript
- [ ] ET EXPLOIT_KIT RedKit - Potential Java Exploit Requested - 3 digit jar
- [ ] ET EXPLOIT_KIT Robopak - Landing Page Received
- [ ] ET EXPLOIT_KIT PDF /XFA and PDF-1.[0-4] Spec Violation (seen in pamdql and other EKs)
- [ ] ET EXPLOIT_KIT CritXPack Jar Request (2)
- [ ] ET EXPLOIT_KIT g01pack - Landing Page Received - applet and 32AlphaNum.jar
- [ ] ET EXPLOIT_KIT Unknown_gmf EK - Payload Download Received
- [x] ET EXPLOIT_KIT Unknown_gmf EK - pdfx.html
- [ ] ET EXPLOIT_KIT Magnitude EK (formerly Popads) Embedded Open Type Font file .eot
- [ ] ET EXPLOIT_KIT SofosFO 20 Dec 12 - .jar file request
- [ ] ET EXPLOIT_KIT SofosFO - possible second stage landing page
- [ ] ET EXPLOIT_KIT pamdql/Sweet Orange delivering exploit kit payload
- [ ] ET EXPLOIT_KIT Topic EK Requesting Jar
- [ ] ET EXPLOIT_KIT Sweet Orange Java payload request (1)
- [ ] ET EXPLOIT_KIT Unknown_gmf/Styx EK - fnts.html
- [ ] ET EXPLOIT_KIT Possible CrimeBoss Generic URL Structure
- [ ] ET EXPLOIT_KIT DRIVEBY SPL - Landing Page Received
- [x] ET EXPLOIT_KIT Redkit Exploit Kit Three Numerical Character Naming Convention PDF Request
- [ ] ET EXPLOIT_KIT StyX Landing Page
- [ ] ET EXPLOIT_KIT Redkit Class Request (1)
- [x] ET EXPLOIT_KIT Possible Red Dot Exploit Kit Single Character JAR Request
- [x] ET EXPLOIT_KIT Gondad Exploit Kit Post Exploitation Request
- [ ] ET EXPLOIT_KIT Redkit Class Request (3)
- [x] ET EXPLOIT_KIT JDB Exploit Kit Landing Page
- [x] ET EXPLOIT_KIT JDB Exploit Kit JAR Download
- [ ] ET EXPLOIT_KIT Impact Exploit Kit Landing Page
- [x] ET EXPLOIT_KIT Styx Exploit Kit Secondary Landing
- [ ] ET EXPLOIT_KIT WhiteHole Exploit Kit Jar Request
- [x] ET EXPLOIT_KIT Styx Exploit Kit Jerk.cgi TDS
- [x] ET EXPLOIT_KIT CritXPack - Landing Page - Received
- [ ] ET EXPLOIT_KIT Exploit Kit Java jpg download
- [ ] ET EXPLOIT_KIT Unknown_MM - Java Exploit - jaxws.jar
- [x] ET EXPLOIT_KIT Unknown_MM - Payload Download
- [ ] ET EXPLOIT_KIT Sakura Exploit Kit Encrypted Binary (1)
- [ ] ET EXPLOIT_KIT CoolEK Payload - obfuscated binary base 0
- [ ] ET EXPLOIT_KIT TDS Vdele
- [ ] ET EXPLOIT_KIT CoolEK landing applet plus class Feb 18 2013
- [ ] ET EXPLOIT_KIT CoolEK/BHEK/Impact EK Java7 Exploit Class Request (1)
- [ ] ET EXPLOIT_KIT CoolEK/BHEK/Impact EK Java7 Exploit Class Request (3)
- [x] ET EXPLOIT_KIT StyX Landing Page (2)
- [x] ET EXPLOIT_KIT Styx Exploit Kit Payload Download
- [ ] ET EXPLOIT_KIT CrimeBoss - Java Exploit - jhan.jar
- [ ] ET EXPLOIT_KIT g01pack Exploit Kit .blogsite. Landing Page
- [ ] ET EXPLOIT_KIT CrimeBoss - Java Exploit - Recent Jar (2)
- [ ] ET EXPLOIT_KIT CrimeBoss - Stats Access
- [ ] ET EXPLOIT_KIT CrimeBoss - Setup
- [ ] ET EXPLOIT_KIT Propack Payload Request
- [ ] ET EXPLOIT_KIT Serenity Exploit Kit Landing Page HTML Header
- [x] ET EXPLOIT_KIT CritXPack PDF Request
- [x] ET EXPLOIT_KIT Unknown EK Landing URL
- [ ] ET EXPLOIT_KIT Zuponcic EK Java Exploit Jar
- [ ] ET EXPLOIT_KIT probable malicious Glazunov Javascript injection
- [ ] ET EXPLOIT_KIT Zuponcic Hostile Jar
- [ ] ET EXPLOIT_KIT CrimeBoss - Stats Load Fail
- [x] ET EXPLOIT_KIT RedKit - Potential Payload Requested - /2Digit.html
- [x] ET EXPLOIT_KIT CritXPack Landing Pattern
- [ ] ET EXPLOIT_KIT CritXPack PDF Request (2)
- [ ] ET EXPLOIT_KIT NuclearPack - Landing Page Received - applet and 32HexChar.jar
- [ ] ET EXPLOIT_KIT Unknown_gmf EK - Payload Download Requested
- [ ] ET EXPLOIT_KIT Unknown_gmf EK - Server Response - Application Error
- [ ] ET EXPLOIT_KIT Unknown_gmf EK - flsh.html
- [x] ET EXPLOIT_KIT SofosFO obfuscator string 19 Dec 12 - possible landing
- [ ] ET EXPLOIT_KIT SofosFO 20 Dec 12 - .pdf file request
- [x] ET EXPLOIT_KIT Hostile Gate landing seen with pamdql/Sweet Orange base64
- [x] ET EXPLOIT_KIT Unknown EK Landing Page
- [ ] ET EXPLOIT_KIT Topic EK Requesting PDF
- [ ] ET EXPLOIT_KIT Redkit encrypted binary (1)
- [ ] ET EXPLOIT_KIT Sweet Orange Java payload request (2)
- [ ] ET EXPLOIT_KIT DRIVEBY RedKit - Landing Page
- [ ] ET EXPLOIT_KIT CoolEK - Landing Page Received
- [ ] ET EXPLOIT_KIT Impact Exploit Kit Class Download
- [x] ET EXPLOIT_KIT StyX Landing Page
- [ ] ET EXPLOIT_KIT Redkit Class Request (2)
- [ ] ET EXPLOIT_KIT Red Dot Exploit Kit Binary Payload Request
- [x] ET EXPLOIT_KIT TDS - in.php
- [ ] ET EXPLOIT_KIT JDB Exploit Kit Landing URL structure
- [x] ET EXPLOIT_KIT Possible JDB Exploit Kit Class Request
- [x] ET EXPLOIT_KIT JDB Exploit Kit Fake Adobe Download
- [ ] ET EXPLOIT_KIT Possible g01pack Landing Page
- [ ] ET EXPLOIT_KIT WhiteHole Exploit Landing Page
- [ ] ET EXPLOIT_KIT WhiteHole Exploit Kit Payload Download
- [ ] ET EXPLOIT_KIT Styx Exploit Kit Landing Applet With Getmyfile.exe Payload
- [ ] ET EXPLOIT_KIT CritXPack - URI - jpfoff.php
- [x] ET EXPLOIT_KIT Unknown_MM EK - Landing Page
- [ ] ET EXPLOIT_KIT Unknown_MM - Java Exploit - jre.jar
- [ ] ET EXPLOIT_KIT Unknown_MM EK - Java Exploit - fbyte.jar
- [ ] ET EXPLOIT_KIT Impact Exploit Kit Landing Page
- [x] ET EXPLOIT_KIT Cool Java Exploit Recent Jar (1)
- [x] ET EXPLOIT_KIT CoolEK Payload Download (5)
- [ ] ET EXPLOIT_KIT CoolEK Possible Java Payload Download
- [ ] ET EXPLOIT_KIT CoolEK/BHEK/Impact EK Java7 Exploit Class Request (2)
- [ ] ET EXPLOIT_KIT CoolEK/BHEK/Impact EK Java7 Exploit Class Request (3)
- [ ] ET EXPLOIT_KIT Styx Exploit Kit Landing Applet With Payload
- [x] ET EXPLOIT_KIT Possible Nicepack EK Landing (Anti-VM)
- [x] ET EXPLOIT_KIT Probable Sakura exploit kit landing page obfuscated applet tag Mar 1 2013

- [x] ET EXPLOIT_KIT Unknown Exploit Kit Java Archive Request (Java-SPLOIT.jar)
- [x] ET EXPLOIT_KIT SUSPICIOUS JAR Download by Java UA with non JAR EXT matches various EKs
- [ ] ET EXPLOIT_KIT Possible Portal TDS Kit GET
- [x] ET EXPLOIT_KIT Base64 http argument in applet (Neutrino/Angler)
- [ ] ET EXPLOIT_KIT GonDadEK Plugin Detect March 11 2013
- [ ] ET EXPLOIT_KIT Sweet Orange applet with obfuscated URL March 03 2013
- [ ] ET EXPLOIT_KIT RedDotv2 Java Check-in
- [x] ET EXPLOIT_KIT Watering Hole applet name AppletHigh.jar
- [x] ET EXPLOIT_KIT Possible RedDotv2 applet with 32hex value Landing Page
- [x] ET EXPLOIT_KIT Probable Sakura exploit kit landing page obfuscated applet tag Mar 28 2013
- [ ] ET EXPLOIT_KIT CrimeBoss Recent Jar (3)
- [ ] ET EXPLOIT_KIT BHEK q.php iframe inbound
- [ ] ET EXPLOIT_KIT BHEK q.php iframe outbound
- [ ] ET EXPLOIT_KIT Possible Sakura Jar Download
- [ ] ET EXPLOIT_KIT Sakura encrypted binary (2)
- [ ] ET EXPLOIT_KIT GonDadEK Java Exploit Requested
- [ ] ET EXPLOIT_KIT GonDadEK Kit Jar
- [x] ET EXPLOIT_KIT GrandSoft PDF Payload Download
- [ ] ET EXPLOIT_KIT Fiesta - Payload - flashplayer11
- [ ] ET EXPLOIT_KIT Sakura - Payload Requested
- [ ] ET EXPLOIT_KIT Sakura - Landing Page - Received
- [x] ET EXPLOIT_KIT Possible Java Applet JNLP applet_ssv_validated Click To Run Bypass
- [x] ET EXPLOIT_KIT Magnitude EK (formerly Popads) Flash Exploit Requested
- [ ] ET EXPLOIT_KIT Unknown EK UAC Disable in Uncompressed JAR
- [x] ET EXPLOIT_KIT - Possible Redkit 1-4 char JNLP request
- [ ] ET EXPLOIT_KIT Possible Java Applet JNLP applet_ssv_validated in Base64 3
- [ ] ET EXPLOIT_KIT CVE-2013-2423 IVKM PoC Seen in Unknown EK
- [ ] ET EXPLOIT_KIT IE HTML+TIME ANIMATECOLOR with eval as seen in unknown EK
- [ ] ET EXPLOIT_KIT FlimKit Landing
- [ ] ET EXPLOIT_KIT Unknown_MM - Java Exploit - cee.jar
- [ ] ET EXPLOIT_KIT Unknown EK Requesting Payload
- [ ] ET EXPLOIT_KIT KaiXin Exploit Kit Java Class 2 May 24 2013
- [ ] ET EXPLOIT_KIT KaiXin Exploit Landing Page 2 May 24 2013
- [ ] ET EXPLOIT_KIT HellSpawn EK Landing 2 May 24 2013
- [ ] ET EXPLOIT_KIT Possible HellSpawn EK Java Artifact May 24 2013
- [ ] ET EXPLOIT_KIT Sakura - Payload Requested
- [ ] ET EXPLOIT_KIT Probable Nuclear exploit kit landing page
- [ ] ET EXPLOIT_KIT Metasploit Based Unknown EK Jar Download June 03 2013
- [x] ET EXPLOIT_KIT CoolEK Payload Download (9)
- [x] ET EXPLOIT_KIT Unknown EK Landing (Payload Downloaded Via Dropbox)
- [ ] ET EXPLOIT_KIT Unknown EK Jar 2 June 12 2013
- [ ] ET EXPLOIT_KIT Dotka Chef EK .cache request
- [ ] ET EXPLOIT_KIT CritX/SafePack/FlashPack URI Format June 17 2013 1
- [ ] ET EXPLOIT_KIT MALVERTISING Unknown_InlFRAME - RedTDS URI Structure
- [ ] ET EXPLOIT_KIT Unknown_InlFRAME - Redirect to /iniframe/ URI
- [ ] ET EXPLOIT_KIT NailedPack EK Landing June 18 2013
- [ ] ET EXPLOIT_KIT X20 EK Payload Download
- [ ] ET EXPLOIT_KIT Rawin Exploit Kit Jar 1.7.x
- [ ] ET EXPLOIT_KIT Rawin Exploit Kit Jar 1.6 (New)
- [x] ET EXPLOIT_KIT Unknown Exploit Kit Exploit Request
- [x] ET EXPLOIT_KIT SofosFO/GrandSoft landing applet plus class Mar 03 2013
- [ ] ET EXPLOIT_KIT Possible Portal TDS Kit GET (2)
- [ ] ET EXPLOIT_KIT Possible CrimeBoss Generic URL Structure
- [ ] ET EXPLOIT_KIT SNET EK Downloading Payload
- [x] ET EXPLOIT_KIT Redkit Landing Page URL March 03 2013
- [ ] ET EXPLOIT_KIT CrimeBoss - Java Exploit - jmx.jar
- [ ] ET EXPLOIT_KIT Watering Hole applet name AppletLow.jar
- [ ] ET EXPLOIT_KIT Sweet Orange Java obfuscated binary (3)
- [ ] ET EXPLOIT_KIT Sweet Orange applet with obfuscated URL April 01 2013
- [ ] ET EXPLOIT_KIT CrimeBoss Recent Jar (4)
- [ ] ET EXPLOIT_KIT BHEK ff.php iframe inbound
- [ ] ET EXPLOIT_KIT BHEK ff.php iframe outbound
- [ ] ET EXPLOIT_KIT Potential Fiesta Flash Exploit
- [x] ET EXPLOIT_KIT RedKit applet + obfuscated URL Apr 7 2013
- [ ] ET EXPLOIT_KIT GonDadEK Java Exploit Requested
- [x] ET EXPLOIT_KIT RedKit/Sakura/CritX/SafePack/FlashPack applet + obfuscated URL Apr 10 2013
- [ ] ET EXPLOIT_KIT Sakura obfuscated javascript Apr 21 2013
- [ ] ET EXPLOIT_KIT Sakura - Java Exploit Recievied
- [ ] ET EXPLOIT_KIT Sakura - Payload Downloaded
- [x] ET EXPLOIT_KIT Possible Java Applet JNLP applet_ssv_validated in Base64
- [ ] ET EXPLOIT_KIT Magnitude EK (formerly Popads) Java JNLP Requested
- [ ] ET EXPLOIT_KIT Unknown_MM - Java Exploit - jreg.jar
- [ ] ET EXPLOIT_KIT Eval With Base64.decode seen in DOL Watering Hole Attack 05/01/13
- [ ] ET EXPLOIT_KIT Possible Java Applet JNLP applet_ssv_validated in Base64 2
- [ ] ET EXPLOIT_KIT Unknown EK Requsting Payload
- [ ] ET EXPLOIT_KIT HellSpawn EK Requesting Jar
- [x] ET EXPLOIT_KIT FlimKit hex.zip Java Downloading Jar
- [ ] ET EXPLOIT_KIT Sakura obfuscated javascript May 10 2013
- [x] ET EXPLOIT_KIT FlimKit Post Exploit Payload Download
- [ ] ET EXPLOIT_KIT KaiXin Exploit Kit Java Class 1 May 24 2013
- [ ] ET EXPLOIT_KIT KaiXin Exploit Landing Page 1 May 24 2013
- [x] ET EXPLOIT_KIT HellSpawn EK Landing 1 May 24 2013
- [ ] ET EXPLOIT_KIT Possible HellSpawn EK Fake Flash May 24 2013
- [ ] ET EXPLOIT_KIT Sakura - Landing Page - Received May 29 2013
- [ ] ET EXPLOIT_KIT Sakura encrypted binary (2)
- [ ] ET EXPLOIT_KIT CritX/SafePack Reporting Plugin Detect Data June 03 2013
- [x] ET EXPLOIT_KIT Sakura obfuscated javascript Jun 1 2013
- [ ] ET EXPLOIT_KIT Glazunov EK Downloading Jar
- [ ] ET EXPLOIT_KIT Unknown EK Jar 1 June 12 2013
- [ ] ET EXPLOIT_KIT Unknown EK Jar 3 June 12 2013
- [ ] ET EXPLOIT_KIT Dotka Chef EK exploit/payload URI request
- [ ] ET EXPLOIT_KIT CritX/SafePack/FlashPack URI Format June 17 2013 2
- [ ] ET EXPLOIT_KIT Unknown_InlFRAME - URI Structure
- [ ] ET EXPLOIT_KIT Unknown_InlFRAME - In Referer
- [ ] ET EXPLOIT_KIT RedKit Jar Download June 20 2013
- [ ] ET EXPLOIT_KIT Rawin Exploit Kit Landing URI Struct
- [ ] ET EXPLOIT_KIT Rawin Exploit Kit Jar 1.6 (Old)
- [ ] ET EXPLOIT_KIT Rawin Exploit Kit Jar 1.6 (New)

- [ ] ET EXPLOIT_KIT Cool/BHEK/Goon Applet with Alpha-Numeric Encoded HTML entity
- [ ] ET EXPLOIT_KIT Neutrino Exploit Kit Clicker.php TDS
- [ ] ET EXPLOIT_KIT Neutrino Exploit Kit XOR decodeURIComponent
- [ ] ET EXPLOIT_KIT Sweet Orange applet structure June 27 2013
- [ ] ET EXPLOIT_KIT Lucky7 Java Exploit URI Struct June 28 2013
- [ ] ET EXPLOIT_KIT CritX/SafePack/FlashPack Jar Download Jul 01 2013
- [ ] ET EXPLOIT_KIT Unknown Malvertising Exploit Kit Hostile Jar pipe.class
- [ ] ET EXPLOIT_KIT Unknown Malvertising Exploit Kit Hostile Jar cm2.jar
- [ ] ET EXPLOIT_KIT Lucky7 EK IE Exploit
- [ ] ET EXPLOIT_KIT /Styx EK - /jovf.html
- [ ] ET EXPLOIT_KIT FlimKit Landing Applet Jul 05 2013
- [ ] ET EXPLOIT_KIT Styx iframe with obfuscated Java version check Jul 04 2013
- [x] ET EXPLOIT_KIT Cool Exploit Kit Plugin-Detect July 08 2013
- [ ] ET EXPLOIT_KIT CritX/SafePack Java Exploit Payload June 03 2013
- [ ] ET EXPLOIT_KIT DotkaChef JJencode Script URI Struct
- [ ] ET EXPLOIT_KIT Styx PDF July 15 2013
- [ ] ET EXPLOIT_KIT FlimKit JNLP URI Struct
- [ ] ET EXPLOIT_KIT X20 EK Landing July 22 2013
- [x] ET EXPLOIT_KIT Sibhost/FlimKit/Glazunov Jar with lowercase class names
- [x] ET EXPLOIT_KIT Java UA Requesting Numeric.ext From Base Dir (Observed in Redkit/Sakura)
- [x] ET EXPLOIT_KIT Possible Java Applet JNLP applet_ssv_validated in Base64 (Reversed)
- [x] ET EXPLOIT_KIT Possible Java Applet JNLP applet_ssv_validated in Base64 2 (Reversed)
- [ ] ET EXPLOIT_KIT PluginDetect plus Java version check
- [ ] ET EXPLOIT_KIT %Hex Encoded jnlp_embedded (Observed in Sakura)
- [ ] ET EXPLOIT_KIT %Hex Encoded/base64 1 applet_ssv_validated (Observed in Sakura)
- [ ] ET EXPLOIT_KIT %Hex Encoded/base64 3 applet_ssv_validated (Observed in Sakura)
- [ ] ET EXPLOIT_KIT Plugin-Detect with global % replace on unescaped string (Sakura)
- [ ] ET EXPLOIT_KIT Rawin EK Java 1.7 /caramel.jar
- [ ] ET EXPLOIT_KIT X20 EK Download Aug 07 2013
- [ ] ET EXPLOIT_KIT FlimKit obfuscated hex-encoded jnlp_embedded Aug 08 2013
- [ ] ET EXPLOIT_KIT Styx EK - /jvvn.html
- [ ] ET EXPLOIT_KIT Possible BHEK Landing URI Format
- [ ] ET EXPLOIT_KIT Sweet Orange Landing with Applet Aug 30 2013
- [x] ET EXPLOIT_KIT Sakura Landing with Applet Aug 30 2013
- [ ] ET EXPLOIT_KIT Sakura EK Landing Sep 06 2013
- [ ] ET EXPLOIT_KIT Unknown Bleeding EK Variant Landing JAR Sep 06 2013
- [ ] ET EXPLOIT_KIT CottonCastle EK Java Jar
- [ ] ET EXPLOIT_KIT Possible SNET EK VBS Download
- [x] ET EXPLOIT_KIT SNET EK Encoded VBS 2
- [ ] ET EXPLOIT_KIT Possible CoolEK Variant Payload Download Sep 16 2013
- [x] ET EXPLOIT_KIT DRIVEBY SweetOrange - Java Exploit Downloaded
- [ ] ET EXPLOIT_KIT Unknown EK Using Office/.Net ROP/ASLR Bypass
- [ ] ET EXPLOIT_KIT Unknown EK Using Office/.Net ROP/ASLR Bypass
- [ ] ET EXPLOIT_KIT Unknown EK Using Office/.Net ROP/ASLR Bypass
- [ ] ET EXPLOIT_KIT Rawin EK - Java Exploit - bona.jar
- [ ] ET EXPLOIT_KIT LightsOut EK Payload Download
- [ ] ET EXPLOIT_KIT Possible LightsOut EK info3i.php
- [ ] ET EXPLOIT_KIT Possible LightsOut EK sort.html
- [ ] ET EXPLOIT_KIT Possible LightsOut EK negc.html
- [ ] ET EXPLOIT_KIT Possible LightsOut EK leks.jar
- [x] ET EXPLOIT_KIT Neutrino Exploit Kit Redirector To Landing Page
- [ ] ET EXPLOIT_KIT Applet tag in jjencode as (as seen in Dotka Chef EK)
- [ ] ET EXPLOIT_KIT Cool Exploit Kit iframe with obfuscated Java version check Jun 26 2013
- [x] ET EXPLOIT_KIT Redirect to DotkaChef EK Landing
- [ ] ET EXPLOIT_KIT Sibhost Status Check GET Jul 01 2013
- [ ] ET EXPLOIT_KIT CritX/SafePack/FlashPack EXE Download Jul 01 2013
- [x] ET EXPLOIT_KIT Unknown Malvertising Exploit Kit Hostile Jar app.jar
- [x] ET EXPLOIT_KIT Lucky7 EK Landing Encoded Plugin-Detect
- [ ] ET EXPLOIT_KIT /Styx EK - /jlnp.html
- [ ] ET EXPLOIT_KIT /Styx EK - /jorg.html
- [ ] ET EXPLOIT_KIT Sweet Orange applet structure Jul 05 2013
- [ ] ET EXPLOIT_KIT Sweet Orange applet July 08 2013
- [ ] ET EXPLOIT_KIT Sibhost Zip as Applet Archive July 08 2013
- [ ] ET EXPLOIT_KIT g01pack - Java JNLP Requested
- [x] ET EXPLOIT_KIT Cool PDF July 15 2013
- [ ] ET EXPLOIT_KIT FlimKit Jar URI Struct
- [x] ET EXPLOIT_KIT Sibhost Zip as Applet Archive July 08 2013
- [ ] ET EXPLOIT_KIT DRIVEBY Rawin - Landing Page Received
- [ ] ET EXPLOIT_KIT DRIVEBY Possible CritXPack - Landing Page - jnlp_embedded
- [ ] ET EXPLOIT_KIT Possible Sakura Jar Download
- [x] ET EXPLOIT_KIT Possible Java Applet JNLP applet_ssv_validated Click To Run Bypass (Reversed)
- [x] ET EXPLOIT_KIT Possible Java Applet JNLP applet_ssv_validated in Base64 3 (Reversed)
- [x] ET EXPLOIT_KIT %Hex Encoded Applet (Observed in Sakura)
- [ ] ET EXPLOIT_KIT %Hex Encoded applet_ssv_validated (Observed in Sakura)
- [ ] ET EXPLOIT_KIT %Hex Encoded/base64 2 applet_ssv_validated (Observed in Sakura)
- [ ] ET EXPLOIT_KIT Styx Exploit Kit Landing Applet With Payload Aug 02 2013
- [ ] ET EXPLOIT_KIT Rawin EK Java (Old) /golem.jar
- [ ] ET EXPLOIT_KIT Styx iframe with obfuscated Java version check Jul 04 2013
- [ ] ET EXPLOIT_KIT Rawin -TDS - POST w/Java Version
- [ ] ET EXPLOIT_KIT Unknown EK setSecurityManager hex August 14 2013
- [ ] ET EXPLOIT_KIT Sweet Orange Landing with Applet Aug 26 2013
- [ ] ET EXPLOIT_KIT Unknown EK Landing Aug 27 2013
- [ ] ET EXPLOIT_KIT Rawin EK Java /victoria.jar
- [ ] ET EXPLOIT_KIT GondadEK Landing Sept 03 2013
- [x] ET EXPLOIT_KIT Unknown Bleeding EK Variant Landing Sep 06 2013
- [ ] ET EXPLOIT_KIT FlimKit Landing Page
- [x] ET EXPLOIT_KIT Unknown EK Fake Microsoft Security Update Applet Sep 16 2013
- [x] ET EXPLOIT_KIT SNET EK Encoded VBS 1
- [x] ET EXPLOIT_KIT SNET EK Encoded VBS 3
- [ ] ET EXPLOIT_KIT CoolEK Variant Landing Page - Applet Sep 16 2013
- [x] ET EXPLOIT_KIT DRIVEBY Styx - TDS - Redirect To Landing Page
- [ ] ET EXPLOIT_KIT Unknown EK Using Office/.Net ROP/ASLR Bypass
- [ ] ET EXPLOIT_KIT Unknown EK Using Office/.Net ROP/ASLR Bypass
- [ ] ET EXPLOIT_KIT Unknown EK Using Office/.Net ROP/ASLR Bypass
- [ ] ET EXPLOIT_KIT Unknown EK Used in various watering hole attacks
- [ ] ET EXPLOIT_KIT Possible LightsOut EK info3i.html
- [ ] ET EXPLOIT_KIT Possible LightsOut EK inden2i.html
- [ ] ET EXPLOIT_KIT Possible LightsOut EK leks.html
- [ ] ET EXPLOIT_KIT Possible LightsOut EK negq.html
- [ ] ET EXPLOIT_KIT Possible LightsOut EK start.jar

- [ ] ET EXPLOIT_KIT Possible LightsOut EK stoq.jar
- [ ] ET EXPLOIT_KIT Possible LightsOut EK inden2i.php
- [ ] ET EXPLOIT_KIT Possible LightsOut EK gami.jar
- [x] ET EXPLOIT_KIT Sweet Orange Landing with Applet Sep 30 2013
- [ ] ET EXPLOIT_KIT HiMan EK Landing Oct 1 2013
- [ ] ET EXPLOIT_KIT HiMan EK Reporting Host/Exploit Info
- [x] ET EXPLOIT_KIT DotkaChef EK initial landing from Oct 02 2013 mass-site compromise EK campaign
- [ ] ET EXPLOIT_KIT Unknown EK Landing
- [ ] ET EXPLOIT_KIT Styx EK jply.html
- [ ] ET EXPLOIT_KIT Fake MS Security Update EK (Payload Download)
- [ ] ET EXPLOIT_KIT Unknown Malvertising Related EK Landing Oct 14 2013
- [ ] ET EXPLOIT_KIT Magnitude EK - Landing Page - Java ClassID and 32/32 archive Oct 16 2013
- [ ] ET EXPLOIT_KIT Possible Magnitude EK (formerly Popads) IE Exploit with IE UA Oct 16 2013
- [x] ET EXPLOIT_KIT Styx Landing Page Oct 25 2013
- [x] ET EXPLOIT_KIT Java File Sent With X-Powered By HTTP Header - Common In Exploit Kits
- [ ] ET EXPLOIT_KIT Sweet Orange encrypted payload
- [ ] ET EXPLOIT_KIT Nuclear EK JAR URI Struct Nov 05 2013
- [ ] ET EXPLOIT_KIT Styx iframe with obfuscated CVE-2013-2551
- [ ] ET EXPLOIT_KIT Grandsoft/SofosFO EK PDF URI Struct
- [x] ET EXPLOIT_KIT Possible Styx EK SilverLight Payload
- [x] ET EXPLOIT_KIT Possible WhiteLotus EK 2013-2551 Exploit 1
- [x] ET EXPLOIT_KIT Possible WhiteLotus EK 2013-2551 Exploit 3
- [ ] ET EXPLOIT_KIT StyX EK Payload Cookie
- [ ] ET EXPLOIT_KIT Possible Goon EK Jar Download
- [ ] ET EXPLOIT_KIT Possible Java Lang Runtime in B64 Observed in Goon EK 2
- [ ] ET EXPLOIT_KIT Nuclear EK CVE-2013-2551 URI Struct Nov 26 2013
- [ ] ET EXPLOIT_KIT SNET EK Activity Nov 27 2013
- [ ] ET EXPLOIT_KIT HiMan EK - Landing Page
- [ ] ET EXPLOIT_KIT Magnitude EK (formerly Popads) Java Jar Download
- [x] ET EXPLOIT_KIT Sweet Orange Landing Page Dec 09 2013
- [ ] ET EXPLOIT_KIT heapSpray in jjencode
- [ ] ET EXPLOIT_KIT SPL2 EK Dec 09 2013 Java Request
- [ ] ET EXPLOIT_KIT Styx Exploit Kit - EOT Exploit
- [ ] ET EXPLOIT_KIT Possible CVE-2013-2551 As seen in SPL2 EK
- [ ] ET EXPLOIT_KIT HiMan EK Secondary Landing
- [ ] ET EXPLOIT_KIT CrimePack PDF Exploit
- [ ] ET EXPLOIT_KIT CrimePack HCP Exploit
- [ ] ET EXPLOIT_KIT CrimePack Jar 2 Dec 16 2013
- [ ] ET EXPLOIT_KIT DotkaChef Payload Dec 20 2013
- [ ] ET EXPLOIT_KIT GoonEK Landing with CVE-2013-2551 Dec 29 2013
- [ ] ET EXPLOIT_KIT GoonEK Landing Jan 10 2014
- [ ] ET EXPLOIT_KIT Nuclear EK CVE-2013-3918
- [ ] ET EXPLOIT_KIT GoonEK Landing Jan 21 2013 SilverLight 1
- [ ] ET EXPLOIT_KIT GoonEK Landing Jan 21 2013 SilverLight 3
- [ ] ET EXPLOIT_KIT Goon EK Java JNLP URI Struct Feb 12 2014
- [ ] ET EXPLOIT_KIT GoonEK Landing Feb 19 2014 2
- [ ] ET EXPLOIT_KIT OnClick Anti-BOT TDS Hidden Form Feb 25 2014
- [ ] ET EXPLOIT_KIT LightsOut EK Exploit/Payload Request
- [x] ET EXPLOIT_KIT SWF filename used in IE 2014-0322 Watering Hole Attacks
- [ ] ET EXPLOIT_KIT Possible Neutrino/Fiesta EK SilverLight Exploit March 05 2014 DLL Naming Convention
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK CVE-2013-2551 URI Struct Nov 26 2013
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK Landing Page Mar 12 2014
- [ ] ET EXPLOIT_KIT GoonEK Landing Mar 20 2014
- [ ] ET EXPLOIT_KIT Possible LightsOut EK erno_rfq.html
- [ ] ET EXPLOIT_KIT Possible LightsOut EK gami.html
- [x] ET EXPLOIT_KIT LightsOut EK POST Compromise POST
- [ ] ET EXPLOIT_KIT CoolEK Jar Download Sep 30 2013
- [ ] ET EXPLOIT_KIT Obfuscated http 2 digit sep in applet (Seen in HiMan EK)
- [x] ET EXPLOIT_KIT BHEK Payload Download (java only alternate method may overlap with 2017454)
- [x] ET EXPLOIT_KIT Sweet Orange Landing with Applet Oct 4 2013
- [ ] ET EXPLOIT_KIT FiestaEK js-redirect
- [ ] ET EXPLOIT_KIT Fiesta EK Landing Oct 09 2013
- [ ] ET EXPLOIT_KIT Unknown EK Initial Payload Internet Connectivity Check
- [ ] ET EXPLOIT_KIT Nuclear EK CVE-2013-2551 IE Exploit URI Struct
- [x] ET EXPLOIT_KIT Magnitude EK (formerly Popads) Java Exploit 32-32 byte hex java payload request Oct 16 2013
- [ ] ET EXPLOIT_KIT Sweet Orange Landing Page Oct 25 2013
- [ ] ET EXPLOIT_KIT Nuclear EK PDF URI Struct
- [ ] ET EXPLOIT_KIT Possible Sweet Orange payload Request
- [ ] ET EXPLOIT_KIT SofosFO/Grandsoft Plugin-Detect
- [ ] ET EXPLOIT_KIT Nuclear EK Payload URI Struct Nov 05 2013
- [x] ET EXPLOIT_KIT Possible Magnitude IE EK Payload Nov 8 2013
- [ ] ET EXPLOIT_KIT Possible Sweet Orange IE Payload Request
- [ ] ET EXPLOIT_KIT WhiteLotus EK PluginDetect Nov 20 2013
- [x] ET EXPLOIT_KIT Possible WhiteLotus EK 2013-2551 Exploit 2
- [ ] ET EXPLOIT_KIT Sweet Orange Landing Page Nov 21 2013
- [ ] ET EXPLOIT_KIT Possible Goon EK Java Payload
- [ ] ET EXPLOIT_KIT Possible Java Lang Runtime in B64 Observed in Goon EK 1
- [ ] ET EXPLOIT_KIT Possible Java Lang Runtime in B64 Observed in Goon EK 3
- [ ] ET EXPLOIT_KIT Nuclear EK IE Exploit CVE-2013-2551
- [ ] ET EXPLOIT_KIT HiMan EK - Flash Exploit
- [ ] ET EXPLOIT_KIT HiMan EK - TDS - POST hyt=
- [x] ET EXPLOIT_KIT Safe/CritX/FlashPack URI Struct .php?id=Hex
- [ ] ET EXPLOIT_KIT Styx EK iexp.html
- [ ] ET EXPLOIT_KIT SPL2 EK Landing Dec 09 2013
- [ ] ET EXPLOIT_KIT Styx Exploit Kit - JAR Exploit
- [ ] ET EXPLOIT_KIT SPL2 EK SilverLight
- [ ] ET EXPLOIT_KIT HiMan EK Exploit URI Struct
- [ ] ET EXPLOIT_KIT Grandsoft/SofosFO EK Java Payload URI Struct
- [ ] ET EXPLOIT_KIT CrimePack Java Exploit
- [ ] ET EXPLOIT_KIT CrimePack Jar 1 Dec 16 2013
- [ ] ET EXPLOIT_KIT DotkaChef Landing URI Struct
- [ ] ET EXPLOIT_KIT TDS Unknown_.aso - URI - IP.aso
- [ ] ET EXPLOIT_KIT GoonEK encrypted binary (1)
- [ ] ET EXPLOIT_KIT Possible Neutrino/Fiesta EK SilverLight Exploit Jan 13 2014 DLL Naming Convention
- [ ] ET EXPLOIT_KIT Possible AnglerEK Landing URI Struct
- [ ] ET EXPLOIT_KIT GoonEK Landing Jan 21 2013 SilverLight 2
- [ ] ET EXPLOIT_KIT Fiesta EK Landing Jan 24 2013
- [ ] ET EXPLOIT_KIT Possible GoonEK Landing Feb 19 2014 1
- [ ] ET EXPLOIT_KIT OnClick Anti-BOT TDS POST Feb 25 2014
- [ ] ET EXPLOIT_KIT Hello/LightsOut EK Secondary Landing
- [ ] ET EXPLOIT_KIT Rawin EK Java fakav.jar
- [ ] ET EXPLOIT_KIT Possible Fiesta Jar with four-letter class names
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK PDF URI Struct March 12 2014
- [ ] ET EXPLOIT_KIT DRIVEBY Styx Landing Page Mar 08 2014
- [x] ET EXPLOIT_KIT GoonEK encrypted binary (3)
- [ ] ET EXPLOIT_KIT DRIVEBY Possible CritX/SafePack/FlashPack IE Exploit

- [ ] ET EXPLOIT_KIT DRIVEBY Goon/Infinity EK Landing Mar 31 2014
- [ ] ET EXPLOIT_KIT EvilTDS Redirection
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK SWF Struct
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK PDF
- [x] ET EXPLOIT_KIT DRIVEBY EL8 EK Landing
- [x] ET EXPLOIT_KIT Fiesta SilverLight Exploit Download
- [ ] ET EXPLOIT_KIT DRIVEBY Goon/Infinity EK Landing May 05 2014
- [ ] ET EXPLOIT_KIT 32-byte by 32-byte PHP EK Gate with HTTP POST
- [ ] ET EXPLOIT_KIT DRIVEBY FlashPack 2013-2551 May 13 2014
- [ ] ET EXPLOIT_KIT DRIVEBY FlashPack Flash Exploit flash2014.php
- [ ] ET EXPLOIT_KIT Gongda EK Secondary Landing
- [ ] ET EXPLOIT_KIT Gongda EK Landing 2
- [ ] ET EXPLOIT_KIT CottonCastle EK Landing June 05 2014
- [ ] ET EXPLOIT_KIT DRIVEBY FlashPack Flash Exploit flash0515.php
- [ ] ET EXPLOIT_KIT CottonCastle EK Jar Download Method 2
- [ ] ET EXPLOIT_KIT BleedingLife Exploit Kit SWF Exploit Request
- [ ] ET EXPLOIT_KIT Safe/CritX/FlashPack EK Secondary Landing
- [ ] ET EXPLOIT_KIT Sweet Orange EK Common Java Exploit
- [ ] ET EXPLOIT_KIT Safe/CritX/FlashPack EK CVE-2013-3918
- [ ] ET EXPLOIT_KIT Safe/CritX/FlashPack EK Secondary Landing June 25 2014
- [ ] ET EXPLOIT_KIT Safe/CritX/FlashPack EK Secondary Landing Jul 11 2014
- [ ] ET EXPLOIT_KIT Fiesta EK randomized javascript Gate Jul 18 2014
- [ ] ET EXPLOIT_KIT XMLDOM Check for Presence Kaspersky AV Observed in RIG EK
- [ ] ET EXPLOIT_KIT Sweet Orange EK CDN Landing Page
- [ ] ET EXPLOIT_KIT Safe/CritX/FlashPack EK Plugin Detect IE Exploit
- [ ] ET EXPLOIT_KIT Safe/CritX/FlashPack EK Plugin Detect Flash Exploit
- [x] ET EXPLOIT_KIT Nuclear Exploit Kit exe.exe Payload
- [ ] ET EXPLOIT_KIT Turla/SPL EK Java Applet
- [ ] ET EXPLOIT_KIT Turla/SPL EK Java Exploit
- [ ] ET EXPLOIT_KIT DRIVEBY Archie.EK PluginDetect URI Struct
- [ ] ET EXPLOIT_KIT DRIVEBY Archie.EK Landing
- [ ] ET EXPLOIT_KIT Malvertising Leading to EK Aug 19 2014 M1
- [ ] ET EXPLOIT_KIT Sweet Orange EK Thread Specific Java Exploit
- [ ] ET EXPLOIT_KIT Unknown Malvertising EK Landing URI Sruct Aug 22 2014
- [ ] ET EXPLOIT_KIT Unknown Malvertising EK Silverlight URI Sruct Aug 22 2014
- [ ] ET EXPLOIT_KIT Unknown Malvertising EK Payload URI Sruct Aug 22 2014
- [ ] ET EXPLOIT_KIT Archie EK CVE-2014-0497 Aug 24 2014
- [ ] ET EXPLOIT_KIT Archie EK Landing Aug 24 2014
- [ ] ET EXPLOIT_KIT FlashPack EK Redirect Aug 25 2014
- [ ] ET EXPLOIT_KIT FlashPack EK JS Include Aug 25 2014
- [ ] ET EXPLOIT_KIT NullHole EK Landing Aug 27 2014
- [ ] ET EXPLOIT_KIT NullHole EK Landing Redirect Aug 27 2014
- [x] ET EXPLOIT_KIT ScanBox Framework used in WateringHole Attacks Initial (POST)
- [ ] ET EXPLOIT_KIT Archie EK Sending Plugin-Detect Data
- [ ] ET EXPLOIT_KIT FlashPack EK Redirect Sept 01 2014
- [ ] ET EXPLOIT_KIT Astrum EK Landing
- [ ] ET EXPLOIT_KIT Sweet Orange EK Java Exploit
- [x] ET EXPLOIT_KIT Possible Astrum EK URI Struct
- [ ] ET EXPLOIT_KIT Fiesta EK Gate
- [x] ET EXPLOIT_KIT Nuclear EK Gate Sep 16 2014
- [ ] ET EXPLOIT_KIT Nuclear EK CVE-2013-2551 URI Struct Sept 17 2014
- [ ] ET EXPLOIT_KIT Nuclear EK Redirect Sept 18 2014
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK PDF Struct (no alert)
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK 2013-3918
- [ ] ET EXPLOIT_KIT DRIVEBY Possible Job314 EK JAR URI Struct
- [ ] ET EXPLOIT_KIT Possible Sweet Orange redirection 19 September 2014

- [ ] ET EXPLOIT_KIT DRIVEBY Goon/Infinity EK Landing Mar 31 2014
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK SWF Struct
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK SWF
- [x] ET EXPLOIT_KIT DRIVEBY Possible Goon/Infinity/Magnitude EK SilverLight Exploit
- [x] ET EXPLOIT_KIT Fiesta URI Struct
- [x] ET EXPLOIT_KIT Fiesta Flash Exploit Download
- [ ] ET EXPLOIT_KIT Goon/Infinity URI Struct EK Landing May 05 2014
- [x] ET EXPLOIT_KIT DRIVEBY Nuclear EK Landing May 05 2014
- [ ] ET EXPLOIT_KIT DRIVEBY FlashPack Flash Exploit flash2013.php
- [x] ET EXPLOIT_KIT DRIVEBY FlashPack Plugin-Detect May 13 2014
- [ ] ET EXPLOIT_KIT Gongda EK Landing 1
- [x] ET EXPLOIT_KIT CottonCastle EK URI Struct
- [ ] ET EXPLOIT_KIT CottonCastle EK Landing EK Struct
- [ ] ET EXPLOIT_KIT CottonCastle EK Landing June 05 2014 2
- [ ] ET EXPLOIT_KIT BleedingLife Exploit Kit Landing Page Requested
- [ ] ET EXPLOIT_KIT BleedingLife Exploit Kit JAR Exploit Request
- [ ] ET EXPLOIT_KIT Safe/CritX/FlashPack EK Secondary Landing 2
- [ ] ET EXPLOIT_KIT Multiple EKs CVE-2013-3918
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK Landing May 23 2014
- [ ] ET EXPLOIT_KIT Evil EK Redirector Cookie June 27 2014
- [ ] ET EXPLOIT_KIT Fake CDN Sweet Orange Gate July 17 2014
- [x] ET EXPLOIT_KIT Possible Sweet Orange redirection 21 July 2014
- [ ] ET EXPLOIT_KIT XMLDOM Check for Presence TrendMicro AV Observed in RIG EK
- [ ] ET EXPLOIT_KIT Safe/CritX/FlashPack EK Secondary Landing June 28 2014
- [ ] ET EXPLOIT_KIT Safe/CritX/FlashPack EK Plugin Detect Java Exploit
- [ ] ET EXPLOIT_KIT Malvertising Redirection to Exploit Kit Aug 07 2014
- [ ] ET EXPLOIT_KIT DRIVEBY Malicious Plugin Detect URI struct
- [ ] ET EXPLOIT_KIT Turla/SPL EK Java Exploit
- [ ] ET EXPLOIT_KIT Turla/SPL EK Java Exploit Requested - /spl/
- [ ] ET EXPLOIT_KIT DRIVEBY Archie.EK CVE-2013-2551 URI Struct
- [ ] ET EXPLOIT_KIT Malvertising Leading to EK Aug 19 2014 M3
- [ ] ET EXPLOIT_KIT Malvertising Leading to EK Aug 19 2014 M2
- [ ] ET EXPLOIT_KIT Unknown Malvertising EK Landing Aug 22 2014
- [ ] ET EXPLOIT_KIT Unknown Malvertising EK Payload URI Sruct Aug 22 2014
- [ ] ET EXPLOIT_KIT Unknown Malvertising EK Flash URI Sruct Aug 22 2014
- [ ] ET EXPLOIT_KIT Archie EK CVE-2014-0515 Aug 24 2014
- [ ] ET EXPLOIT_KIT Archie EK Secondary Landing Aug 24 2014
- [ ] ET EXPLOIT_KIT FlashPack EK Exploit Flash Post Aug 25 2014
- [ ] ET EXPLOIT_KIT FlashPack EK Exploit Landing Aug 25 2014
- [ ] ET EXPLOIT_KIT BleedingLife EK Variant Aug 26 2014
- [ ] ET EXPLOIT_KIT RIG EK Landing URI Struct
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK Landing Aug 27 2014
- [ ] ET EXPLOIT_KIT Archie EK SilverLight URI Struct
- [x] ET EXPLOIT_KIT Possible Archie/Metasploit SilverLight Exploit
- [ ] ET EXPLOIT_KIT Astrum EK Landing
- [ ] ET EXPLOIT_KIT Sweet Orange CDN Gate Sept 09 2014 Method 2
- [ ] ET EXPLOIT_KIT Nuclear EK Silverlight URI Struct
- [ ] ET EXPLOIT_KIT Malvertising Leading to EK Aug 19 2014 M4
- [ ] ET EXPLOIT_KIT Fiesta EK Silverlight Based Redirect
- [ ] ET EXPLOIT_KIT Nuclear EK CVE-2013-2551 Sept 17 2014
- [ ] ET EXPLOIT_KIT RIG EK Landing Page Sept 17 2014
- [ ] ET EXPLOIT_KIT Nuclear EK Redirect Sept 18 2014
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK PDF
- [ ] ET EXPLOIT_KIT DRIVEBY Job314 EK Landing
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK Landing Sep 29 2014
- [ ] ET EXPLOIT_KIT Nuclear EK Payload URI Struct Oct 5 2014 (no alert)

- [ ] ET EXPLOIT_KIT Nuclear EK Payload URI Struct Oct 5 2014
- [x] ET EXPLOIT_KIT DRIVEBY Sednit EK IE Exploit CVE-2014-1776 M1
- [x] ET EXPLOIT_KIT DRIVEBY Generic CollectGarbage in JJEncode (Observed in Sednit)
- [ ] ET EXPLOIT_KIT Job314 EK URI Landing Struct
- [ ] ET EXPLOIT_KIT Likely SweetOrange EK Java Exploit Struct (JAR)
- [ ] ET EXPLOIT_KIT Possible Sweet Orange Flash/IE Payload Request
- [ ] ET EXPLOIT_KIT Likely SweetOrange EK Java Exploit Struct (JNLP)
- [x] ET EXPLOIT_KIT Fiesta SilverLight 5.x Exploit URI Struct
- [ ] ET EXPLOIT_KIT Evil EK Redirector Cookie Nov 03 2014
- [x] ET EXPLOIT_KIT Fiesta EK Landing Nov 05 2014
- [ ] ET EXPLOIT_KIT Archie EK Exploit Flash URI Struct
- [ ] ET EXPLOIT_KIT Archie EK Exploit IE URI Struct
- [x] ET EXPLOIT_KIT Nuclear SilverLight Exploit
- [ ] ET EXPLOIT_KIT Possible HanJuan EK URI Struct Actor Specific
- [ ] ET EXPLOIT_KIT Nuclear EK Payload URI Struct Nov 07 2014
- [ ] ET EXPLOIT_KIT Evil EK Redirector Cookie Nov 07 2014
- [ ] ET EXPLOIT_KIT Job314 EK Landing Nov 10 2014
- [ ] ET EXPLOIT_KIT Archie EK Landing Nov 17 2014
- [ ] ET EXPLOIT_KIT Archie EK Flash Exploit URI Struct Nov 17 2014
- [ ] ET EXPLOIT_KIT Archie EK Landing URI Struct 2 Nov 17 2014
- [ ] ET EXPLOIT_KIT SPL2 EK Landing Nov 18 2014
- [ ] ET EXPLOIT_KIT SPL2 EK JS HashLib Nov 18 2014
- [ ] ET EXPLOIT_KIT SweetOrange EK Landing Nov 19 2014
- [ ] ET EXPLOIT_KIT Archie EK T2 PD Struct Nov 20 2014
- [ ] ET EXPLOIT_KIT Archie EK T2 SWF Exploit Struct Nov 20 2014
- [ ] ET EXPLOIT_KIT Malicious Iframe Leading to EK
- [x] ET EXPLOIT_KIT WinHttpRequest Downloading EXE Non-Port 80 (Likely Exploit Kit)
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK SWF
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK Payload (flowbits set)
- [ ] ET EXPLOIT_KIT Nuclear EK Landing Dec 03 2014
- [ ] ET EXPLOIT_KIT Probable malicious download from e-mail link /1.php
- [ ] ET EXPLOIT_KIT Nuclear EK SilverLight Exploit
- [ ] ET EXPLOIT_KIT Malicious Referer Bulk Traffic Sometimes Leading to EKs (Possible Bedep infection) Dec 16 2014
- [ ] ET EXPLOIT_KIT Archie EK T2 Activity Dec 18 2014
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Dec 22 2014 Player
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK Landing Dec 29 2014
- [ ] ET EXPLOIT_KIT Nuclear EK Landing Jan 14 2014
- [ ] ET EXPLOIT_KIT Nuclear EK Landing Jan 21 2014
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK Exploit Struct Jan 23 2015
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK SWF M2
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK Landing Jan 27 2015 M1
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK Landing Feb 01 2015 M2
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK Landing Feb 03 2015 M2
- [x] ET EXPLOIT_KIT KaiXin Landing Page M2
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Feb 11 2015 Blog
- [x] ET EXPLOIT_KIT Unknown EK Landing Feb 16 2015 b64 2 M1
- [x] ET EXPLOIT_KIT Double-Encoded Reverse Base64/Dean Edwards Packed JavaScript Observed in Unknown EK Feb 16 2015 b64 1 M2
- [x] ET EXPLOIT_KIT Unknown EK Landing Feb 16 2015 b64 3 M2
- [x] ET EXPLOIT_KIT KaiXin EK Jar URI Struct
- [ ] ET EXPLOIT_KIT KaiXin EK Possible Jar Download
- [x] ET EXPLOIT_KIT KaiXin Secondary Landing Page M2
- [ ] ET EXPLOIT_KIT DRIVEBY Possible Unknown EK HFS CVE-2014-6332
- [ ] ET EXPLOIT_KIT DRIVEBY Unknown EK Landing
- [x] ET EXPLOIT_KIT DRIVEBY [PwC CTD] -- MultiGroup - ScanBox Watering Hole iframe
- [x] ET EXPLOIT_KIT DRIVEBY [PwC CTD] -- MultiGroup - ScanBox Watering Hole Content form tag appended to head
- [x] ET EXPLOIT_KIT DRIVEBY [PwC CTD] -- MultiGroup - TH3BUG and Non-Targetted Groups Watering Hole Deobfuscation function
- [x] ET EXPLOIT_KIT DRIVEBY Sednit EK Landing
- [x] ET EXPLOIT_KIT DRIVEBY Sednit EK IE Exploit CVE-2013-1347 M1
- [ ] ET EXPLOIT_KIT Job314 EK URI Exploit/Payload Struct
- [x] ET EXPLOIT_KIT Nuclear EK Gate Injected iframe Oct 22 2014
- [ ] ET EXPLOIT_KIT Likely SweetOrange EK Flash Exploit URI Struct
- [ ] ET EXPLOIT_KIT FlashPack EK Plugin-Detect Post
- [x] ET EXPLOIT_KIT Fiesta Flash Exploit URI Struct
- [ ] ET EXPLOIT_KIT Sweet Orange Landing Nov 3 2014
- [ ] ET EXPLOIT_KIT Possible Sweet Orange redirection Nov 4 2014
- [ ] ET EXPLOIT_KIT Archie EK Exploit Flash URI Struct
- [ ] ET EXPLOIT_KIT Archie EK Exploit SilverLight URI Struct
- [x] ET EXPLOIT_KIT Nuclear SilverLight URI Struct (noalert)
- [ ] ET EXPLOIT_KIT Possible HanJuan EK Flash Payload DL
- [ ] ET EXPLOIT_KIT Possible HanJuan EK Actor Specific Injected iframe
- [ ] ET EXPLOIT_KIT Archie EK Exploit Flash URI Struct
- [ ] ET EXPLOIT_KIT Archie EK Landing URI Struct
- [ ] ET EXPLOIT_KIT Archie EK Landing Nov 10 2014
- [ ] ET EXPLOIT_KIT Archie EK Landing Nov 17 2014 M2
- [ ] ET EXPLOIT_KIT Archie EK Flash Exploit URI Struct 2 Nov 17 2014
- [ ] ET EXPLOIT_KIT NullHole EK Exploit URI Struct
- [ ] ET EXPLOIT_KIT SPL2 EK PluginDetect Data Hash Nov 18 2014
- [ ] ET EXPLOIT_KIT SPL2 EK Flash Exploit Nov 18 2014
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK SWF
- [ ] ET EXPLOIT_KIT Archie EK T2 Landing Struct Nov 20 2014
- [ ] ET EXPLOIT_KIT Possible Internet Explorer CVE-2014-6332 Common Construct b64 3 (Observed in Archie EK)
- [x] ET EXPLOIT_KIT KaiXin Landing Page Nov 25 2014
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK Exploit Struct
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK SWF
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK Payload
- [ ] ET EXPLOIT_KIT Malicious Iframe Leading to EK Dec 08 2014
- [ ] ET EXPLOIT_KIT Malicious Redirect Leading to EK Dec 08 2014
- [ ] ET EXPLOIT_KIT Malicious JS Leading to Fiesta EK
- [x] ET EXPLOIT_KIT Evil Flash Redirector to RIG EK Dec 17 2014
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Dec 22 2014 Video
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Dec 22 2014 Search
- [ ] ET EXPLOIT_KIT Nuclear EK Landing Jan 06 2014
- [ ] ET EXPLOIT_KIT Nuclear EK Landing Jan 19 2014
- [ ] ET EXPLOIT_KIT Possible Sweet Orange redirection Jan 22 2015
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK SWF M2
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK SilverLight M2
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK Landing Jan 27 2015 M2
- [ ] ET EXPLOIT_KIT DRIVEBY Nuclear EK Landing Feb 03 2015 M2
- [ ] ET EXPLOIT_KIT KaiXin Secondary Landing Page
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Feb 11 2015 Banner
- [x] ET EXPLOIT_KIT Unknown EK Landing Feb 16 2015 b64 1 M1
- [x] ET EXPLOIT_KIT Unknown EK Landing Feb 16 2015 b64 3 M1
- [x] ET EXPLOIT_KIT Unknown EK Landing Feb 16 2015 b64 2 M2
- [ ] ET EXPLOIT_KIT Uknown EK Java Exploit
- [ ] ET EXPLOIT_KIT KaiXin EK Possible Jar Download
- [ ] ET EXPLOIT_KIT Unknown EK Comment in Body
- [x] ET EXPLOIT_KIT KaiXin Landing M3
- [x] ET EXPLOIT_KIT DRIVEBY Likely Evil EXE with no referer from HFS webserver (used by Unknown EK)
- [x] ET EXPLOIT_KIT DRIVEBY [PwC CTD] -- MultiGroup - ScanBox and Targetted Watering Holes PDF
- [x] ET EXPLOIT_KIT DRIVEBY [PwC CTD] -- MultiGroup - ScanBox and Targetted Watering Holes ActiveX Call
- [x] ET EXPLOIT_KIT DRIVEBY [PwC CTD] -- MultiGroup - ScanBox Watering Hole function return value
- [ ] ET EXPLOIT_KIT KaiXin Secondary Landing Page

- [ ] ET EXPLOIT_KIT Sweet Orange EK Flash Exploit IE March 03 2015
- [x] ET EXPLOIT_KIT WindowBase64.atob Function In Edwards Packed JavaScript - Possible iFrame Injection Detected
- [ ] ET EXPLOIT_KIT Fiesta EK Landing URI Struct March 6 2015
- [ ] ET EXPLOIT_KIT Unknown Malicious Second Stage Download URI Struct M1 Feb 06 2015
- [x] ET EXPLOIT_KIT Unknown Malicious Second Stage Download URI Struct M2 Feb 06 2015
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK March 16 2015
- [x] ET EXPLOIT_KIT MWI Maldoc Exploit Kit Stats Callout
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Mar 19 2015
- [ ] ET EXPLOIT_KIT Possible HanJuan Landing March 20 2015
- [x] ET EXPLOIT_KIT RIG Payload URI Struct March 20 2015
- [x] ET EXPLOIT_KIT RIG Exploit URI Struct March 20 2015
- [x] ET EXPLOIT_KIT RIG Landing URI Struct March 20 2015
- [x] ET EXPLOIT_KIT RIG EK Landing March 20 2015
- [ ] ET EXPLOIT_KIT RIG EK Landing March 20 2015 M2
- [ ] ET EXPLOIT_KIT HanJuan EK Landing March 24 2015 M1
- [ ] ET EXPLOIT_KIT HanJuan EK Landing March 24 2015 M2
- [ ] ET EXPLOIT_KIT VBScript Driveby MAR 31 2015
- [ ] ET EXPLOIT_KIT VBScript Driveby Related TDS MAR 31 2015
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Apr 2 2015
- [ ] ET EXPLOIT_KIT Malicious Redirect Leading to EK Apr 03 2015
- [ ] ET EXPLOIT_KIT Nuclear EK Landing Apr 03 2015
- [ ] ET EXPLOIT_KIT Nuclear EK Landing Apr 03 2015
- [ ] ET EXPLOIT_KIT DRIVEBY Router DNS Changer Apr 07 2015
- [ ] ET EXPLOIT_KIT Nuclear EK Landing Apr 08 2015
- [ ] ET EXPLOIT_KIT Magnitude Flash Exploit (IE) M2
- [x] ET EXPLOIT_KIT DRIVEBY Router DNS Changer Apr 07 2015 M2
- [ ] ET EXPLOIT_KIT SPL2 EK Post-Compromise Data Dump M1
- [ ] ET EXPLOIT_KIT SPL2 EK Post-Compromise Data Dump M2
- [ ] ET EXPLOIT_KIT SPL2 EK Post-Compromise Data Dump M3
- [ ] ET EXPLOIT_KIT Sundown EK Landing Apr 20 2015
- [ ] ET EXPLOIT_KIT Sundown EK Flash Exploit Apr 20 2015
- [ ] ET EXPLOIT_KIT Nuclear EK Landing Apr 22 2015
- [x] ET EXPLOIT_KIT Fiesta EK Landing Apr 23 2015
- [x] ET EXPLOIT_KIT Fiesta EK IE Exploit Apr 23 2015
- [x] ET EXPLOIT_KIT Fiesta EK Flash Exploit Apr 23 2015
- [x] ET EXPLOIT_KIT Fiesta EK SilverLight Exploit Apr 23 2015
- [ ] ET EXPLOIT_KIT Fiesta EK Java Exploit Apr 23 2015
- [ ] ET EXPLOIT_KIT Fiesta EK PDF Exploit Apr 23 2015
- [x] ET EXPLOIT_KIT Sundown EK Secondary Landing Apr 20 2015
- [x] ET EXPLOIT_KIT Download file with Powershell via LNK file (observed in Sundown EK)
- [ ] ET EXPLOIT_KIT Possible Sundown EK URI Struct T1 Apr 24 2015
- [ ] ET EXPLOIT_KIT Possible Sundown EK Payload Struct T1 Apr 24 2015
- [ ] ET EXPLOIT_KIT Sundown EK Secondary Landing T1 M2 Apr 24 2015
- [x] ET EXPLOIT_KIT Possible Sundown EK Payload Struct T2 M1 Apr 24 2015
- [ ] ET EXPLOIT_KIT Possible Sundown EK Payload Struct T2 M2 Apr 24 2015
- [ ] ET EXPLOIT_KIT Possible Sundown EK Flash Exploit Struct T2 Apr 24 2015
- [ ] ET EXPLOIT_KIT CottonCastle/Niteris EK Landing URI Struct April 29 2015 M1
- [ ] ET EXPLOIT_KIT CottonCastle/Niteris EK Landing URI Struct April 29 2015 M2
- [ ] ET EXPLOIT_KIT CottonCastle/Niteris EK Java Exploit URI Struct April 29 2015
- [ ] ET EXPLOIT_KIT CottonCastle/Niteris EK URI Struct April 29 2015
- [ ] ET EXPLOIT_KIT CottonCastle/Niteris EK Payload April 29 2015
- [ ] ET EXPLOIT_KIT CottonCastle/Niteris EK POST Beacon April 29 2015
- [ ] ET EXPLOIT_KIT CottonCastle/Niteris EK Landing April 29 2015
- [ ] ET EXPLOIT_KIT CottonCastle/Niteris EK Exploit Struct April 30 2015
- [ ] ET EXPLOIT_KIT CottonCastle/Niteris EK SWF Exploit April 30 2015
- [ ] ET EXPLOIT_KIT CottonCastle/Niteris EK SWF Exploit April 30 2015
- [ ] ET EXPLOIT_KIT CottonCastle/Niteris EK SilverLight Exploit April 30 2015
- [ ] ET EXPLOIT_KIT Unknown EK Landing Page May 01 2015
- [x] ET EXPLOIT_KIT Unknown EK Secondary Landing Page May 01 2015 M1
- [x] ET EXPLOIT_KIT Unknown EK Secondary Landing Page May 01 2015 M2
- [ ] ET EXPLOIT_KIT Magnitude EK Flash Payload ShellCode Apr 23 2015
- [ ] ET EXPLOIT_KIT CottonCastle/Niteris EK Receiving Payload May 7 2015
- [ ] ET EXPLOIT_KIT DNSChanger EK Landing May 12 2015
- [x] ET EXPLOIT_KIT DNSChanger EK Secondary Landing May 12 2015 M2
- [ ] ET EXPLOIT_KIT Sundown EK Landing May 21 2015 M1
- [ ] ET EXPLOIT_KIT Sundown EK Landing May 21 2015 M2
- [ ] ET EXPLOIT_KIT DNSChanger EK Landing URI Struct May 22 2015
- [x] ET EXPLOIT_KIT suspicious VBE-encoded script (seen in Sundown EK)
- [ ] ET EXPLOIT_KIT Likely Evil JS used in Unknown EK Landing
- [x] ET EXPLOIT_KIT Likely Evil JS used in Unknown EK Landing
- [ ] ET EXPLOIT_KIT KaiXin Secondary Landing Jun 09 2015
- [ ] ET EXPLOIT_KIT Possible Evil Redirector Leading to EK June 11 2015
- [x] ET EXPLOIT_KIT KaiXin Landing M4
- [x] ET EXPLOIT_KIT KaiXin Secondary Landing Page
- [x] ET EXPLOIT_KIT KaiXin Secondary Landing Page
- [ ] ET EXPLOIT_KIT CottonCastle/Niteris EK Landing URI Struct June 19 2015 M3
- [ ] ET EXPLOIT_KIT Likely CottonCastle/Niteris EK Response June 19 2015
- [ ] ET EXPLOIT_KIT CottonCastle/Niteris EK Exploit URI Struct June 19 2015
- [ ] ET EXPLOIT_KIT CottonCastle/Niteris EK Payload June 19 2015
- [ ] ET EXPLOIT_KIT CottonCastle/Niteris EK Flash Exploit URI Struct June 19 2015
- [ ] ET EXPLOIT_KIT CottonCastle/Niteris EK Landing June 19 2015
- [x] ET EXPLOIT_KIT Suspicious JS Observed in Unknown EK Landing
- [ ] ET EXPLOIT_KIT KaiXin Secondary Landing Page June 22 2015
- [x] ET EXPLOIT_KIT Possible Evil Redirector Leading to EK June 10 2015
- [ ] ET EXPLOIT_KIT Magnitude CVE-2015-3113 Jun 29 2015 M1
- [ ] ET EXPLOIT_KIT NullHole EK Landing URI struct
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Jul 02
- [x] ET EXPLOIT_KIT Evil Redirector Leading to EK Jul 08
- [x] ET EXPLOIT_KIT HanJuan EK Current Campaign Landing URI Struct Jul 10 2015
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Jul 17
- [ ] ET EXPLOIT_KIT NullHole URI Struct Jul 22 2015 M2
- [x] ET EXPLOIT_KIT ScanBox Jun 06 2015 M1 T1
- [x] ET EXPLOIT_KIT ScanBox Jun 06 2015 M2 T1
- [x] ET EXPLOIT_KIT ScanBox Jun 06 2015 M3 T1
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Jul 29
- [ ] ET EXPLOIT_KIT Nuclear EK Exploit URI Struct Aug 12
- [ ] ET EXPLOIT_KIT CottonCastle/Niteris EK Secondary Landing Aug 17 2015
- [ ] ET EXPLOIT_KIT CottonCastle/Niteris EK Landing Aug 17 2015
- [ ] ET EXPLOIT_KIT CottonCastle/Niteris EK Secondary Landing URI Struct Aug 17 2015
- [ ] ET EXPLOIT_KIT CottonCastle/Niteris EK Exploit URI Struct Aug 17 2015

- [ ] ET EXPLOIT_KIT Possible TDS Redirecting to EK Aug 19 2015
- [ ] ET EXPLOIT_KIT Possible Magnitude EK Landing URI Struct Aug 21 2015
- [ ] ET EXPLOIT_KIT Magnitude EK Landing Aug 21 2015
- [x] ET EXPLOIT_KIT Magnitude/Hunter EK IE Exploit Aug 23 2015
- [ ] ET EXPLOIT_KIT Nuclear EK IE Exploit Aug 23 2015
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Aug 31 2015 T2 (BizCN)
- [x] ET EXPLOIT_KIT Evil Redirector Leading to EK September 04 2015
- [ ] ET EXPLOIT_KIT Spartan EK Secondary Flash Exploit DL
- [x] ET EXPLOIT_KIT SUSPICIOUS Grey Advertising Often Leading to EK
- [ ] ET EXPLOIT_KIT Possible Spartan EK Secondary Flash Exploit DL M2
- [x] ET EXPLOIT_KIT Possible Spartan/Nuclear EK Payload
- [x] ET EXPLOIT_KIT Unknown Malicious Second Stage Download URI Struct Sept 15 2015
- [ ] ET EXPLOIT_KIT Unknown Malicious Second Stage Download URI Struct Sept 15 2015
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Sept 25 2015
- [x] ET EXPLOIT_KIT Evil Redirector Leading To EK Sep 30 2015
- [x] ET EXPLOIT_KIT KaiXin Landing M5 1 Oct 05 2015
- [ ] ET EXPLOIT_KIT KaiXin Landing M5 2 Oct 05 2015
- [ ] ET EXPLOIT_KIT KaiXin Landing M5 3 Oct 05 2015
- [x] ET EXPLOIT_KIT KaiXin Landing Page Oct 05 2015
- [ ] ET EXPLOIT_KIT Magnitude EK Landing Oct 08 2015
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Oct 26 2015
- [x] ET EXPLOIT_KIT Possible Malicious Redirect Leading to EK Oct 29
- [ ] ET EXPLOIT_KIT Evil Redirector Leadking to EK Nov 2015
- [x] ET EXPLOIT_KIT Possible Evil Redirector Leading to EK Nov 09 2015 M1
- [x] ET EXPLOIT_KIT Possible Evil Redirector Leading to EK Nov 09 2015 M2
- [ ] ET EXPLOIT_KIT Possible Nuclear EK Nov 13 2015 Landing URI struct
- [ ] ET EXPLOIT_KIT Possible Nuclear EK Landing Nov 17 2015
- [x] ET EXPLOIT_KIT Possible Spartan/Nuclear EK Payload
- [ ] ET EXPLOIT_KIT Possible Nuclear EK Landing Nov 27 2015
- [x] ET EXPLOIT_KIT Evil Redirector Leading to EK Dec 09
- [x] ET EXPLOIT_KIT Evil Redirector Leading to EK Mon Dec 21 2015 5
- [ ] ET EXPLOIT_KIT Evil Redirect Leading to EK Dec 22 2015 (Proxy Filtering)
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Mon Dec 26 2015
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Mon Dec 26 2015 2
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Jan 6th 2016 M1
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Jan 6th 2016 M2
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Jan 27 2016 (Evil Keitaro FB Set)
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK (Known Evil Keitaro TDS)
- [x] ET EXPLOIT_KIT Possible Keitaro TDS Redirect
- [x] ET EXPLOIT_KIT EITest Evil Redirect Leading to EK Feb 01 2016
- [x] ET EXPLOIT_KIT RIG encrypted payload M1 Feb 02 2016
- [x] ET EXPLOIT_KIT Evil Redirector Leading to EK Feb 05 2016
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Feb 07 2016
- [ ] ET EXPLOIT_KIT Evil Redirect Leading to EK Feb 23 2016
- [ ] ET EXPLOIT_KIT Evil Redirect Leading to EK Feb 25 2016
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Mar 15 2016 M1
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Mar 15 2016 M2
- [x] ET EXPLOIT_KIT Evil Redirect Leading to EK Mar 18 2016
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Mar 19 2016 M1
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Mar 19 2016 M2
- [ ] ET EXPLOIT_KIT Evil Redirector Leading To EK Mar 22 2016
- [ ] ET EXPLOIT_KIT Possible Evil Redirector Leading to EK EITest Mar 27
- [ ] ET EXPLOIT_KIT Possible Evil Redirector Leading to EK EITest Mar 27 M2
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK April 12 2016 M1
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK April 12 2016 M2
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Apr 20 2016
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Apr 21 2016 M2
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Apr 27 2016 (fbset)
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Apr 27 2016
- [x] ET EXPLOIT_KIT Evil Redirector Leading to EK Apr 28 2016
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Apr 29 2016
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK (delivered via e-mail)
- [ ] ET EXPLOIT_KIT Evil Redirect Leading to EK May 13 2016
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Jun 03 2016
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Jun 06 2016
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Jun 14 2016
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Jun 15 2016
- [ ] ET EXPLOIT_KIT Evil Redirect Leading to EK Jun 22 2016 M1
- [ ] ET EXPLOIT_KIT Evil Redirect Leading to EK Jun 22 2016 M2
- [x] ET EXPLOIT_KIT RIG EK Payload Jun 26 2016
- [x] ET EXPLOIT_KIT RIG EK Payload Jul 05 2016
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Jul 10 M2
- [ ] ET EXPLOIT_KIT Evil Redirector Leading To EK Jul 10 M1
- [x] ET EXPLOIT_KIT Evil Redirector Leading to EK Jul 12 2016
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Jul 13 2016 2
- [ ] ET EXPLOIT_KIT Evil Redirect Leading to EK Mar 30 M3
- [x] ET EXPLOIT_KIT Evil Redirect Leading to EK Jul 28 2016
- [ ] ET EXPLOIT_KIT Evil Redirector Leading To EK Jul 30 M1
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Aug1 2016
- [ ] ET EXPLOIT_KIT EITest Flash Redirect Aug 09 2016
- [ ] ET EXPLOIT_KIT Evil Redirect Leading to EK Aug 17 2016
- [ ] ET EXPLOIT_KIT Possible Evil Redirector Leading to EK EITest Sep 02 M2
- [ ] ET EXPLOIT_KIT Encoded CVE-2014-6332 (As Observed in SunDown EK) M1
- [ ] ET EXPLOIT_KIT Encoded CVE-2014-6332 (As Observed in SunDown EK) M2
- [ ] ET EXPLOIT_KIT Encoded CVE-2014-6332 (As Observed in SunDown EK) M3
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Sep 12 2016 (Flash)
- [ ] ET EXPLOIT_KIT EITest Inject (compromised site) Sep 12 2016
- [ ] ET EXPLOIT_KIT EITest Inject (compromised site) M2 Sep 12 2016
- [x] ET EXPLOIT_KIT CVE-2016-0189 Exploit as Observed in Sundown/RIG EK (b641)
- [x] ET EXPLOIT_KIT CVE-2016-0189 Exploit as Observed in Sundown/RIG EK (b642)
- [x] ET EXPLOIT_KIT CVE-2016-0189 Exploit as Observed in Sundown/RIG EK (b643)
- [x] ET EXPLOIT_KIT CVE-2016-0189 Exploit as Observed in Sundown/RIG EK (b644)
- [x] ET EXPLOIT_KIT CVE-2016-0189 Exploit as Observed in Sundown/RIG EK (b645)
- [x] ET EXPLOIT_KIT CVE-2016-0189 Exploit as Observed in Sundown/RIG EK (b646)
- [x] ET EXPLOIT_KIT RIG EK Landing Sep 12 2016 T2
- [x] ET EXPLOIT_KIT RIG EK Landing Sep 13 2016 (b641)
- [x] ET EXPLOIT_KIT RIG EK Landing Sep 13 2016 (b642)
- [x] ET EXPLOIT_KIT RIG EK Landing Sep 13 2016 (b643)
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Sep 19 2016
- [ ] ET EXPLOIT_KIT Possible EITest Flash Redirect Sep 19 2016
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Sep 19 2016 (EItest Inject)
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Sep 19 2016 (EItest Inject) M2
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Sep 20 2016
- [ ] ET EXPLOIT_KIT SunDown EK Flash Exploit Sep 22 2016

- [ ] ET EXPLOIT_KIT SunDown EK NOP Sled Sep 22 2016 (b641)
- [x] ET EXPLOIT_KIT SunDown EK NOP Sled Sep 22 2016 (b643)
- [x] ET EXPLOIT_KIT SunDown EK Slight Sep 22 2016 (b642)
- [ ] ET EXPLOIT_KIT SunDown EK CVE-2015-0016 Sep 22 2016 (b641)
- [x] ET EXPLOIT_KIT SunDown EK CVE-2015-0016 Sep 22 2016 (b643)
- [ ] ET EXPLOIT_KIT SunDown EK CVE-2016-0189 Sep 22 2016 (b642)
- [ ] ET EXPLOIT_KIT SunDown EK CVE-2013-2551 Sep 22 2016 (b641)
- [ ] ET EXPLOIT_KIT SunDown EK CVE-2013-2551 Sep 22 2016 (b643)
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Sep 26 2016 T2
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK (EITest Inject) Oct 03 2016
- [ ] ET EXPLOIT_KIT SunDown EK Landing Oct 03 2016
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Oct 19 2016
- [x] ET EXPLOIT_KIT RIG EK URI struct Oct 24 2016 (RIG-v)
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Nov 01 2016
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK EITest Inject Oct 17 2016 M2
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK EITest Inject Oct 17 2016 M3
- [x] ET EXPLOIT_KIT Internet Explorer Information Disclosure Vuln as Observed in RIG EK Prefilter M2 Dec 06
- [x] ET EXPLOIT_KIT EITest SocEng Inject Jan 15 2017 M1
- [ ] ET EXPLOIT_KIT EITest SocEng Inject Jan 15 2017 EXE Download
- [x] ET EXPLOIT_KIT Possible Broken/Filtered RIG EK Payload Download
- [x] ET EXPLOIT_KIT Terror EK Landing M1 Feb 07 2016 M1
- [x] ET EXPLOIT_KIT RIG EK URI Struct Feb 26 2017
- [ ] ET EXPLOIT_KIT Evil Redirect Leading to EK March 07 2017
- [x] ET EXPLOIT_KIT RIG EK URI Struct Mar 13 2017
- [x] ET EXPLOIT_KIT Terror EK Payload Download M1 Mar 14 2017
- [x] ET EXPLOIT_KIT Terror EK Payload RC4 Key M1 Mar 14 2017
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK March 15 2017 M2
- [ ] ET EXPLOIT_KIT Suspicious Decimal IP Redirect - Observed in RIG EK Redirects M2
- [ ] ET EXPLOIT_KIT Suspicious Decimal IP Redirect - Observed in RIG EK Redirects M4
- [ ] ET EXPLOIT_KIT Suspicious Decimal IP Redirect - Observed in RIG EK Redirects M6
- [ ] ET EXPLOIT_KIT Suspicious Decimal IP Redirect - Observed in RIG EK Redirects M8
- [ ] ET EXPLOIT_KIT Suspicious Decimal IP Redirect - Observed in RIG EK Redirects M10
- [x] ET EXPLOIT_KIT Terror EK CVE-2016-0189 Exploit M2
- [x] ET EXPLOIT_KIT Terror EK Payload Download
- [x] ET EXPLOIT_KIT EITest SocENG Inject M2
- [x] ET EXPLOIT_KIT EITest Exploit Kit Redirection Script
- [ ] ET EXPLOIT_KIT Terror EK Landing URI T1 Jun 02 2017
- [x] ET EXPLOIT_KIT Terror EK Payload URI T1 Jun 02 2017 M2
- [x] ET EXPLOIT_KIT Terror EK Landing T1 Jun 02 2017 M2
- [x] ET EXPLOIT_KIT SUSPICIOUS Request for Grey Advertising Often Leading to EK
- [x] ET EXPLOIT_KIT SunDown EK RIP Landing M1 B642
- [ ] ET EXPLOIT_KIT SunDown EK RIP Landing M2 B641
- [ ] ET EXPLOIT_KIT SunDown EK RIP Landing M2 B643
- [x] ET EXPLOIT_KIT SunDown EK RIP Landing M3 B642
- [x] ET EXPLOIT_KIT SunDown EK RIP Landing M4 B641
- [x] ET EXPLOIT_KIT Bingo EK Payload Download
- [x] ET EXPLOIT_KIT RIG EK Broken/Filtered Payload Download Jun 19 2017
- [ ] ET EXPLOIT_KIT EITest Keitaro Evil Redirect Leading to SocENG July 25 2017
- [x] ET EXPLOIT_KIT Magnitude EK Landing M1 Aug 05 2017
- [ ] ET EXPLOIT_KIT Hancitor/Tordal Document Inbound
- [ ] ET EXPLOIT_KIT SunDown EK NOP Sled Sep 22 2016 (b642)
- [ ] ET EXPLOIT_KIT SunDown EK Slight Sep 22 2016 (b641)
- [x] ET EXPLOIT_KIT SunDown EK Slight Sep 22 2016 (b643)
- [ ] ET EXPLOIT_KIT SunDown EK CVE-2015-0016 Sep 22 2016 (b642)
- [ ] ET EXPLOIT_KIT SunDown EK CVE-2016-0189 Sep 22 2016 (b641)
- [x] ET EXPLOIT_KIT SunDown EK CVE-2016-0189 Sep 22 2016 (b643)
- [ ] ET EXPLOIT_KIT SunDown EK CVE-2013-2551 Sep 22 2016 (b642)
- [ ] ET EXPLOIT_KIT Evil Redirect Leading to EK Sep 26 2016
- [ ] ET EXPLOIT_KIT EITest Inject (compromised site) Sep 12 2016
- [x] ET EXPLOIT_KIT Flash Exploit Likely SunDown EK
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK EITest Inject Oct 17 2016
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Oct 19 2016 T2
- [ ] ET EXPLOIT_KIT DNSChanger EK Secondary Landing Oct 31 2016
- [ ] ET EXPLOIT_KIT Sundown/Xer EK Landing Jul 06 2016 M1
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Nov 15 2016
- [x] ET EXPLOIT_KIT Internet Explorer Information Disclosure Vuln as Observed in RIG EK Prefilter M1 Dec 06
- [ ] ET EXPLOIT_KIT EITest SocEng Inject Jan 15 2017 M2
- [x] ET EXPLOIT_KIT EITest SocEng Inject Jan 15 2017 M2
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK EITest Inject Oct 17 2016 M4
- [x] ET EXPLOIT_KIT EITest SocEng Inject Jan 15 2017 EXE Download
- [x] ET EXPLOIT_KIT Terror EK Landing M1 Feb 07 2016 M2
- [x] ET EXPLOIT_KIT RIG EK Landing Feb 26 2016
- [ ] ET EXPLOIT_KIT EITest SocEng Fake Font DL March 09 2017
- [x] ET EXPLOIT_KIT RIG EK URI Struct Mar 13 2017 M2
- [x] ET EXPLOIT_KIT Terror EK Payload Download M2 Mar 14 2017
- [x] ET EXPLOIT_KIT Evil Redirector Leading to EK March 15 2017
- [ ] ET EXPLOIT_KIT Suspicious Decimal IP Redirect - Observed in RIG EK Redirects M1
- [ ] ET EXPLOIT_KIT Suspicious Decimal IP Redirect - Observed in RIG EK Redirects M3
- [ ] ET EXPLOIT_KIT Suspicious Decimal IP Redirect - Observed in RIG EK Redirects M5
- [ ] ET EXPLOIT_KIT Suspicious Decimal IP Redirect - Observed in RIG EK Redirects M7
- [ ] ET EXPLOIT_KIT Suspicious Decimal IP Redirect - Observed in RIG EK Redirects M9
- [x] ET EXPLOIT_KIT Terror EK CVE-2016-0189 Exploit
- [x] ET EXPLOIT_KIT Terror EK CVE-2015-2419 Exploit
- [ ] ET EXPLOIT_KIT EITest SocENG Payload DL
- [ ] ET EXPLOIT_KIT EITest SocENG Inject M3
- [ ] ET EXPLOIT_KIT HoeflerText Chrome Popup DriveBy Download Attempt 1
- [x] ET EXPLOIT_KIT Terror EK Payload URI T1 Jun 02 2017
- [x] ET EXPLOIT_KIT Terror EK Landing T1 Jun 02 2017 M1
- [x] ET EXPLOIT_KIT SUSPICIOUS DNS Request for Grey Advertising Often Leading to EK
- [x] ET EXPLOIT_KIT SunDown EK RIP Landing M1 B641
- [x] ET EXPLOIT_KIT SunDown EK RIP Landing M1 B643
- [ ] ET EXPLOIT_KIT SunDown EK RIP Landing M2 B642
- [x] ET EXPLOIT_KIT SunDown EK RIP Landing M3 B641
- [x] ET EXPLOIT_KIT SunDown EK RIP Landing M3 B643
- [x] ET EXPLOIT_KIT SunDown EK RIP Landing M4 B642
- [x] ET EXPLOIT_KIT RIG EK URI Struct Jun 13 2017
- [x] ET EXPLOIT_KIT EITest Inject July 25 2017
- [x] ET EXPLOIT_KIT RIG encrypted payload M1 Aug 01 2017
- [x] ET EXPLOIT_KIT Magnitude EK Landing M2 Aug 05 2017
- [ ] ET EXPLOIT_KIT Disdain EK URI Struct Aug 23 2017 M1

- [ ] ET EXPLOIT_KIT Disdain EK URI Struct Aug 23 2017 M2
- [x] ET EXPLOIT_KIT Disdain EK Payload Aug 23 2017
- [x] ET EXPLOIT_KIT Disdain EK Flash Exploit M1 Aug 23 2017
- [x] ET EXPLOIT_KIT Disdain EK Flash Exploit M2 Aug 23 2017
- [x] ET EXPLOIT_KIT Disdain EK Flash Exploit M3 Aug 23 2017
- [ ] ET EXPLOIT_KIT Disdain EK Landing Aug 23 2017
- [x] ET EXPLOIT_KIT RIG EK Rip Sep 05 2017
- [x] ET EXPLOIT_KIT RIG EK Rip Sep 05 2017 M2
- [x] ET EXPLOIT_KIT RIG EK encrypted payload Sept 11 (1)
- [x] ET EXPLOIT_KIT HoeflerText Chrome Popup DriveBy Download Attempt 2
- [x] ET EXPLOIT_KIT Dadong Exploit Kit Downloaded
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Feb 24 2016 (Evil Keitaro FB Set)
- [ ] ET EXPLOIT_KIT Evil Redirector Leading to EK Feb 29 2016 (Evil Keitaro FB Set)
- [x] ET EXPLOIT_KIT Bingo Exploit Kit Landing May 08 2017
- [x] ET EXPLOIT_KIT GrandSoft EK IE Exploit Jan 30 2018
- [x] ET EXPLOIT_KIT [PTsecurity] Grandsoft EK Payload
- [x] ET EXPLOIT_KIT Underminer EK IE Exploit
- [x] ET EXPLOIT_KIT Possible Malvertising Redirect to EK M1
- [x] ET EXPLOIT_KIT Possible Malvertising EK Redirect to EK M2
- [ ] ET EXPLOIT_KIT Underminer EK Flash Exploit
- [x] ET EXPLOIT_KIT Possible Underminer EK Landing
- [x] ET EXPLOIT_KIT Underminer EK Key POST
- [x] ET EXPLOIT_KIT Underminer EK Resource File Download M1
- [x] ET EXPLOIT_KIT Underminer EK Resource File Download M2
- [x] ET EXPLOIT_KIT Underminer EK Plugin Check
- [x] ET EXPLOIT_KIT Underminer EK Flash/WAV Loader
- [x] ET EXPLOIT_KIT Underminer EK SWF Request
- [x] ET EXPLOIT_KIT Spelevo EK Landing M1
- [x] ET EXPLOIT_KIT Spelevo EK Landing M2
- [x] ET EXPLOIT_KIT Spelevo EK Landing M3
- [x] ET EXPLOIT_KIT Spelevo EK Post-Compromise Data Dump
- [x] ET EXPLOIT_KIT Spelevo EK Flash Exploit Attempt
- [x] ET EXPLOIT_KIT Possible Router EK Landing Page Inbound 2019-05-24
- [x] ET EXPLOIT_KIT Obfuscated LordEK Landing M1
- [x] ET EXPLOIT_KIT Observed LordEK HTTP POST Request
- [x] ET EXPLOIT_KIT Obfuscated LordEK Landing M2
- [x] ET EXPLOIT_KIT RIG EK - Unexpected Victim Location Server Response
- [x] ET EXPLOIT_KIT Redirect on ActiveXObject support
- [x] ET EXPLOIT_KIT Spelevo VBS Payload Downloaded
- [x] ET EXPLOIT_KIT Spelevo Download Payload Landing
- [x] ET EXPLOIT_KIT Capesand EK Landing
- [x] ET EXPLOIT_KIT PluginDetect Observed - Possible EK Activity
- [x] ET EXPLOIT_KIT Capesand EK Visitor Tracking
- [x] ET EXPLOIT_KIT Possible MSFVenom Exploit via Browser
- [x] ET EXPLOIT_KIT Powershell Download Command Observed within Flash File - Probable EK Activity
- [ ] ET EXPLOIT_KIT Possible PurpleFox/RIG EK Flash Request M1
- [x] ET EXPLOIT_KIT Possible PurpleFox/RIG EK Flash Request M2
- [x] ET EXPLOIT_KIT Possible PurpleFox EK Framework Landing
- [x] ET EXPLOIT_KIT Possible PurpleFox EK Framework Landing - Various Exploits
- [x] ET EXPLOIT_KIT Possible PurpleFox EK Framework Payload
- [x] ET EXPLOIT_KIT Possible PurpleFox EK Framework Flash HEAD Request
- [x] ET EXPLOIT_KIT Possible PurpleFox EK Framework Flash GET Request
- [x] ET EXPLOIT_KIT Possible PurpleFox EK Framework URI Struct Landing Request
- [x] ET EXPLOIT_KIT Possible PurpleFox EK Framework URI Struct Flash Request
- [x] ET EXPLOIT_KIT Possible PurpleFox EK Framework Payload
- [x] ET EXPLOIT_KIT Possible PurpleFox EK Framework Payload
- [x] ET EXPLOIT_KIT BottleEK Landing
- [x] ET EXPLOIT_KIT BottleEK Plugin Check JS
- [x] ET EXPLOIT_KIT BottleEK Plugin Check Response
- [x] ET EXPLOIT_KIT Suspicious VBS Encoding Observed in BottleEK
- [x] ET EXPLOIT_KIT BottleEK Payload Request
- [x] ET EXPLOIT_KIT Magnitude EK JSE
- [x] ET EXPLOIT_KIT PurpleFox EK Domain in DNS Lookup
- [x] ET EXPLOIT_KIT Possible PurpleFox EK Framework URI Struct Payload Request M1
- [x] ET EXPLOIT_KIT Possible PurpleFox EK Redirect
- [x] ET EXPLOIT_KIT Possible PurpleFox EK Framework URI Struct Jpg Request
- [x] ET EXPLOIT_KIT Observed Evil Keitaro TDS Redirection Domain (fiberswatch .com in TLS SNI)
- [x] ET EXPLOIT_KIT Possible PurpleFox EK Redirect M2
- [x] ET EXPLOIT_KIT Suspicious GitHack TLS SNI Request - Possible PurpleFox EK
- [x] ET EXPLOIT_KIT Suspicious GitHack DNS Request - Possible PurpleFox EK
- [ ] ET EXPLOIT_KIT Observed BottleEK Domain in DNS Lookup 2021-04-15
- [x] ET EXPLOIT_KIT Parrot TDS Check
- [x] ET EXPLOIT_KIT Parrot TDS Cleared Response
- [x] ET EXPLOIT_KIT Parrot TDS Malicious Response
- [x] ET EXPLOIT_KIT NDSW/NDSX Javascript Inject
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (jqueryns .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (jqscr .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (jsqur .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (jqueryh .org)
- [ ] ET EXPLOIT_KIT TA569 TDS Domain in DNS Lookup (xjquery .com)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (devqeury .org)
- [x] ET EXPLOIT_KIT TDS Landing Page - Observed Leading to CryptoClipper
- [x] ET EXPLOIT_KIT TDS checkResult Request - Observed Leading to CryptoClipper
- [x] ET EXPLOIT_KIT Balada Injector Script
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (devcodejs .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (backendjs .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (assistpayout .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (jsviewdev .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (jquery0 .com)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (jquery01 .com)

- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (jquery-bin .com)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (getquery .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (etaqeryg .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (debquery .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (rygesqua .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (aeryqget .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (quaryget .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (squaryge .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (tqeuryge .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (ygequary .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (uaqryges .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (greenpapers .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (waterlinesheet .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (lemonicecold .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (neworderspath .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (deeptrickday .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (dailytickyclock .org)
- [x] ET EXPLOIT_KIT Observed Balada TDS Domain (scriptsplatform .com in TLS SNI)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (cancelledfirestarter .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (greedyfines .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (libertader .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (linedgreen .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (windowlight .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (biggreenlimes .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (linedloop .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (slurpslimes .org)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in DNS Lookup (updateadobeflash .website)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in DNS Lookup (googletagmanagar .com)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in DNS Lookup (google-analytiks .com)
- [x] ET EXPLOIT_KIT Keitaro Set-Cookie Inbound to RogueRaticate (4cdcb)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in TLS SNI (google-analytiks .com)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in TLS SNI (googletagmanagar .com)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in TLS SNI (updateadobeflash .website)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (drilledgas .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (drilledgas .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (sevenpunches .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (sevenpunches .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (surelytheme .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS in TLS SNI (surelytheme .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (chestedband .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (limonpart .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (chestedband .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (limonpart .org)
- [x] ET EXPLOIT_KIT Parrot TDS Check M2
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (bluegaslamp .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (bluegaslamp .org)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in DNS Lookup (gstatick .com)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in TLS SNI (gstatick .com)
- [ ] ET EXPLOIT_KIT Fake Browser Update in DNS Lookup
- [ ] ET EXPLOIT_KIT Fake Browser Update in TLS SNI
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in DNS Lookup (analytics-google-x91 .com)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in TLS SNI (analytics-google-x91 .com)
- [ ] ET EXPLOIT_KIT Fake Browser Update Domain in DNS Lookup (cheetahsnv .com)
- [ ] ET EXPLOIT_KIT Fake Browser Update Domain in TLS SNI (cheetahsnv .com)
- [ ] ET EXPLOIT_KIT Fake Browser Update Domain in DNS Lookup (offshorechain .org)
- [ ] ET EXPLOIT_KIT Fake Browser Update Domain in DNS Lookup (polyfieldgallery .com)
- [ ] ET EXPLOIT_KIT Fake Browser Update Domain in TLS SNI (polyfieldgallery .com)
- [ ] ET EXPLOIT_KIT Fake Browser Update Domain in DNS Lookup (seosuccesslab .com)
- [ ] ET EXPLOIT_KIT Fake Browser Update Domain in TLS SNI (seosuccesslab .com)
- [ ] ET EXPLOIT_KIT ClearFake Domain in DNS Lookup (adqdqqewqewplzoqmzq .site)
- [ ] ET EXPLOIT_KIT ClearFake Domain in DNS Lookup (borbrbmrtxtrbxrq .site)
- [ ] ET EXPLOIT_KIT ClearFake Domain in DNS Lookup (komomjinndqndqwf .store)
- [ ] ET EXPLOIT_KIT ClearFake Domain in DNS Lookup (omdowqind .site)
- [ ] ET EXPLOIT_KIT ClearFake Domain in DNS Lookup (wffewiuofegwumzowefmgwezfzew .site)
- [ ] ET EXPLOIT_KIT ClearFake Domain in DNS Lookup (wnimodmoiejn .site)
- [ ] ET EXPLOIT_KIT ClearFake Domain in TLS SNI (adqdqqewqewplzoqmzq .site)
- [ ] ET EXPLOIT_KIT ClearFake Domain in TLS SNI (borbrbmrtxtrbxrq .site)
- [ ] ET EXPLOIT_KIT ClearFake Domain in TLS SNI (komomjinndqndqwf .store)
- [ ] ET EXPLOIT_KIT ClearFake Domain in TLS SNI (omdowqind .site)
- [ ] ET EXPLOIT_KIT ClearFake Domain in TLS SNI (wffewiuofegwumzowefmgwezfzew .site)

- [ ] ET EXPLOIT_KIT ClearFake Domain in TLS SNI (wnimodmoiejn .site)
- [ ] ET EXPLOIT_KIT Fake Browser Update Domain in DNS Lookup (martinreamask .com)
- [ ] ET EXPLOIT_KIT Fake Browser Update Domain in TLS SNI (martinreamask .com)
- [ ] ET EXPLOIT_KIT ClearFake Fingerprinting Domain in DNS Lookup (stats-best .site)
- [ ] ET EXPLOIT_KIT Fake Browser Update Domain in DNS Lookup (phimnhanh .info)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (throatpills .org)
- [ ] ET EXPLOIT_KIT ClearFake Domain in DNS Lookup (ewkekezmwzfevwvwvvmmmmmmwfwf .site)
- [ ] ET EXPLOIT_KIT ClearFake Domain in TLS SNI (ewkekezmwzfevwvwvvmmmmmmwfwf .site)
- [ ] ET EXPLOIT_KIT ClearFake Domain in DNS Lookup (pwwqkppwqkezqer .site)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in DNS Lookup (googlestates .com)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (darkmansion .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (draggedline .org)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (marcborowy .com)
- [ ] ET EXPLOIT_KIT ClearFake Domain in DNS Lookup (oekofkkfkoeefkefbnhgtrq .space)
- [ ] ET EXPLOIT_KIT ClearFake Domain in DNS Lookup (znqjdnqzdqzfqmfqmkfq .site)
- [ ] ET EXPLOIT_KIT ClearFake Domain in TLS SNI (oekofkkfkoeefkefbnhgtrq .space)
- [ ] ET EXPLOIT_KIT ClearFake Domain in TLS SNI (znqjdnqzdqzfqmfqmkfq .site)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in DNS Lookup (gctatick .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (xxxmir .info)
- [ ] ET EXPLOIT_KIT ClearFake Domain in DNS Lookup (oiuytyfvq621mb .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (whitedrill .org)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (cristinaamaro .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (machinetext .org)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (krafttopia .net)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (greedyclowns .org)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (mansaentertainment .com)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in DNS Lookup (import19ksnx9ajsn .com)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (redsnowynose .org)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in DNS Lookup (statistiks-google .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (cpmmasters .com)
- [x] ET EXPLOIT_KIT Keitaro Set-Cookie Inbound to RogueRaticate (3a7ee)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (aflomusic .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (aflomusic .com)
- [ ] ET EXPLOIT_KIT ScamClub Domain in DNS Lookup (Wstatkblsenmb1234 .top)
- [ ] ET EXPLOIT_KIT ScamClub Domain in DNS Lookup (tetstwitn12 .xyz)
- [ ] ET EXPLOIT_KIT ScamClub Domain in DNS Lookup (Bhgusz .space)
- [ ] ET EXPLOIT_KIT ScamClub Domain in DNS Lookup (Luckypapa .top)
- [ ] ET EXPLOIT_KIT ScamClub Domain in DNS Lookup (Luckypuppy .top)
- [ ] ET EXPLOIT_KIT ScamClub Domain in DNS Lookup (bbd383ttka21 .top)
- [ ] ET EXPLOIT_KIT ScamClub Domain in DNS Lookup (2022325luckyday .top)
- [x] ET EXPLOIT_KIT Keitaro Set-Cookie Inbound to ClearFake (71eb8)
- [ ] ET EXPLOIT_KIT Fake Browser Update Domain in DNS Lookup (seyishalom .com)
- [ ] ET EXPLOIT_KIT Fake Browser Update Domain in TLS SNI (seyishalom .com)
- [ ] ET EXPLOIT_KIT ClearFake Fingerprinting Domain in TLS SNI (stats-best .site)
- [ ] ET EXPLOIT_KIT Fake Browser Update Domain in TLS SNI (phimnhanh .info)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (throatpills .org)
- [ ] ET EXPLOIT_KIT ClearFake Domain in DNS Lookup (dust-0001 .delorazahnow .workers .dev)
- [ ] ET EXPLOIT_KIT ClearFake Domain in TLS SNI (dust-0001 .delorazahnow .workers .dev)
- [ ] ET EXPLOIT_KIT ClearFake Domain in TLS SNI (pwwqkppwqkezqer .site)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in TLS SNI (googlestates .com)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (darkmansion .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (draggedline .org)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (marcborowy .com)
- [ ] ET EXPLOIT_KIT ClearFake Domain in DNS Lookup (gkrokbmrkmrxtmxrxr .space)
- [ ] ET EXPLOIT_KIT ClearFake Domain in DNS Lookup (owkdzodqzodqjefjnnejenefe .site)
- [ ] ET EXPLOIT_KIT ClearFake Domain in TLS SNI (gkrokbmrkmrxtmxrxr .space)
- [ ] ET EXPLOIT_KIT ClearFake Domain in TLS SNI (owkdzodqzodqjefjnnejenefe .site)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in TLS SNI (gctatick .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (xxxmir .info)
- [ ] ET EXPLOIT_KIT ClearFake Domain in TLS SNI (oiuytyfvq621mb .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (whitedrill .org)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (cristinaamaro .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (machinetext .org)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (krafttopia .net)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (greedyclowns .org)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (mansaentertainment .com)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in TLS SNI (import19ksnx9ajsn .com)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (redsnowynose .org)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in TLS SNI (statistiks-google .com)
- [ ] ET EXPLOIT_KIT ZPHP in TLS SNI (cpmmasters .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (credit-volta .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (credit-volta .com)
- [ ] ET EXPLOIT_KIT ScamClub Domain in DNS Lookup (Waytopmobirtb .com)
- [ ] ET EXPLOIT_KIT ScamClub Domain in DNS Lookup (waytopmobi .com)
- [ ] ET EXPLOIT_KIT ScamClub Domain in DNS Lookup (Apsbvl .space)
- [ ] ET EXPLOIT_KIT ScamClub Domain in DNS Lookup (axufcs .space)
- [ ] ET EXPLOIT_KIT ScamClub Domain in DNS Lookup (Namecheap Inc .)
- [ ] ET EXPLOIT_KIT ScamClub Domain in DNS Lookup (Namecheap Inc .)
- [ ] ET EXPLOIT_KIT ScamClub Domain in DNS Lookup (21bustqisw2 .top)
- [ ] ET EXPLOIT_KIT ScamClub Domain in TLS SNI (Waytopmobirtb .com)

- [ ] ET EXPLOIT_KIT ScamClub Domain in TLS SNI (Wstatkblsenmb1234 .top)
- [ ] ET EXPLOIT_KIT ScamClub Domain in TLS SNI (waytopmobi .com)
- [ ] ET EXPLOIT_KIT ScamClub Domain in TLS SNI (tetstwitn12 .xyz)
- [ ] ET EXPLOIT_KIT ScamClub Domain in TLS SNI (Apsbvl .space)
- [ ] ET EXPLOIT_KIT ScamClub Domain in TLS SNI (Bhgusz .space)
- [ ] ET EXPLOIT_KIT ScamClub Domain in TLS SNI (axufcs .space)
- [ ] ET EXPLOIT_KIT ScamClub Domain in TLS SNI (Luckypapa .top)
- [ ] ET EXPLOIT_KIT ScamClub Domain in TLS SNI (Namecheap Inc .)
- [ ] ET EXPLOIT_KIT ScamClub Domain in TLS SNI (Luckypuppy .top)
- [ ] ET EXPLOIT_KIT ScamClub Domain in TLS SNI (Namecheap Inc .)
- [ ] ET EXPLOIT_KIT ScamClub Domain in TLS SNI (bbd383ttka21 .top)
- [ ] ET EXPLOIT_KIT ScamClub Domain in TLS SNI (21bustqisw2 .top)
- [ ] ET EXPLOIT_KIT ScamClub Domain in TLS SNI (2022325luckyday .top)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (nilselsholz .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (nilselsholz .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (amazonascash .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (profille-cex-io .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (raloco .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (amazonascash .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (raloco .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (profille-cex-io .com)
- [ ] ET EXPLOIT_KIT Fake Browser Update Domain in DNS Lookup (onlinecasinopinup .xyz)
- [ ] ET EXPLOIT_KIT Fake Browser Update Domain in DNS Lookup (christopherchabannes .com)
- [ ] ET EXPLOIT_KIT Fake Browser Update Domain in TLS SNI (christopherchabannes .com)
- [ ] ET EXPLOIT_KIT Fake Browser Update Domain in DNS Lookup (s127581-statspixel .com)
- [ ] ET EXPLOIT_KIT Fake Browser Update Domain in TLS SNI (s127581-statspixel .com)
- [ ] ET EXPLOIT_KIT Fake Browser Update Domain in TLS SNI (onlinecasinopinup .xyz)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (residencialcasabrasileira .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (fablane .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (residencialcasabrasileira .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (fablane .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (configuratorpro .com)
- [x] ET EXPLOIT_KIT JavaScript DOS Injection
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (antiqueglossary .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (configuratorpro .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (antiqueglossary .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (eastrenclouds .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (eastrenclouds .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (gnavigatio .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (gnavigatio .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (climedballon .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (climedballon .org)
- [x] ET EXPLOIT_KIT Fake Chrome Update Landing Page Redirect to Payload (2023-10-26)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (arauas .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (gamefllix .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (arauas .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (gamefllix .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (dodgesteelbuildings .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (dodgesteelbuildings .com)
- [x] ET EXPLOIT_KIT RogueRaticate Domain in DNS Lookup (zxcdota2huysasi .com)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in DNS Lookup (rentfrejob .com)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in DNS Lookup (neurotonix--buy .us)
- [x] ET EXPLOIT_KIT RogueRaticate Domain in TLS SNI (zxcdota2huysasi .com)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in TLS SNI (rentfrejob .com)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in TLS SNI (neurotonix--buy .us)
- [x] ET EXPLOIT_KIT Keitaro Set-Cookie Inbound to RogueRaticate (212bb)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (implacavelvideos .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (kgscrew .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (implacavelvideos .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (kgscrew .com)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (metallife .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (metallife .org)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (cubicalwave .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (defeatdiseasewithdata .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (cubicalwave .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (defeatdiseasewithdata .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (cinaprofilm .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (cinaprofilm .com)
- [ ] ET EXPLOIT_KIT Fake Browser Update Domain in DNS Lookup (bingbuy .com)
- [ ] ET EXPLOIT_KIT Fake Browser Update Domain in TLS SNI (bingbuy .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (frightysever .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (bigbricks .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (frightysever .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (bigbricks .org)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in DNS Lookup (updateadobeflash .com)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in DNS Lookup (alsmgjk-igusj .com)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in TLS SNI (updateadobeflash .com)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in TLS SNI (alsmgjk-igusj .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (vibedroom .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (vibedroom .org)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (farmexpressmachine .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (pdfinfinity .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (farmexpressmachine .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (pdfinfinity .com)
- [x] ET EXPLOIT_KIT ClearFake Fingerprinting Domain in DNS Lookup (stats-tracked .com)
- [x] ET EXPLOIT_KIT ClearFake Fingerprinting Domain in TLS SNI (stats-tracked .com)

- [ ] ET EXPLOIT_KIT RogueRaticate Domain in DNS Lookup (koolstoredeluxe .com)
- [x] ET EXPLOIT_KIT Keitaro Set-Cookie Inbound to RogueRaticate (7fcd2)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (addisonlynch .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (addisonlynch .com)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in TLS SNI (izikatka0010 .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (limeerror .org)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (cwgmanagementllc .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (louisianaworkingdogs .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (louisianaworkingdogs .com)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (risenpeaches .org)
- [ ] ET EXPLOIT_KIT ClearFake Domain in TLS SNI (longlakeweb .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (forumsecrets .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (forumsecrets .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (treegreeny .org)
- [ ] ET EXPLOIT_KIT ClearFake Domain in TLS SNI (midatlanticlabel .com)
- [ ] ET EXPLOIT_KIT ClearFake Domain in TLS SNI (thebestthings1337 .online)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (daddygarages .org)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in TLS SNI (jagernaut .com)
- [ ] ET EXPLOIT_KIT ClearFake Domain in TLS SNI (excellentpatterns .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (informativosatelital .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (informativosatelital .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (paradoxmarine .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (emperorplan .org)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in DNS Lookup (en-za-wordpress .org)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in DNS Lookup (en-au-wordpress .org)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in DNS Lookup (en-us-wordpress .org)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in DNS Lookup (wordpress .securityplugins .org)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in DNS Lookup (wpsrv .zip)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in DNS Lookup (wpops .zip)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in TLS SNI (en-za-wordpress .org)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in TLS SNI (en-au-wordpress .org)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in TLS SNI (en-us-wordpress .org)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in TLS SNI (wordpress .securityplugins .org)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in TLS SNI (wpsrv .zip)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in TLS SNI (wpops .zip)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (jokergame1 .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (jokergame1 .com)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in TLS SNI (kokokakalala .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (mitchvandenborn .com)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in TLS SNI (koolstoredeluxe .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (andreeasasser .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (andreeasasser .com)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in DNS Lookup (izikatka0010 .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (limeerror .org)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (cwgmanagementllc .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (ilokod .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (ilokod .com)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (risenpeaches .org)
- [ ] ET EXPLOIT_KIT ClearFake Domain in DNS Lookup (longlakeweb .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (gpksanfrancisco .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (gpksanfrancisco .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (treegreeny .org)
- [ ] ET EXPLOIT_KIT ClearFake Domain in DNS Lookup (midatlanticlabel .com)
- [ ] ET EXPLOIT_KIT ClearFake Domain in DNS Lookup (thebestthings1337 .online)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (daddygarages .org)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in DNS Lookup (jagernaut .com)
- [ ] ET EXPLOIT_KIT ClearFake Domain in DNS Lookup (excellentpatterns .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (nelubelei .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (nelubelei .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (paradoxmarine .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (emperorplan .org)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in DNS Lookup (en-ca-wordpress .org)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in DNS Lookup (en-nz-wordpress .org)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in DNS Lookup (en-gb-wordpress .org)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in DNS Lookup (wordpress .secureplatform .org)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in DNS Lookup (wpgate .zip)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in DNS Lookup (wpsys .zip)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in TLS SNI (en-ca-wordpress .org)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in TLS SNI (en-nz-wordpress .org)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in TLS SNI (en-gb-wordpress .org)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in TLS SNI (wordpress .secureplatform .org)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in TLS SNI (wpgate .zip)
- [ ] ET EXPLOIT_KIT Fake WordPress CVE Plugin Domain in TLS SNI (wpsys .zip)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (perfilcovid .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (perfilcovid .com)
- [ ] ET EXPLOIT_KIT RogueRaticate Domain in DNS Lookup (kokokakalala .com)
- [x] ET EXPLOIT_KIT Keitaro Set-Cookie Inbound to RogueRaticate (17923)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (mindsnatchers .com)

- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (mitchvandenborn .com)
- [ ] ET EXPLOIT_KIT ClearFake Domain in DNS Lookup (marybskitchen .com)
- [ ] ET EXPLOIT_KIT ClearFake Domain in TLS SNI (marybskitchen .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (catsndogz .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (circuspride .org)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (lindarealtytulum .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (lindarealtytulum .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (biggerfun .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (confirmapply .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (froggysnow .org)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (proexbit .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (proximaideia .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (polatliems .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (onlinesavingsjournal .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (realestateagentnorfolkvirginia .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (ratingsentry .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (jennifergalvin .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (jesusanaya .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (jennifergalvin .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (jesusanaya .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (nowordshere .org)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (arkadyevna .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (boxtechcompany .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (choosetotruck .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (cloudwebhub .pro)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (electricnico .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (lazittarl .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (codecruncher .pro)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (mariateresacalderon .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (debasesingle .life)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (debasesingle .life)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (scorelineupdate .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (scorelineupdate .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (specialcraftbox .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (colorschemeas .com)
- [x] ET EXPLOIT_KIT Balada JavaScript Inject
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (bestselllerservice .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (listwithstats .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (decentralappps .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (getsmallcount .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (gybritanalytsesystem .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (linestoget .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (promsmotion .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (selectofmychoices .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (specialtaskevents .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (statisticplatform .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (mindsnatchers .com)
- [x] ET EXPLOIT_KIT ClearFake Domain in DNS Lookup (onewayskateboard .com)
- [x] ET EXPLOIT_KIT ClearFake Domain in TLS SNI (onewayskateboard .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (catsndogz .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (circuspride .org)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (fulfillityourself .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (fulfillityourself .com)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (froggysnow .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (biggerfun .org)
- [ ] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (confirmapply .org)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (onlinesavingsjournal .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (realestateagentnorfolkvirginia .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (proexbit .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (proximaideia .com)
- [ ] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (polatliems .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (ratingsentry .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (kineticwing .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (plannedtomatoes .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (kineticwing .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (plannedtomatoes .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (nowordshere .org)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (choosetotruck .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (arkadyevna .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (boxtechcompany .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (cloudwebhub .pro)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (electricnico .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (lazittarl .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (codecruncher .pro)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (mariateresacalderon .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (frenchpies .org)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (frenchpies .org)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (phinetik .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (phinetik .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (specialcraftbox .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (colorschemeas .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (beatifulllhistory .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (clickandanalytics .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (dataofpages .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (getmygateway .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (greenfastline .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (lineferaline .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (playerofsunshine .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (selectchoise .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (specialnewspaper .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (startperfectsolutions .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (statisticscripts .com)

- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (statisticsplatform .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (stratosbody .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (beatifullllhistory .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (bestselllerservice .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (clickandanalytics .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (compage .listwithstats .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (dataofpages .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (decentralappps .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (getmygateway .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (getsmallcount .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (greenfastline .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (gybritanalytsesystem .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (lineferaline .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (linestoget .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (playerofsunshine .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (promsmotion .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (selectchoise .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (selectofmychoices .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (specialnewspaper .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (specialtaskevents .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (startperfectsolutions .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (statisticplatform .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (statisticscripts .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (statisticsplatform .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (stratosbody .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (searchgear .pro)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (searchgear .pro)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (stablelightway .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (stablelightway .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (flyspecialline .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (flyspecialline .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (suezey .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (appboltonik .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (suezey .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (appboltonik .com)
- [x] ET EXPLOIT_KIT VexTrio Domain in DNS Lookup (bonustop-price .life)
- [x] ET EXPLOIT_KIT VexTrio Domain in DNS Lookup (allprizeshub .life)
- [x] ET EXPLOIT_KIT VexTrio Domain in DNS Lookup (greatbonushere .top)
- [x] ET EXPLOIT_KIT VexTrio Domain in DNS Lookup (prizes-topwin .life)
- [x] ET EXPLOIT_KIT VexTrio Domain in DNS Lookup (womanflirting .life)
- [x] ET EXPLOIT_KIT VexTrio Domain in DNS Lookup (a .crystalcraft .top)
- [x] ET EXPLOIT_KIT VexTrio Domain in DNS Lookup (logsmetrics .com)
- [x] ET EXPLOIT_KIT VexTrio Domain in DNS Lookup (webdatatrace .com)
- [x] ET EXPLOIT_KIT VexTrio Domain in TLS SNI (bonustop-price .life)
- [x] ET EXPLOIT_KIT VexTrio Domain in TLS SNI (allprizeshub .life)
- [x] ET EXPLOIT_KIT VexTrio Domain in TLS SNI (greatbonushere .top)
- [x] ET EXPLOIT_KIT VexTrio Domain in TLS SNI (prizes-topwin .life)
- [x] ET EXPLOIT_KIT VexTrio Domain in TLS SNI (womanflirting .life)
- [x] ET EXPLOIT_KIT VexTrio Domain in TLS SNI (a .crystalcraft .top)
- [x] ET EXPLOIT_KIT VexTrio Domain in TLS SNI (logsmetrics .com)
- [x] ET EXPLOIT_KIT VexTrio Domain in TLS SNI (webdatatrace .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (climosfevelt .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (climosfevelt .com)
- [x] ET EXPLOIT_KIT TA569 Middleware Domain in DNS Lookup (iredelltx .com)
- [x] ET EXPLOIT_KIT TA569 Middleware Domain in DNS Lookup (acuiplast .com)
- [x] ET EXPLOIT_KIT TA569 Middleware Domain in DNS Lookup (binder-sa .com)
- [x] ET EXPLOIT_KIT TA569 Middleware Domain in DNS Lookup (ficinity .com)
- [x] ET EXPLOIT_KIT TA569 Middleware Domain in TLS SNI (iredelltx .com)
- [x] ET EXPLOIT_KIT TA569 Middleware Domain in TLS SNI (acuiplast .com)
- [x] ET EXPLOIT_KIT TA569 Middleware Domain in TLS SNI (binder-sa .com)
- [x] ET EXPLOIT_KIT TA569 Middleware Domain in TLS SNI (ficinity .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in DNS Lookup (cachetransferjs .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in DNS Lookup (cachewebspace .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in DNS Lookup (googlecloudad .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in DNS Lookup (googlecloudns .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in DNS Lookup (ping .cachespace .net)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in DNS Lookup (sync .webappclick .net)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in DNS Lookup (storage .webfiledata .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in DNS Lookup (webcachedata .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in DNS Lookup (webdataspace .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in TLS SNI (cachetransferjs .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in TLS SNI (cachewebspace .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in TLS SNI (googlecloudad .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in TLS SNI (googlecloudns .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in TLS SNI (ping .cachespace .net)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in TLS SNI (sync .webappclick .net)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in TLS SNI (storage .webfiledata .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in TLS SNI (webcachedata .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in TLS SNI (webdataspace .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in DNS Lookup (visitclouds .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in TLS SNI (visitclouds .com)
- [x] ET EXPLOIT_KIT TA569 Middleware Domain in DNS Lookup (mwasro .com)
- [x] ET EXPLOIT_KIT TA569 Middleware Domain in TLS SNI (mwasro .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (lightsteper .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (lightsteper .com)
- [x] ET EXPLOIT_KIT VexTrio Domain in DNS Lookup (lookup-domain .com)
- [x] ET EXPLOIT_KIT VexTrio Domain in TLS SNI (lookup-domain .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (ripnoticebook .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (andiandnoah .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (ghostcitygames .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (ripnoticebook .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (andiandnoah .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (ghostcitygames .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in DNS Lookup (followcache .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in TLS SNI (followcache .com)
- [x] ET EXPLOIT_KIT Balada Domain in DNS Lookup (statisticsong .com)
- [x] ET EXPLOIT_KIT Balada Domain in TLS SNI (statisticsong .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (gigeconomycase .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (pngairservices .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (gigeconomycase .com)

- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (pngairservices .com)
- [x] ET EXPLOIT_KIT Fake Browser Update Domain in DNS Lookup (telotrace .com)
- [x] ET EXPLOIT_KIT Fake Browser Update Domain in TLS SNI (telotrace .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (eeatgoodx .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in TLS SNI (trust .resourcehost .net)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (oemmasters .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (oemmasters .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in DNS Lookup (share .clickstat360 .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in TLS SNI (share .clickstat360 .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (gspiceyl .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (tnoodlezy .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (snackfunp .com)
- [x] ET EXPLOIT_KIT TA569 Middleware Domain in TLS SNI (aitcaid .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in TLS SNI (visitscloud .com)
- [x] ET EXPLOIT_KIT TA569 Middleware Domain in TLS SNI (ronreznick .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (casinovipclubs .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (casinovipclubs .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (vfxfilmschool .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in TLS SNI (absolutecache .com)
- [x] ET EXPLOIT_KIT TA569 Middleware Domain in TLS SNI (germanclics .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (myclubpicks .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (myclubpicks .com)
- [x] ET EXPLOIT_KIT Fake Browser Update Domain in DNS Lookup (donnows .com)
- [x] ET EXPLOIT_KIT Fake Browser Update Domain in TLS SNI (donnows .com)
- [x] ET EXPLOIT_KIT Fake Browser Update Domain in TLS SNI (posiit .com)
- [x] ET EXPLOIT_KIT Fake Browser Update Domain in TLS SNI (freegeneratorai .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in TLS SNI (googlecloudstream .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (ads-quantum .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (gitbrancher .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (machineryideas .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (funcallback .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (asyncfunctionapi .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (asyncfunctionapi .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (bbsupplyandsalon .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (bigcuda .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (eoskinec .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (growcalm .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (aljannatquranteach .com)
- [x] ET EXPLOIT_KIT Fake Browser Update Domain in DNS Lookup (cdn3-jquery .info)
- [x] ET EXPLOIT_KIT Fake Browser Update Domain in TLS SNI (cdn3-jquery .info)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (eeatgoodx .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in DNS Lookup (trust .resourcehost .net)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (mysticselect .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (mysticselect .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in DNS Lookup (webdatacache .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in TLS SNI (webdatacache .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (tnoodlezy .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (snackfunp .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (gspiceyl .com)
- [x] ET EXPLOIT_KIT TA569 Middleware Domain in DNS Lookup (aitcaid .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in DNS Lookup (visitscloud .com)
- [x] ET EXPLOIT_KIT TA569 Middleware Domain in DNS Lookup (ronreznick .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (grantallardserver .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (grantallardserver .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (vfxfilmschool .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in DNS Lookup (absolutecache .com)
- [x] ET EXPLOIT_KIT TA569 Middleware Domain in DNS Lookup (germanclics .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (jimissupercool .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (jimissupercool .com)
- [x] ET EXPLOIT_KIT Fake Browser Update Domain in DNS Lookup (s14-nextjs .net)
- [x] ET EXPLOIT_KIT Fake Browser Update Domain in TLS SNI (s14-nextjs .net)
- [x] ET EXPLOIT_KIT Fake Browser Update Domain in DNS Lookup (posiit .com)
- [x] ET EXPLOIT_KIT Fake Browser Update Domain in DNS Lookup (freegeneratorai .com)
- [x] ET EXPLOIT_KIT Parrot TDS Domain in DNS Lookup (googlecloudstream .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (ads-quantum .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (gitbrancher .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (machineryideas .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (funcallback .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in DNS Lookup (varinspector .com)
- [x] ET EXPLOIT_KIT TA569 Keitaro TDS Domain in TLS SNI (varinspector .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (aljannatquranteach .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (betsmovepiyango47 .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (eduvationgroup .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (ezwhatsappp .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (grupodistribuidora .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (bbsupplyandsalon .com)

- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (betsmovepiyango47 .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (bigcuda .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (eduvationgroup .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (eoskinec .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (ezwhatsappp .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (growcalm .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (grupodistribuidora .com)
- [x] ET EXPLOIT_KIT TA569 Middleware Domain in DNS Lookup (egisela .com)
- [x] ET EXPLOIT_KIT TA569 Middleware Domain in TLS SNI (egisela .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (africanbeatmaker .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (aiifolrida .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (amarod .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in DNS Lookup (auburnartwalk .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (africanbeatmaker .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (aiifolrida .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (amarod .com)
- [x] ET EXPLOIT_KIT ZPHP Domain in TLS SNI (auburnartwalk .com)

emerging-ftp.rules Hide

- [ ] ET FTP USER login flowbit
- [ ] ET FTP HP-UX LIST command without login
- [x] ET FTP Possible FTP Daemon Username SELECT FROM SQL Injection Attempt
- [x] ET FTP Possible FTP Daemon Username DELETE FROM SQL Injection Attempt
- [x] ET FTP Possible FTP Daemon Username INSERT INTO SQL Injection Attempt
- [x] ET FTP Possible FTP Daemon Username UPDATE SET SQL Injection Attempt
- [x] ET FTP Possible FTP Daemon Username UNION SELECT SQL Injection Attempt
- [x] ET FTP Possible FTP Daemon Username INTO OUTFILE SQL Injection Attempt
- [ ] ET FTP FTP CWD command attempt without login
- [ ] ET FTP FTP SITE command attempt without login
- [ ] ET FTP FTP RMDIR command attempt without login
- [ ] ET FTP FTP MKDIR command attempt without login
- [ ] ET FTP FTP PWD command attempt without login
- [ ] ET FTP FTP RETR command attempt without login
- [ ] ET FTP FTP NLST command attempt without login
- [ ] ET FTP FTP RNTO command attempt without login
- [ ] ET FTP FTP RNFR command attempt without login
- [ ] ET FTP FTP STOR command attempt without login
- [ ] ET FTP ProFTPD Backdoor Inbound Backdoor Open Request (ACIDBITCHEZ)
- [x] ET FTP Outbound Java Anonymous FTP Login
- [x] ET FTP Outbound Java Downloading jar over FTP
- [x] ET FTP Vulnerable WS_FTP Version in FTP Banner Response (CVE-2023-40044)
- [ ] GPL FTP ADMw0rm ftp login attempt
- [ ] GPL FTP NextFTP client overflow
- [x] GPL FTP .forward
- [ ] GPL FTP .rhosts
- [x] GPL FTP CWD ~root attempt
- [ ] GPL FTP CEL overflow attempt
- [ ] GPL FTP SITE EXEC format string
- [ ] GPL FTP OpenBSD x86 ftpd
- [ ] GPL FTP PWD overflow
- [ ] GPL FTP XXXXX overflow
- [ ] GPL FTP wu-ftpd 2.6.0 site exec format string overflow Solaris 2.8
- [ ] GPL FTP wu-ftpd 2.6.0 site exec format string overflow FreeBSD
- [ ] GPL FTP wu-ftpd 2.6.0 site exec format string overflow Linux
- [ ] GPL FTP wu-ftpd 2.6.0 site exec format string overflow generic
- [ ] GPL FTP wu-ftpd 2.6.0 site exec format string check
- [ ] GPL FTP wu-ftpd 2.6.0
- [x] GPL FTP MKD overflow
- [x] GPL FTP iss scan
- [x] GPL FTP pass wh00t
- [x] GPL FTP passwd retrieval attempt
- [x] GPL FTP piss scan
- [x] GPL FTP saint scan
- [x] GPL FTP satan scan
- [ ] GPL FTP serv-u directory transversal
- [x] GPL FTP SITE EXEC attempt
- [x] GPL FTP tar parameters
- [ ] GPL FTP FTP no password
- [ ] GPL FTP FTP Bad login
- [ ] GPL FTP FTP 'STOR 1MB' possible warez site
- [ ] GPL FTP FTP 'RETR 1MB' possible warez site
- [ ] GPL FTP FTP 'CWD / ' possible warez site
- [ ] GPL FTP FTP 'CWD ' possible warez site
- [ ] GPL FTP MKD space space possible warez site
- [ ] GPL FTP FTP 'MKD .' possible warez site
- [ ] GPL FTP FTP anonymous login attempt
- [ ] GPL FTP MKD / possible warez site
- [x] GPL FTP CWD ...
- [x] GPL FTP STAT overflow attempt
- [ ] GPL FTP FTP file_id.diz access possible warez site
- [ ] GPL FTP FTP anonymous ftp login attempt
- [x] GPL FTP SITE overflow attempt
- [ ] GPL FTP format string attempt
- [x] GPL FTP SITE CHOWN overflow attempt
- [x] GPL FTP CMD overflow attempt
- [x] GPL FTP RNFR ./.// attempt
- [x] GPL FTP invalid MODE
- [x] GPL FTP large PWD command
- [ ] GPL FTP large SYST command
- [x] GPL FTP CWD ~ attempt
- [x] GPL FTP CWD ~ attempt
- [x] GPL FTP USER overflow attempt
- [ ] GPL FTP command overflow attempt
- [ ] GPL FTP STAT * dos attempt
- [ ] GPL FTP STAT ? dos attempt
- [x] GPL FTP CWD .... attempt
- [x] GPL FTP SITE NEWER attempt
- [x] GPL FTP SITE CPWD overflow attempt
- [x] GPL FTP CWD overflow attempt
- [x] GPL FTP SITE NEWER overflow attempt
- [x] GPL FTP SITE ZIPCHK overflow attempt
- [x] GPL FTP authorized_keys file transferred
- [x] GPL FTP shadow retrieval attempt
- [x] GPL FTP RMDIR overflow attempt
- [ ] GPL FTP SITE EXEC format string attempt
- [x] GPL FTP PASS overflow attempt
- [x] GPL FTP MKD overflow attempt
- [x] GPL FTP REST overflow attempt
- [x] GPL FTP DELE overflow attempt
- [x] GPL FTP RMD overflow attempt
- [x] GPL FTP LIST directory traversal attempt
- [x] GPL FTP CWD Root directory transversal attempt
- [ ] GPL FTP USER format string attempt
- [ ] GPL FTP PASS format string attempt
- [ ] GPL FTP LIST integer overflow attempt
- [ ] GPL FTP MKDIR format string attempt
- [ ] GPL FTP RENAME format string attempt

- [ ] GPL FTP LIST buffer overflow attempt
- [ ] GPL FTP SITE CHMOD overflow attempt
- [ ] GPL FTP STOR overflow attempt
- [ ] GPL FTP XCWD overflow attempt
- [x] GPL FTP XMKD overflow attempt
- [x] GPL FTP NLST overflow attempt
- [x] GPL FTP RNTO overflow attempt
- [x] GPL FTP STOU overflow attempt
- [x] GPL FTP APPE overflow attempt
- [x] GPL FTP RETR overflow attempt
- [x] GPL FTP invalid MDTM command attempt
- [ ] GPL FTP format string attempt
- [x] GPL FTP ALLO overflow attempt
- [x] GPL FTP MDTM overflow attempt
- [ ] GPL FTP RETR format string attempt
- [x] GPL FTP RNFR overflow attempt
- [x] GPL FTP PORT bounce attempt
- [ ] GPL FTP REST with numeric argument

- [ ] **emerging-games.rules** Show
- [x] **emerging-hunting.rules** Hide

- [ ] ET HUNTING OUTBOUND Suspicious Email Attachment
- [x] ET HUNTING Suspicious FTP 220 Banner on Local Port (-)
- [x] ET HUNTING Suspicious Mozilla User-Agent - Likely Fake (Mozilla/4.0)
- [ ] ET HUNTING Suspicious Mozilla User-Agent typo (MOzilla/4.0)
- [ ] ET HUNTING Suspicious Mozilla User-Agent Separator - likely Fake (Mozilla/4.0+(compatible +MSIE+)
- [x] ET HUNTING Double User-Agent (User-Agent User-Agent)
- [x] ET HUNTING Suspicious User Agent (_)
- [x] ET HUNTING Suspicious Empty User-Agent
- [x] ET HUNTING Suspicious User-Agent (c \windows)
- [x] ET HUNTING Suspicious User-Agent (NULL)
- [x] ET HUNTING Suspicious User-Agent (C slash)
- [x] ET HUNTING FTP CWD to windows system32 - Suspicious
- [ ] ET HUNTING Suspicious SMTP handshake outbound
- [ ] ET HUNTING Suspicious SMTP handshake reply
- [x] ET HUNTING Suspicious Malformed Double Accept Header
- [ ] ET HUNTING Suspicious Executable (Win exe under 128)
- [ ] ET HUNTING Suspicious Executable (PE offset 160)
- [ ] ET HUNTING Suspicious Executable (PE offset 512)
- [x] ET HUNTING Set flow on bmp file get
- [ ] ET HUNTING Suspicious Mozilla User-Agent Likely Fake (Mozilla/5.0)
- [x] ET HUNTING Suspicious Chmod Usage in URI (Inbound)
- [ ] ET HUNTING Data POST to an image file (gif)
- [ ] ET HUNTING Data POST to an image file (jpg)
- [ ] ET HUNTING Data POST to an image file (jpeg)
- [ ] ET HUNTING Data POST to an image file (bmp)
- [ ] ET HUNTING Data POST to an image file (png)
- [x] ET HUNTING Suspicious HTML Script Tag in 401 Unauthorized Response (External Source)
- [ ] ET HUNTING Suspicious User-Agent Beginning with digits - Likely spyware/trojan
- [ ] ET HUNTING Suspicious Non-Escaping backslash in User-Agent Outbound
- [ ] ET HUNTING Suspicious Non-Escaping backslash in User-Agent Inbound
- [x] ET HUNTING Suspicious exe.exe request - possible downloader/Oficla
- [ ] ET HUNTING Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake
- [ ] ET HUNTING Suspicious FTP 220 Banner on Local Port (spaced)
- [x] ET HUNTING Suspicious POST With Reference to WINDOWS Folder Possible Malware Infection
- [x] ET HUNTING Suspicious Percentage Symbol Usage in FTP Username
- [x] ET HUNTING Suspicious Quotation Mark Usage in FTP Username
- [x] ET HUNTING Abnormal User-Agent No space after colon - Likely Hostile
- [x] ET HUNTING Zero Content-Length HTTP POST with data (outbound)
- [x] ET HUNTING Suspicious Embedded Shockwave Flash In PDF
- [x] ET HUNTING Suspicious Purported MSIE 7 with terse HTTP Headers GET to PHP
- [x] ET HUNTING Hiloti Style GET to PHP with invalid terse MSIE headers
- [ ] ET HUNTING Suspicious IAT HttpAddRequestHeader - Can Be Used For HTTP CnC
- [ ] ET HUNTING Suspicious IAT ZwProtectVirtualMemory - Undocumented API Which Can be Used for Rootkit Functionality
- [ ] ET HUNTING Suspicious IAT EnableExecuteProtectionSupport - Undocumented API to Modify DEP
- [ ] ET HUNTING Suspicious IAT SetKeyboardState - Can Be Used for Keylogging
- [x] ET HUNTING EXE Using Suspicious IAT ZwUnmapViewOfSection Possible Malware Process Hollowing
- [x] ET HUNTING Suspicious User-Agent Containing .exe
- [x] ET HUNTING Suspicious User-Agent (Agent and 5 or 6 digits)
- [x] ET HUNTING SUSPICIOUS *.doc.exe in HTTP URL
- [x] ET HUNTING SUSPICIOUS *.pdf.exe in HTTP URL
- [x] ET HUNTING SUSPICIOUS *.doc.exe in HTTP HEADER
- [x] ET HUNTING SUSPICIOUS *.pdf.exe in HTTP HEADER
- [x] ET HUNTING Suspicious HTTP Request for gift.exe
- [ ] ET HUNTING Suspicious Self Signed SSL Certificate CN of common Possible SSL CnC
- [ ] ET HUNTING Suspicious Self Signed SSL Certificate with admin@common Possible SSL CnC
- [x] ET HUNTING Suspicious Invalid HTTP Accept Header of ?
- [x] ET HUNTING PDF Containing Subform with JavaScript
- [x] ET HUNTING Suspicious HTTP Referer C Drive Path
- [x] ET HUNTING EXE Download With Content Type Specified As Empty
- [ ] ET HUNTING PDF embedded in XDP file (Possibly Malicious)
- [x] ET HUNTING Suspicious Windows Executable WriteProcessMemory
- [x] ET HUNTING Suspicious Windows Executable CreateRemoteThread
- [x] ET HUNTING Suspicious Windows NT version 7 User-Agent
- [x] ET HUNTING Suspicious Windows NT version 8 User-Agent
- [x] ET HUNTING Suspicious Windows NT version 9 User-Agent
- [x] ET HUNTING Suspicious Windows NT version 1 User-Agent
- [x] ET HUNTING Suspicious Windows NT version 2 User-Agent
- [x] ET HUNTING Suspicious Windows NT version 3 User-Agent
- [x] ET HUNTING Suspicious svchost.exe in URI - Possible Process Dump/ Trojan Download
- [x] ET HUNTING Suspicious winlogin.exe in URI
- [x] ET HUNTING Suspicious services.exe in URI
- [x] ET HUNTING Suspicious lsass.exe in URI
- [x] ET HUNTING Suspicious explorer.exe in URI
- [x] ET HUNTING Suspicious smss.exe in URI
- [x] ET HUNTING Suspicious csrss.exe in URI
- [x] ET HUNTING Suspicious rundll32.exe in URI
- [x] ET HUNTING Suspicious Possible CollectGarbage in base64 1
- [x] ET HUNTING Suspicious Possible CollectGarbage in base64 2
- [x] ET HUNTING Suspicious Possible CollectGarbage in base64 3
- [ ] ET HUNTING Suspicious Windows NT version 0 User-Agent
- [x] ET HUNTING Invalid User-Agent - MSIE 9 on Windows NT 5
- [x] ET HUNTING Suspicious MSIE 10 on Windows NT 5
- [x] ET HUNTING SUSPICIOUS IRC - PRIVMSG *.(exe|tar|tgz|zip) download command
- [x] ET HUNTING SUSPICIOUS IRC - NICK and 3 Letter Country Code

- [x] ET HUNTING SUSPICIOUS IRC - NICK and Possible Windows XP/7
- [x] ET HUNTING SUSPICIOUS IRC - NICK and -PC
- [x] ET HUNTING SUSPICIOUS Reassigned Eval Function 2
- [x] ET HUNTING SUSPICIOUS UA (iexplore)
- [x] ET HUNTING SUSPICIOUS Word DOCX with Many ActiveX Objects and Media
- [x] ET HUNTING SUSPICIOUS taskmgr.exe in URI Probable Process Dump/ Trojan Download
- [x] ET HUNTING SUSPICIOUS connhost.exe in URI Probable Process Dump/Trojan Download
- [x] ET HUNTING SUSPICIOUS wimhost.exe in URI Probable Process Dump/ Trojan Download
- [x] ET HUNTING SUSPICIOUS waulct.exe in URI Probable Process Dump/ Trojan Download
- [x] ET HUNTING SUSPICIOUS mssrs.exe in URI Probable Process Dump/ Trojan Download
- [x] ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class file Accessing Security Manager
- [x] ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class Accessing Importing glassfish
- [x] ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class Importing jmx mbeanserver
- [x] ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class Importing glassfish external statistics impl
- [x] ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class Mozilla JS Class Creation
- [x] ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class Importing tracing Provider Factory
- [x] ET HUNTING SUSPICIOUS winhost(32|64).exe in URI
- [x] ET HUNTING SUSPICIOUS SMTP EXE - ZIP file with .exe filename inside (Inbound)
- [x] ET HUNTING SUSPICIOUS SMTP EXE - EXE SMTP Attachment
- [x] ET HUNTING SUSPICIOUS SMTP EXE - RAR file with .com filename inside
- [x] ET HUNTING SUSPICIOUS SMTP EXE - RAR file with .scr filename inside
- [x] ET HUNTING suspicious - gzipped file via JAVA - could be pack200-ed JAR
- [ ] ET HUNTING Suspicious User-Agent 100 non-printable char
- [x] ET HUNTING Suspicious Request for Pdf.exe Observed in Zeus/ Luminosity Link
- [x] ET HUNTING SUSPICIOUS .PIF File Inside of Zip
- [x] ET HUNTING SUSPICIOUS Java Lang Runtime in Response
- [x] ET HUNTING SUSPICIOUS .exe Downloaded from SVN/HTTP on GoogleCode
- [x] ET HUNTING JAR Sent Claiming To Be Image - Likely Exploit Kit
- [x] ET HUNTING Self-Signed Cert O=XX Observed
- [x] ET HUNTING GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 2
- [x] ET HUNTING SUSPICIOUS Crystalize Filter in Uncompressed Flash
- [x] ET HUNTING SUSPICIOUS Possible automated connectivity check (www.msn.com)
- [x] ET HUNTING SUSPICIOUS Possible automated connectivity check (www.yahoo.com)
- [x] ET HUNTING SUSPICIOUS EXE Download from Google Common Data Storage with no Referer
- [x] ET HUNTING Generic .bin download from Dotted Quad
- [x] ET HUNTING Generic CollectGarbage in Hex
- [x] ET HUNTING SUSPICIOUS SMTP Attachment Inbound PPT attachment with Embedded OLE Object M1
- [x] ET HUNTING SUSPICIOUS SMTP Attachment Inbound PPT attachment with Embedded OLE Object M3
- [x] ET HUNTING SUSPICIOUS IRC - NICK and Win
- [x] ET HUNTING SUSPICIOUS Reassigned Eval Function 1
- [x] ET HUNTING SUSPICIOUS Reassigned Eval Function 3
- [ ] ET HUNTING SUSPICIOUS Possible Secondary Indicator of Java Exploit (Artifact Observed mostly in EKs/a few mis-configured apps)
- [x] ET HUNTING SUSPICIOUS msctcd.exe in URI Probable Process Dump/ Trojan Download
- [x] ET HUNTING SUSPICIOUS wsqmocn.exe in URI Probable Process Dump/Trojan Download
- [x] ET HUNTING SUSPICIOUS lgfxsrvc.exe in URI Probable Process Dump/ Trojan Download
- [x] ET HUNTING SUSPICIOUS winlog.exe in URI Probable Process Dump/ Trojan Download
- [x] ET HUNTING SUSPICIOUS alg.exe in URI Probable Process Dump/ Trojan Download
- [x] ET HUNTING SUSPICIOUS winhosts.exe in URI Probable Process Dump/Trojan Download
- [x] ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class file Importing Protection Domain
- [x] ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class B64 encoded class
- [x] ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class Importing mbeanserver Introspector
- [x] ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class Importing management MBeanServer
- [x] ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class Hex Encoded Class file
- [x] ET HUNTING SUSPICIOUS Java Request With Uncompressed JAR/Class Importing Classes used in awt exploits
- [x] ET HUNTING SUSPICIOUS pony.exe in URI
- [x] ET HUNTING SUSPICIOUS SMTP EXE - RAR file with .exe filename inside
- [x] ET HUNTING SUSPICIOUS SMTP EXE - ZIP file with .com filename inside
- [x] ET HUNTING SUSPICIOUS SMTP EXE - ZIP file with .scr filename inside
- [x] ET HUNTING suspicious - uncompressed pack200-ed JAR
- [x] ET HUNTING Suspicious Possible Process Dump in POST body
- [x] ET HUNTING Suspicious UA (^IE[\d\s])
- [x] ET HUNTING Suspicious Jar name JavaUpdate.jar
- [x] ET HUNTING SUSPICIOUS .CPL File Inside of Zip
- [x] ET HUNTING SUSPICIOUS XXTEA UTF-16 Encoded HTTP Response
- [x] ET HUNTING HTTP request for resource ending in .scr
- [x] ET HUNTING JAR Sent Claiming To Be Text Content - Likely Exploit Kit
- [x] ET HUNTING GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1
- [x] ET HUNTING SUSPICIOUS OVH Shared Host SSL Certificate (Observed In Use by Some Trojans)
- [x] ET HUNTING SUSPICIOUS Possible automated connectivity check (www.google.com)
- [x] ET HUNTING SUSPICIOUS Possible automated connectivity check (www.bing.com)
- [x] ET HUNTING SUSPICIOUS Possible WebShell Login Form (Outbound)
- [x] ET HUNTING HTTP Executable Download from suspicious domain with direct request/fake browser (multiple families)
- [x] ET HUNTING Suspicious Base64 Encoded ZIP File in HTML Body (Magic Bytes)
- [x] ET HUNTING SUSPICIOUS PPT Download with Embedded OLE Object
- [x] ET HUNTING SUSPICIOUS SMTP Attachment Inbound PPT attachment with Embedded OLE Object M2
- [x] ET HUNTING SUSPICIOUS SMTP Attachment Inbound PPT attachment with Embedded OLE Object M4

- [x] ET HUNTING SUSPICIOUS SMTP Attachment Inbound PPT attachment with Embedded OLE Object M5
- [x] ET HUNTING SUSPICIOUS Possible Office Doc with Embedded VBA Project
- [x] ET HUNTING SUSPICIOUS Possible Office Doc with Embedded VBA Project (Wide)
- [x] ET HUNTING SUSPICIOUS *.rar.exe in HTTP URL
- [x] ET HUNTING Windows nbtstat -r Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET HUNTING Download file with BITS via LNK file (Likely Malicious)
- [x] ET HUNTING Suspicious SWF filename movie(dot)swf in doc root
- [x] ET HUNTING Suspicious Script Loaded from Pastebin
- [x] ET HUNTING Suspicious Accept in HTTP POST - Possible Alphacrypt/ TeslaCrypt
- [x] ET HUNTING Suspicious BITS EXE DL From Dotted Quad
- [x] ET HUNTING SUSPICIOUS Firesale gTLD IE Flash request to set non-standard filename (some overlap with 2021752)
- [x] ET HUNTING SUSPICIOUS Excel Add-in Download M1
- [ ] ET HUNTING Suspicious SMTP Settings in XLS - Possible Phishing Document
- [ ] ET HUNTING SUSPICIOUS busybox shell
- [x] ET HUNTING Suspicious HTTP Refresh to SMS Aug 16 2016
- [x] ET HUNTING Possible EXE Download From Suspicious TLD (.science) - set
- [x] ET HUNTING Possible EXE Download From Suspicious TLD (.stream) - set
- [x] ET HUNTING Possible EXE Download From Suspicious TLD (.gdn) - set
- [x] ET HUNTING Possible EXE Download From Suspicious TLD (.accountant) - set
- [x] ET HUNTING Possible EXE Download From Suspicious TLD (.link) - set
- [x] ET HUNTING Possible EXE Download From Suspicious TLD
- [x] ET HUNTING Suspicious VNC Remote Admin Request
- [x] ET HUNTING ARM Binary Downloaded via WGET Containing Suspicious Netcat Command - Possible IoT Malware
- [x] ET HUNTING Suspicious Possible Zip DL containing single VBS script
- [x] ET HUNTING SUSPICIOUS PSHELL Downloader Primitives B641 Oct 19 2017
- [x] ET HUNTING SUSPICIOUS PSHELL Downloader Primitives B643 Oct 19 2017
- [x] ET HUNTING SUSPICIOUS PSHELL Downloader Primitives B645W Oct 19 2017
- [x] ET HUNTING Suspicious Request for Doc to IP Address with Terse Headers
- [x] ET HUNTING Observed Let's Encrypt Certificate for Suspicious TLD (.gdn)
- [x] ET HUNTING Observed Let's Encrypt Certificate for Suspicious TLD (.ga)
- [x] ET HUNTING Observed Let's Encrypt Certificate for Suspicious TLD (.xyz)
- [x] ET HUNTING Possible EXE Download From Suspicious TLD (.webcam) - set
- [x] ET HUNTING Possible EXE Download From Suspicious TLD (.tokyo) - set
- [x] ET HUNTING Possible EXE Download From Suspicious TLD (.work) - set
- [x] ET HUNTING Suspicious EXE Download Content-Type image/jpeg
- [x] ET HUNTING Observed Suspicious SSL Cert (External IP Lookup - ident .me)
- [x] ET HUNTING Possible EXE Download From Suspicious TLD (.icu) - set
- [x] ET HUNTING SUSPICIOUS SMTP Attachment Inbound PPT attachment with Embedded OLE Object M6
- [x] ET HUNTING SUSPICIOUS Possible Office Doc with Embedded VBA Project
- [x] ET HUNTING Terse Named Filename EXE Download - Possibly Hostile
- [x] ET HUNTING Generic - Mozilla 4.0 EXE Request
- [x] ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response
- [x] ET HUNTING Suspicious X-mailer Synapse Inbound to SMTP Server
- [x] ET HUNTING SUSPICIOUS Possible Evil Download wsf Double Ext No Referer
- [x] ET HUNTING Download Request Containing Suspicious Filename - Crypted
- [x] ET HUNTING SUSPICIOUS Single JS file inside of ZIP Download (Observed as lure in malspam campaigns)
- [x] ET HUNTING SUSPICIOUS EXE Download from specific file share site (used in recent maldoc campaign)
- [x] ET HUNTING SUSPICIOUS Firesale gTLD EXE DL with no Referer June 13 2016
- [x] ET HUNTING SUSPICIOUS Excel Add-in Download M2
- [x] ET HUNTING SUSPICIOUS Path to BusyBox
- [ ] ET HUNTING SUSPICIOUS busybox enable
- [x] ET HUNTING Suspicious Proxifier DL (non-browser observed in maldoc campaigns)
- [x] ET HUNTING Possible EXE Download From Suspicious TLD (.top) - set
- [x] ET HUNTING Possible EXE Download From Suspicious TLD (.download) - set
- [x] ET HUNTING Possible EXE Download From Suspicious TLD (.biz) - set
- [x] ET HUNTING Possible EXE Download From Suspicious TLD (.click) - set
- [x] ET HUNTING Possible EXE Download From Suspicious TLD (.win) - set
- [x] ET HUNTING Suspicious Empty SSL Certificate - Observed in Cobalt Strike
- [x] ET HUNTING SUSPICIOUS Local file read using read protocol
- [x] ET HUNTING Request for .bin with BITS/ User-Agent
- [x] ET HUNTING SUSPICIOUS DOC Download from commonly abused file share site
- [x] ET HUNTING SUSPICIOUS PSHELL Downloader Primitives B642 Oct 19 2017
- [x] ET HUNTING SUSPICIOUS PSHELL Downloader Primitives B644W Oct 19 2017
- [x] ET HUNTING SUSPICIOUS PSHELL Downloader Primitives B645W Oct 19 2017
- [x] ET HUNTING Observed Let's Encrypt Certificate for Suspicious TLD (.ml)
- [x] ET HUNTING Observed Let's Encrypt Certificate for Suspicious TLD (.gq)
- [x] ET HUNTING Observed Let's Encrypt Certificate for Suspicious TLD (.cf)
- [x] ET HUNTING Possible EXE Download From Suspicious TLD (.men) - set
- [x] ET HUNTING Possible EXE Download From Suspicious TLD (.yokohama) - set
- [x] ET HUNTING Possible EXE Download From Suspicious TLD (.gq) - set
- [x] ET HUNTING Suspicious Redirect to Download EXE from Bitbucket
- [x] ET HUNTING Possibly Suspicious Request for Putty.exe from Non-Standard Download Location
- [x] ET HUNTING Observed Let's Encrypt Certificate for Suspicious TLD (.icu)
- [x] ET HUNTING PowerShell Hidden Window Command Common In Powershell Stagers M1

- [x] ET HUNTING PowerShell Hidden Window Command Common In Powershell Stagers M2
- [x] ET HUNTING PowerShell DownloadFile Command Common In Powershell Stagers
- [x] ET HUNTING PowerShell DownloadData Command Common In Powershell Stagers
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (cookies.txt) M2
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (passwords.txt) M2
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (screenshot.) M2
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (wallet.dat) M2
- [x] ET HUNTING Possible Powershell .ps1 Script Use Over SMB
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (cookie.txt) M1
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (ccdata.txt) M1
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (google_chrome_default_) M1
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Mozilla_Firefox_Cookies) M1
- [x] ET HUNTING Suspicious Registrar Nameservers in DNS Response (carbon2u)
- [x] ET HUNTING Suspicious User-Agent (Random String)
- [x] ET HUNTING Generic IOT Downloader Malware in GET (Outbound)
- [x] ET HUNTING Generic IOT Downloader Malware in GET (Inbound)
- [x] ET HUNTING Suspicious Chmod Usage in URI (Outbound)
- [x] ET HUNTING Powershell Downloader with Start-Process Inbound M1
- [ ] ET HUNTING [TGI] Entrust Entelligence Security Provider (Flowbits Set)
- [x] ET HUNTING EXE Base64 Encoded potential malware
- [x] ET HUNTING EXE Downloaded from Github
- [x] ET HUNTING Generic IOT Downloader Malware in GET (Inbound)
- [x] ET HUNTING Observed Lets Encrypt Certificate - Possible COVID-19 Related M1
- [x] ET HUNTING Possible COVID-19 Domain in SSL Certificate M1
- [x] ET HUNTING Suspicious TLS SNI Request for Possible COVID-19 Domain M1
- [x] ET HUNTING Suspicious Domain Request for Possible COVID-19 Domain M1
- [x] ET HUNTING Suspicious GET Request with Possible COVID-19 Domain M1
- [x] ET HUNTING Suspicious POST Request with Possible COVID-19 Domain M1
- [x] ET HUNTING Suspicious GET Request with Possible COVID-19 URI M1
- [x] ET HUNTING Suspicious POST Request with Possible COVID-19 URI M1
- [x] ET HUNTING Possible Covid19 Themed Email Spam Outbound M2
- [x] ET HUNTING Possible Covid19 Themed Email Spam Outbound M4
- [x] ET HUNTING Possible Covid19 Themed Email Spam Outbound M6
- [x] ET HUNTING Request for EXE via WinHTTP M2
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Hardware.txt)
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (CookiesList.txt)
- [x] ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.oz)
- [x] ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.geek)
- [x] ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.dyn)
- [x] ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.neo)
- [x] ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.null)
- [x] ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.chan)
- [x] ET HUNTING PowerShell NonInteractive Command Common In Powershell Stagers
- [x] ET HUNTING PowerShell DownloadString Command Common In Powershell Stagers
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (cookies.txt) M1
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (passwords.txt) M1
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (screenshot.) M1
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (wallet.dat) M1
- [x] ET HUNTING Suspicious POST with Common Windows Process Names - Possible Process List Exfiltration
- [x] ET HUNTING HTTP Request with Double Cache-Control
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (cookie.txt) M2
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (ccdata.txt) M2
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (google_chrome_default_) M2
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Mozilla_Firefox_Cookies) M2
- [ ] ET HUNTING Observed Suspicious UA (Windows)
- [x] ET HUNTING Generic IOT Downloader Malware in POST (Outbound)
- [x] ET HUNTING Generic IOT Downloader Malware in POST (Inbound)
- [x] ET HUNTING Suspicious TLS SNI Request for Root
- [x] ET HUNTING Telegram API Certificate Observed
- [x] ET HUNTING Suspicious EXE requested with Java UA
- [ ] ET HUNTING [TGI] Possible Cobalt Strike Extra Whitespace HTTP Response
- [x] ET HUNTING Bit.do Shortened Link Request to EXE
- [x] ET HUNTING Generic IOT Downloader Malware in GET (Outbound)
- [x] ET HUNTING Suspected Malicious Telegram Communication (POST)
- [x] ET HUNTING Observed Lets Encrypt Certificate - Possible COVID-19 Related M2
- [x] ET HUNTING Possible COVID-19 Domain in SSL Certificate M2
- [x] ET HUNTING Suspicious TLS SNI Request for Possible COVID-19 Domain M2
- [ ] ET HUNTING Suspicious Domain Request for Possible COVID-19 Domain M2
- [x] ET HUNTING Suspicious GET Request with Possible COVID-19 Domain M2
- [x] ET HUNTING Suspicious POST Request with Possible COVID-19 Domain M2
- [x] ET HUNTING Suspicious GET Request with Possible COVID-19 URI M2
- [x] ET HUNTING Suspicious POST Request with Possible COVID-19 URI M2
- [x] ET HUNTING Possible Covid19 Themed Email Spam Outbound M3
- [x] ET HUNTING Possible Covid19 Themed Email Spam Outbound M5
- [x] ET HUNTING Request for EXE via WinHTTP M1
- [x] ET HUNTING Request for EXE via WinHTTP M3
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Prgrm.txt)
- [x] ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.parody)
- [x] ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.cyb)
- [x] ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.libre)
- [x] ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.bbs)
- [x] ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.o)
- [x] ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.pirate)
- [x] ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.oss)

- [x] ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.epic)
- [x] ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.gopher)
- [x] ET HUNTING Observed DNS Query for EmerDNS TLD (.coin)
- [x] ET HUNTING Observed DNS Query for EmerDNS TLD (.bazar)
- [x] ET HUNTING Suspicious NULL DNS Request
- [ ] ET HUNTING Suspicious Request for Terse Numeric .dat File
- [x] ET HUNTING Suspicious Terse Request for .pif
- [x] ET HUNTING Possible Malicious Document Request to NOIP DynDNS Domain
- [x] ET HUNTING Possible Malicious Document Request to ChangeIP Dynamic DNS Domain
- [x] ET HUNTING Possible Malicious Document Request to Afraid.org Top 100 Dynamic DNS Domain
- [x] ET HUNTING Possible Malicious Document Request to Hostinger Domains
- [x] ET HUNTING Possible Malicious Document Request to .tk domain
- [x] ET HUNTING HTTP POST Form Submitted to Weebly Free Hosting
- [x] ET HUNTING HTTP POST to .php on Appspot Hosting - Possible Phishing
- [x] ET HUNTING Suspicious GET To gate.php with no Referer
- [x] ET HUNTING Suspicious HTTP POST to Free Web Host Atwebpages
- [x] ET HUNTING Request to .XYZ Domain with Minimal Headers
- [x] ET HUNTING Request to 000webhostapp Domain with Minimal Headers
- [x] ET HUNTING Request to .CF Domain with Minimal Headers
- [x] ET HUNTING Request to .TK Domain with Minimal Headers
- [x] ET HUNTING Improperly Spaced Accept Header in User-Agent
- [x] ET HUNTING Suspicious PHP Code in HTTP POST (Inbound)
- [x] ET HUNTING Suspicious PHP Code in HTTP POST (Inbound)
- [x] ET HUNTING HTTP POST to XYZ TLD Containing Pass - Possible Phishing
- [x] ET HUNTING Suspicious HTTP POST Only Containing Pass - Possible Phishing
- [x] ET HUNTING Suspicious POST Format
- [x] ET HUNTING Suspicious POST Format
- [x] ET HUNTING Observed Interesting Content-Type Inbound (application/x-sh)
- [x] ET HUNTING Suspicious Glitch Hosted GET Request - Possible Phishing Landing
- [x] ET HUNTING Suspicious Glitch Hosted TLS SNI Request - Possible Phishing Landing
- [x] ET HUNTING Observed Suspicious SSL Cert (Metasploit in TLS Subject)
- [x] ET HUNTING Generic Powershell DownloadString Command
- [x] ET HUNTING Generic Powershell Starting Wscript Process
- [x] ET HUNTING Terse Request for EXE from DigitalOcean Spaces
- [x] ET HUNTING SSL/TLS Certificate Observed (OpenNIC Project API)
- [x] ET HUNTING Suspicious Netlify Hosted GET Request - Possible Phishing Landing
- [x] ET HUNTING Suspicious Netlify Hosted TLS SNI Request - Possible Phishing Landing
- [x] ET HUNTING Base64 Encoded Server Response (success)
- [x] ET HUNTING Suspicious GET Request for .x64
- [x] ET HUNTING Office Doc Retrieving Shortened URL (bit .do)
- [ ] ET HUNTING Suspected DNS CnC via TXT queries
- [x] ET HUNTING jpg download from fileupload .site
- [x] ET HUNTING Suspicious Windows Commands in POST Body (ipconfig)
- [x] ET HUNTING Suspicious Windows Commands in POST Body (net config)
- [x] ET HUNTING Observed DNS Query for OpenNIC Alternative DNS TLD (.indy)
- [x] ET HUNTING Observed DNS Query for EmerDNS TLD (.lib)
- [x] ET HUNTING Observed DNS Query for EmerDNS TLD (.emc)
- [x] ET HUNTING Observed DNS Query for FurNIC TLD (.fur)
- [x] ET HUNTING URL Observed in PDF Downloaded via Dropbox
- [x] ET HUNTING Suspicious Terse Request for .bmp
- [x] ET HUNTING Possible Malicious Document Request to NOIP DynDNS Domain
- [x] ET HUNTING Possible Malicious Document Request to ChangeIP Dynamic DNS Domain
- [x] ET HUNTING Possible Malicious Document Request to Afraid.org Top 100 Dynamic DNS Domain
- [x] ET HUNTING Possible Malicious Document Request to Hostinger Domains
- [x] ET HUNTING Possible Malicious Document Request to .tk domain
- [x] ET HUNTING HTTP POST Form Submitted to 123formbuilder Free Hosting
- [x] ET HUNTING Cloned Page Hosted on Microsoft Hosting
- [x] ET HUNTING Suspicious Request to Image with User-Agent Ending in .exe
- [x] ET HUNTING Microsoft Malware Protection User-Agent Observed to Non-Microsoft Domain
- [x] ET HUNTING Google Adwords Conversion not from Google
- [x] ET HUNTING Request to .TOP Domain with Minimal Headers
- [x] ET HUNTING Request to .ML Domain with Minimal Headers
- [x] ET HUNTING Request to .GQ Domain with Minimal Headers
- [x] ET HUNTING Request to .GA Domain with Minimal Headers
- [x] ET HUNTING Suspicious PHP Code in HTTP POST (Outbound)
- [x] ET HUNTING Suspicious PHP Code in HTTP POST (Outbound)
- [x] ET HUNTING Redirect to Joom AG Hosted Document - Potential Phishing
- [x] ET HUNTING Suspicious HTTP POST Only Containing Password - Possible Phishing
- [x] ET HUNTING Suspicious POST to Wordpress Folder - Possible Successful Banking Phish
- [x] ET HUNTING Suspicious POST Format
- [x] ET HUNTING Suspicious Use of rzd URL Shortener Service
- [x] ET HUNTING Hidden embedded HTML Document
- [x] ET HUNTING Suspicious Glitch Hosted DNS Request - Possible Phishing Landing
- [x] ET HUNTING Observed Suspicious SSL Cert (Metasploit Self Signed CA)
- [x] ET HUNTING Possible Phishing Page - Page Saved with SingleFile Extension
- [x] ET HUNTING Generic Powershell DownloadFile Command
- [x] ET HUNTING Generic Powershell Launching Hidden Window
- [x] ET HUNTING Observed POST to xsph .ru Domain
- [x] ET HUNTING HTTP Request for OpenNIC API GeoIP Request
- [x] ET HUNTING Suspicious Netlify Hosted DNS Request - Possible Phishing Landing
- [ ] ET HUNTING Malformed Domain Name in DNS Query (Domain Length Exceeds 253 Bytes)
- [x] ET HUNTING Suspicious GET Request for .x86
- [x] ET HUNTING Possible ELF executable sent when remote host claims to send a Text File
- [x] ET HUNTING URL Shortening Service Used by Curl (ic9 .in)
- [x] ET HUNTING Possible REvil 0day Exploitation Activity Inbound
- [x] ET HUNTING Suspicious Windows Commands in POST Body (nltest)
- [x] ET HUNTING Suspicious Windows Commands in POST Body (net view)
- [x] ET HUNTING .exec in HTTP URI Inbound - Possible Exploit Activity

- [x] ET HUNTING .exec in HTTP Header Inbound - Possible Exploit Activity
- [x] ET HUNTING NOP Sled in HTTP URI Inbound - Possible Exploit Activity
- [x] ET HUNTING Base64 Encoded Windows IP Configuration Output in HTTP POST M1
- [x] ET HUNTING Base64 Encoded Windows IP Configuration Output in HTTP POST M3
- [x] ET HUNTING Suspicious Request to iplogger .org Contains Period
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Cookies/Firefox_)
- [x] ET HUNTING Observed Suspicious Request nc.exe in URI
- [x] ET HUNTING Inbound Powershell Creating .lnk File
- [x] ET HUNTING [@Silv0123] Possible Fake Microsoft Office User-Agent Observed
- [x] ET HUNTING Observed Telegram API Domain (api .telegram .org in TLS SNI)
- [ ] ET HUNTING Observed AutoDesk Domain in TLS SNI (autodesk360 .com)
- [x] ET HUNTING Suspicious Terse HTTP Request to textbin
- [x] ET HUNTING Possible UPnP UUID Overflow Exploit Attempt from Internal Host - SUBSCRIBE/UNSUBSCRIBE
- [x] ET HUNTING Possible UPnP UUID Overflow Exploit Attempt from Internal Host - NOTIFY
- [x] ET HUNTING Terse Request for .txt - Likely Hostile
- [x] ET HUNTING Suspicious GET Request (Likely Pentester CnC)
- [x] ET HUNTING Base64 Encoded ipconfig sent via HTTP POST M2
- [x] ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol TCP (CVE-2021-44228)
- [x] ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol (upper TCP Bypass) (CVE-2021-44228)
- [x] ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol (lower TCP Bypass) (CVE-2021-44228)
- [x] ET HUNTING Possible Kimsuky Related Malicious VBScript Inbound
- [x] ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol UDP (Outbound) (CVE-2021-44228)
- [x] ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol (upper UDP Bypass) (Outbound) (CVE-2021-44228)
- [x] ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol (lower UDP Bypass) (Outbound) (CVE-2021-44228)
- [x] ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol (lower UDP Bypass) (CVE-2021-44228)
- [x] ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol (upper UDP Bypass) (CVE-2021-44228)
- [x] ET HUNTING Possible NOBELIUM CnC Traffic (Observed UA)
- [x] ET HUNTING Powershell Request for paste .ee Page
- [x] ET HUNTING Double Extension ZIP File Downloaded from Discord (Request)
- [x] ET HUNTING Double Extension PIF File Downloaded from Discord (Request)
- [x] ET HUNTING Possible Apache Airflow Experimental API Authentication Bypass Attempt (CVE-2020-13927)
- [ ] ET HUNTING Multiple User-Agent Components in a single UA
- [x] ET HUNTING ZIP file exfiltration over raw TCP
- [x] ET HUNTING PE EXE Download over raw TCP
- [x] ET HUNTING ZIP file download over raw TCP
- [x] ET HUNTING Terse Request to note .youdao .com - Possible Download
- [x] ET HUNTING [TW] Likely Hex Executable String
- [ ] ET HUNTING Potential Forced OGNL Evaluation - HTTP Header
- [x] ET HUNTING Request To Suspicious Filename via Powershell (key)
- [x] ET HUNTING [TW] Likely Javascript-Obfuscator Usage Observed M1
- [x] ET HUNTING [TW] Likely Javascript-Obfuscator Usage Observed M3
- [x] ET HUNTING Observed Suspicious Reversed String Inbound (StrReverse)
- [x] ET HUNTING NOP Sled in HTTP Header Inbound - Possible Exploit Activity
- [x] ET HUNTING Screenshot Uploaded to Discord
- [x] ET HUNTING Base64 Encoded Windows IP Configuration Output in HTTP POST M2
- [x] ET HUNTING Base64 Encoded whoami in HTTP Server Response
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Chrome_Default.txt)
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (History/Firefox_)
- [x] ET HUNTING Inbound Powershell Creating .hta File
- [x] ET HUNTING DNS Lookup for 8+ hexadecimal only duckdns domain
- [x] ET HUNTING Telegram API Domain in DNS Lookup
- [x] ET HUNTING Generic Phishkit Javascript Response with Phishy Text
- [x] ET HUNTING Observed AutoDesk Domain in TLS SNI (api .autodesk .com)
- [x] ET HUNTING Possible UPnP UUID Overflow Exploit Attempt from External Host - SUBSCRIBE/UNSUBSCRIBE
- [x] ET HUNTING Possible UPnP UUID Overflow Exploit Attempt from External Host - NOTIFY
- [x] ET HUNTING curl User-Agent to Dotted Quad
- [x] ET HUNTING Suspicious Response (MS-Officecmd)
- [x] ET HUNTING Base64 Encoded ipconfig sent via HTTP POST M1
- [x] ET HUNTING Base64 Encoded ipconfig sent via HTTP POST M3
- [x] ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol UDP (CVE-2021-44228)
- [x] ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol (upper UDP Bypass) (CVE-2021-44228)
- [x] ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol (lower UDP Bypass) (CVE-2021-44228)
- [x] ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol TCP (Outbound) (CVE-2021-44228)
- [x] ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol (upper TCP Bypass) (Outbound) (CVE-2021-44228)
- [x] ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol (lower TCP Bypass) (Outbound) (CVE-2021-44228)
- [x] ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol (lower TCP Bypass) (CVE-2021-44228)
- [x] ET HUNTING Possible Apache log4j RCE Attempt - Any Protocol (upper TCP Bypass) (CVE-2021-44228)
- [ ] ET HUNTING RDP Authentication Bypass Attempt
- [x] ET HUNTING Possible cs2nginx Proxy Redirect
- [x] ET HUNTING SUSPICIOUS .LNK File Inside of Zip
- [x] ET HUNTING Double Extension VBS File Downloaded from Discord (Request)
- [x] ET HUNTING Double Extension EXE File Downloaded from Discord (Request)
- [x] ET HUNTING Observed Malicious Filename in Outbound POST Request (Information.txt)
- [x] ET HUNTING PNG image exfiltration over raw TCP
- [x] ET HUNTING RAR file exfiltration over raw TCP
- [x] ET HUNTING RAR file download over raw TCP
- [x] ET HUNTING Possible Fake Edu Host with __test Cookie
- [ ] ET HUNTING Kaspov Related Hex In HTTP Accept Header
- [ ] ET HUNTING Potential Forced OGNL Evaluation - HTTP URI
- [ ] ET HUNTING Potential Forced OGNL Evaluation - HTTP Body
- [ ] ET HUNTING Request To Suspicious Filename via Powershell (payload)
- [x] ET HUNTING [TW] Likely Javascript-Obfuscator Usage Observed M2
- [x] ET HUNTING Terse Unencrypted Request for Google - Likely Connectivity Check
- [x] ET HUNTING Observed Suspicious Reversed String Inbound (Powershell)

- [x] ET HUNTING Observed Suspicious Reversed String Inbound (Winmgmts)
- [x] ET HUNTING Possible Bot CnC Beacon (GET)
- [x] ET HUNTING [TW] Internet Computer Domain Observed
- [x] ET HUNTING [TW] Internet Computer HTTP Referer Observed
- [ ] ET HUNTING Suspicious HTTP Connection Header Observed
- [x] ET HUNTING Base64 Encoded ipconfig sent via HTTP URI M2
- [x] ET HUNTING Base64 Encoded ipconfig In Server Response M1
- [x] ET HUNTING Base64 Encoded ipconfig In Server Response M3
- [x] ET HUNTING Double Base64 Encoded ipconfig sent via HTTP URI M2
- [x] ET HUNTING Double Base64 Encoded ipconfig sent via HTTP URI M4
- [x] ET HUNTING Double Base64 Encoded ipconfig sent via HTTP URI M6
- [x] ET HUNTING Double Base64 Encoded ipconfig sent via HTTP URI M8
- [x] ET HUNTING Double Base64 Encoded ipconfig sent via HTTP Requset Body M1
- [x] ET HUNTING Double Base64 Encoded ipconfig sent via HTTP Requset Body M3
- [x] ET HUNTING Double Base64 Encoded ipconfig sent via HTTP Requset Body M5
- [x] ET HUNTING Double Base64 Encoded ipconfig sent via HTTP Requset Body M7
- [x] ET HUNTING Double Base64 Encoded ipconfig sent via HTTP Requset Body M9
- [x] ET HUNTING [TW] Uri Contains Likely Urlpages Web Hosting Technique
- [x] ET HUNTING Possible Fake Edu Host On InfinityFree Service
- [x] ET HUNTING Suspicious Domain (laurentprotector .com) in TLS SNI
- [x] ET HUNTING Possible Generic Stealer Sending a Screenshot
- [x] ET HUNTING File Sharing Related Domain in DNS Lookup (filesend .jp)
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Steam_htmlcache.txt)
- [x] ET HUNTING Microsoft Office User-Agent Requesting A Doc File
- [x] ET HUNTING Suspicious User-Agent (Mozilla/5.0_)
- [x] ET HUNTING Terse Request for WordPress Site ending in all digits
- [x] ET HUNTING HTTP GET Request XOR Key 01
- [x] ET HUNTING HTTP GET Request XOR Key 03
- [x] ET HUNTING HTTP GET Request XOR Key 05
- [x] ET HUNTING HTTP GET Request XOR Key 07
- [x] ET HUNTING HTTP GET Request XOR Key 09
- [x] ET HUNTING HTTP GET Request XOR Key 0b
- [x] ET HUNTING HTTP GET Request XOR Key 0d
- [x] ET HUNTING HTTP GET Request XOR Key 0f
- [x] ET HUNTING HTTP GET Request XOR Key 11
- [x] ET HUNTING HTTP GET Request XOR Key 13
- [x] ET HUNTING HTTP GET Request XOR Key 15
- [x] ET HUNTING HTTP GET Request XOR Key 17
- [x] ET HUNTING HTTP GET Request XOR Key 19
- [x] ET HUNTING HTTP GET Request XOR Key 1b
- [x] ET HUNTING HTTP GET Request XOR Key 1d
- [x] ET HUNTING HTTP GET Request XOR Key 1f
- [x] ET HUNTING HTTP GET Request XOR Key 21
- [x] ET HUNTING HTTP GET Request XOR Key 23
- [x] ET HUNTING HTTP GET Request XOR Key 25
- [x] ET HUNTING HTTP GET Request XOR Key 27
- [x] ET HUNTING HTTP GET Request XOR Key 29
- [x] ET HUNTING HTTP GET Request XOR Key 2b
- [x] ET HUNTING HTTP GET Request XOR Key 2d
- [x] ET HUNTING HTTP GET Request XOR Key 2f
- [x] ET HUNTING HTTP GET Request XOR Key 31
- [x] ET HUNTING HTTP GET Request XOR Key 33
- [x] ET HUNTING HTTP GET Request XOR Key 35
- [x] ET HUNTING HTTP GET Request XOR Key 37
- [x] ET HUNTING Possible Bot CnC Checkin (GET)
- [ ] ET HUNTING Suspicious SSL Certificate detected (Observed in US Government Bid Credential Phish)
- [x] ET HUNTING [TW] Internet Computer HTTP Request Observed
- [x] ET HUNTING [TW] Internet Computer HTTP Location Redirect Observed
- [x] ET HUNTING Base64 Encoded ipconfig sent via HTTP URI M1
- [x] ET HUNTING Base64 Encoded ipconfig sent via HTTP URI M3
- [x] ET HUNTING Base64 Encoded ipconfig In Server Response M2
- [x] ET HUNTING Double Base64 Encoded ipconfig sent via HTTP URI M1
- [x] ET HUNTING Double Base64 Encoded ipconfig sent via HTTP URI M3
- [x] ET HUNTING Double Base64 Encoded ipconfig sent via HTTP URI M5
- [x] ET HUNTING Double Base64 Encoded ipconfig sent via HTTP URI M7
- [x] ET HUNTING Double Base64 Encoded ipconfig sent via HTTP URI M9
- [x] ET HUNTING Double Base64 Encoded ipconfig sent via HTTP Requset Body M2
- [x] ET HUNTING Double Base64 Encoded ipconfig sent via HTTP Requset Body M4
- [x] ET HUNTING Double Base64 Encoded ipconfig sent via HTTP Requset Body M6
- [x] ET HUNTING Double Base64 Encoded ipconfig sent via HTTP Requset Body M8
- [x] ET HUNTING Possible PHP Backdoor Command Execution
- [x] ET HUNTING [TW] Page Contains Redirect to Likely Urlpages Web Hosting Technique
- [x] ET HUNTING DNS Lookup to (laurentprotector .com)
- [x] ET HUNTING Possible Generic Stealer Sending System Information
- [x] ET HUNTING File Sharing Related Domain in DNS Lookup (download .mediafire .com)
- [x] ET HUNTING Suspicious User-Agent (record)
- [x] ET HUNTING Observed TinyNuke Admin Panel URL Pattern
- [x] ET HUNTING Microsoft Office User-Agent Requesting An Excel File
- [x] ET HUNTING GET Request to Pastebin .com with PowerShell User-Agent
- [x] ET HUNTING Observed Suspicious SSL Cert (Acme Co)
- [x] ET HUNTING HTTP GET Request XOR Key 02
- [x] ET HUNTING HTTP GET Request XOR Key 04
- [x] ET HUNTING HTTP GET Request XOR Key 06
- [x] ET HUNTING HTTP GET Request XOR Key 08
- [x] ET HUNTING HTTP GET Request XOR Key 0a
- [x] ET HUNTING HTTP GET Request XOR Key 0c
- [x] ET HUNTING HTTP GET Request XOR Key 0e
- [x] ET HUNTING HTTP GET Request XOR Key 10
- [x] ET HUNTING HTTP GET Request XOR Key 12
- [x] ET HUNTING HTTP GET Request XOR Key 14
- [x] ET HUNTING HTTP GET Request XOR Key 16
- [x] ET HUNTING HTTP GET Request XOR Key 18
- [x] ET HUNTING HTTP GET Request XOR Key 1a
- [x] ET HUNTING HTTP GET Request XOR Key 1c
- [x] ET HUNTING HTTP GET Request XOR Key 1e
- [x] ET HUNTING HTTP GET Request XOR Key 20
- [x] ET HUNTING HTTP GET Request XOR Key 22
- [x] ET HUNTING HTTP GET Request XOR Key 24
- [x] ET HUNTING HTTP GET Request XOR Key 26
- [x] ET HUNTING HTTP GET Request XOR Key 28
- [x] ET HUNTING HTTP GET Request XOR Key 2a
- [x] ET HUNTING HTTP GET Request XOR Key 2c
- [x] ET HUNTING HTTP GET Request XOR Key 2e
- [x] ET HUNTING HTTP GET Request XOR Key 30
- [x] ET HUNTING HTTP GET Request XOR Key 32
- [x] ET HUNTING HTTP GET Request XOR Key 34
- [x] ET HUNTING HTTP GET Request XOR Key 36
- [x] ET HUNTING HTTP GET Request XOR Key 38

- [x] ET HUNTING HTTP GET Request XOR Key 39
- [x] ET HUNTING HTTP GET Request XOR Key 3a
- [x] ET HUNTING HTTP GET Request XOR Key 3b
- [x] ET HUNTING HTTP GET Request XOR Key 3c
- [x] ET HUNTING HTTP GET Request XOR Key 3d
- [x] ET HUNTING HTTP GET Request XOR Key 3e
- [x] ET HUNTING HTTP GET Request XOR Key 3f
- [x] ET HUNTING HTTP GET Request XOR Key 40
- [x] ET HUNTING HTTP GET Request XOR Key 41
- [x] ET HUNTING HTTP GET Request XOR Key 42
- [x] ET HUNTING HTTP GET Request XOR Key 43
- [x] ET HUNTING HTTP GET Request XOR Key 44
- [x] ET HUNTING HTTP GET Request XOR Key 45
- [x] ET HUNTING HTTP GET Request XOR Key 46
- [x] ET HUNTING HTTP GET Request XOR Key 47
- [x] ET HUNTING HTTP GET Request XOR Key 48
- [x] ET HUNTING HTTP GET Request XOR Key 49
- [x] ET HUNTING HTTP GET Request XOR Key 4a
- [x] ET HUNTING HTTP GET Request XOR Key 4b
- [x] ET HUNTING HTTP GET Request XOR Key 4c
- [x] ET HUNTING HTTP GET Request XOR Key 4d
- [x] ET HUNTING HTTP GET Request XOR Key 4e
- [x] ET HUNTING HTTP GET Request XOR Key 4f
- [x] ET HUNTING HTTP GET Request XOR Key 50
- [x] ET HUNTING HTTP GET Request XOR Key 51
- [x] ET HUNTING HTTP GET Request XOR Key 52
- [x] ET HUNTING HTTP GET Request XOR Key 53
- [x] ET HUNTING HTTP GET Request XOR Key 54
- [x] ET HUNTING HTTP GET Request XOR Key 55
- [x] ET HUNTING HTTP GET Request XOR Key 56
- [x] ET HUNTING HTTP GET Request XOR Key 57
- [x] ET HUNTING HTTP GET Request XOR Key 58
- [x] ET HUNTING HTTP GET Request XOR Key 59
- [x] ET HUNTING HTTP GET Request XOR Key 5a
- [x] ET HUNTING HTTP GET Request XOR Key 5b
- [x] ET HUNTING HTTP GET Request XOR Key 5c
- [x] ET HUNTING HTTP GET Request XOR Key 5d
- [x] ET HUNTING HTTP GET Request XOR Key 5e
- [x] ET HUNTING HTTP GET Request XOR Key 5f
- [x] ET HUNTING HTTP GET Request XOR Key 60
- [x] ET HUNTING HTTP GET Request XOR Key 61
- [x] ET HUNTING HTTP GET Request XOR Key 62
- [x] ET HUNTING HTTP GET Request XOR Key 63
- [x] ET HUNTING HTTP GET Request XOR Key 64
- [x] ET HUNTING HTTP GET Request XOR Key 65
- [x] ET HUNTING HTTP GET Request XOR Key 66
- [x] ET HUNTING HTTP GET Request XOR Key 67
- [x] ET HUNTING HTTP GET Request XOR Key 68
- [x] ET HUNTING HTTP GET Request XOR Key 69
- [x] ET HUNTING HTTP GET Request XOR Key 6a
- [x] ET HUNTING HTTP GET Request XOR Key 6b
- [x] ET HUNTING HTTP GET Request XOR Key 6c
- [x] ET HUNTING HTTP GET Request XOR Key 6d
- [x] ET HUNTING HTTP GET Request XOR Key 6e
- [x] ET HUNTING HTTP GET Request XOR Key 6f
- [x] ET HUNTING HTTP GET Request XOR Key 70
- [x] ET HUNTING HTTP GET Request XOR Key 71
- [x] ET HUNTING HTTP GET Request XOR Key 72
- [x] ET HUNTING HTTP GET Request XOR Key 73
- [x] ET HUNTING HTTP GET Request XOR Key 74
- [x] ET HUNTING HTTP GET Request XOR Key 75
- [x] ET HUNTING HTTP GET Request XOR Key 76
- [x] ET HUNTING HTTP GET Request XOR Key 77
- [x] ET HUNTING HTTP GET Request XOR Key 78
- [x] ET HUNTING HTTP GET Request XOR Key 79
- [x] ET HUNTING HTTP GET Request XOR Key 7a
- [x] ET HUNTING HTTP GET Request XOR Key 7b
- [x] ET HUNTING HTTP GET Request XOR Key 7c
- [x] ET HUNTING HTTP GET Request XOR Key 7d
- [x] ET HUNTING HTTP GET Request XOR Key 7e
- [x] ET HUNTING HTTP GET Request XOR Key 7f
- [x] ET HUNTING HTTP GET Request XOR Key 80
- [x] ET HUNTING HTTP GET Request XOR Key 81
- [x] ET HUNTING HTTP GET Request XOR Key 82
- [x] ET HUNTING HTTP GET Request XOR Key 83
- [x] ET HUNTING HTTP GET Request XOR Key 84
- [x] ET HUNTING HTTP GET Request XOR Key 85
- [x] ET HUNTING HTTP GET Request XOR Key 86
- [x] ET HUNTING HTTP GET Request XOR Key 87
- [x] ET HUNTING HTTP GET Request XOR Key 88
- [x] ET HUNTING HTTP GET Request XOR Key 89
- [x] ET HUNTING HTTP GET Request XOR Key 8a
- [x] ET HUNTING HTTP GET Request XOR Key 8b
- [x] ET HUNTING HTTP GET Request XOR Key 8c
- [x] ET HUNTING HTTP GET Request XOR Key 8d
- [x] ET HUNTING HTTP GET Request XOR Key 8e
- [x] ET HUNTING HTTP GET Request XOR Key 8f
- [x] ET HUNTING HTTP GET Request XOR Key 90
- [x] ET HUNTING HTTP GET Request XOR Key 91
- [x] ET HUNTING HTTP GET Request XOR Key 92
- [x] ET HUNTING HTTP GET Request XOR Key 93
- [x] ET HUNTING HTTP GET Request XOR Key 94
- [x] ET HUNTING HTTP GET Request XOR Key 95
- [x] ET HUNTING HTTP GET Request XOR Key 96
- [x] ET HUNTING HTTP GET Request XOR Key 97
- [x] ET HUNTING HTTP GET Request XOR Key 98
- [x] ET HUNTING HTTP GET Request XOR Key 99
- [x] ET HUNTING HTTP GET Request XOR Key 9a
- [x] ET HUNTING HTTP GET Request XOR Key 9b
- [x] ET HUNTING HTTP GET Request XOR Key 9c
- [x] ET HUNTING HTTP GET Request XOR Key 9d
- [x] ET HUNTING HTTP GET Request XOR Key 9e
- [x] ET HUNTING HTTP GET Request XOR Key 9f
- [x] ET HUNTING HTTP GET Request XOR Key a0
- [x] ET HUNTING HTTP GET Request XOR Key a1
- [x] ET HUNTING HTTP GET Request XOR Key a2
- [x] ET HUNTING HTTP GET Request XOR Key a3
- [x] ET HUNTING HTTP GET Request XOR Key a4
- [x] ET HUNTING HTTP GET Request XOR Key a5
- [x] ET HUNTING HTTP GET Request XOR Key a6
- [x] ET HUNTING HTTP GET Request XOR Key a7
- [x] ET HUNTING HTTP GET Request XOR Key a8
- [x] ET HUNTING HTTP GET Request XOR Key a9
- [x] ET HUNTING HTTP GET Request XOR Key aa
- [x] ET HUNTING HTTP GET Request XOR Key ab
- [x] ET HUNTING HTTP GET Request XOR Key ac
- [x] ET HUNTING HTTP GET Request XOR Key ad
- [x] ET HUNTING HTTP GET Request XOR Key ae
- [x] ET HUNTING HTTP GET Request XOR Key af
- [x] ET HUNTING HTTP GET Request XOR Key b0
- [x] ET HUNTING HTTP GET Request XOR Key b1
- [x] ET HUNTING HTTP GET Request XOR Key b2
- [x] ET HUNTING HTTP GET Request XOR Key b3
- [x] ET HUNTING HTTP GET Request XOR Key b4
- [x] ET HUNTING HTTP GET Request XOR Key b5
- [x] ET HUNTING HTTP GET Request XOR Key b6
- [x] ET HUNTING HTTP GET Request XOR Key b7
- [x] ET HUNTING HTTP GET Request XOR Key b8
- [x] ET HUNTING HTTP GET Request XOR Key b9
- [x] ET HUNTING HTTP GET Request XOR Key ba

- [x] ET HUNTING HTTP GET Request XOR Key bb
- [x] ET HUNTING HTTP GET Request XOR Key bc
- [x] ET HUNTING HTTP GET Request XOR Key bd
- [x] ET HUNTING HTTP GET Request XOR Key be
- [x] ET HUNTING HTTP GET Request XOR Key bf
- [x] ET HUNTING HTTP GET Request XOR Key c0
- [x] ET HUNTING HTTP GET Request XOR Key c1
- [x] ET HUNTING HTTP GET Request XOR Key c2
- [x] ET HUNTING HTTP GET Request XOR Key c3
- [x] ET HUNTING HTTP GET Request XOR Key c4
- [x] ET HUNTING HTTP GET Request XOR Key c5
- [x] ET HUNTING HTTP GET Request XOR Key c6
- [x] ET HUNTING HTTP GET Request XOR Key c7
- [x] ET HUNTING HTTP GET Request XOR Key c8
- [x] ET HUNTING HTTP GET Request XOR Key c9
- [x] ET HUNTING HTTP GET Request XOR Key ca
- [x] ET HUNTING HTTP GET Request XOR Key cb
- [x] ET HUNTING HTTP GET Request XOR Key cc
- [x] ET HUNTING HTTP GET Request XOR Key cd
- [x] ET HUNTING HTTP GET Request XOR Key ce
- [x] ET HUNTING HTTP GET Request XOR Key cf
- [x] ET HUNTING HTTP GET Request XOR Key d0
- [x] ET HUNTING HTTP GET Request XOR Key d1
- [x] ET HUNTING HTTP GET Request XOR Key d2
- [x] ET HUNTING HTTP GET Request XOR Key d3
- [x] ET HUNTING HTTP GET Request XOR Key d4
- [x] ET HUNTING HTTP GET Request XOR Key d5
- [x] ET HUNTING HTTP GET Request XOR Key d6
- [x] ET HUNTING HTTP GET Request XOR Key d7
- [x] ET HUNTING HTTP GET Request XOR Key d8
- [x] ET HUNTING HTTP GET Request XOR Key d9
- [x] ET HUNTING HTTP GET Request XOR Key da
- [x] ET HUNTING HTTP GET Request XOR Key db
- [x] ET HUNTING HTTP GET Request XOR Key dc
- [x] ET HUNTING HTTP GET Request XOR Key dd
- [x] ET HUNTING HTTP GET Request XOR Key de
- [x] ET HUNTING HTTP GET Request XOR Key df
- [x] ET HUNTING HTTP GET Request XOR Key e0
- [x] ET HUNTING HTTP GET Request XOR Key e1
- [x] ET HUNTING HTTP GET Request XOR Key e2
- [x] ET HUNTING HTTP GET Request XOR Key e3
- [x] ET HUNTING HTTP GET Request XOR Key e5
- [x] ET HUNTING HTTP GET Request XOR Key e6
- [x] ET HUNTING HTTP GET Request XOR Key e7
- [x] ET HUNTING HTTP GET Request XOR Key e8
- [x] ET HUNTING HTTP GET Request XOR Key e9
- [x] ET HUNTING HTTP GET Request XOR Key ea
- [x] ET HUNTING HTTP GET Request XOR Key eb
- [x] ET HUNTING HTTP GET Request XOR Key ec
- [x] ET HUNTING HTTP GET Request XOR Key ed
- [x] ET HUNTING HTTP GET Request XOR Key ee
- [x] ET HUNTING HTTP GET Request XOR Key ef
- [x] ET HUNTING HTTP GET Request XOR Key f0
- [x] ET HUNTING HTTP GET Request XOR Key f1
- [x] ET HUNTING HTTP GET Request XOR Key f2
- [x] ET HUNTING HTTP GET Request XOR Key f3
- [x] ET HUNTING HTTP GET Request XOR Key f4
- [x] ET HUNTING HTTP GET Request XOR Key f5
- [x] ET HUNTING HTTP GET Request XOR Key f6
- [x] ET HUNTING HTTP GET Request XOR Key f7
- [x] ET HUNTING HTTP GET Request XOR Key f8
- [x] ET HUNTING HTTP GET Request XOR Key f9
- [x] ET HUNTING HTTP GET Request XOR Key fa
- [x] ET HUNTING HTTP GET Request XOR Key fb
- [x] ET HUNTING HTTP GET Request XOR Key fc
- [x] ET HUNTING HTTP GET Request XOR Key fd
- [x] ET HUNTING HTTP GET Request XOR Key fe
- [x] ET HUNTING HTTP GET Request XOR Key ff
- [x] ET HUNTING HTTP POST Request XOR Key 01
- [x] ET HUNTING HTTP POST Request XOR Key 02
- [x] ET HUNTING HTTP POST Request XOR Key 03
- [x] ET HUNTING HTTP POST Request XOR Key 04
- [x] ET HUNTING HTTP POST Request XOR Key 05
- [x] ET HUNTING HTTP POST Request XOR Key 06
- [x] ET HUNTING HTTP POST Request XOR Key 07
- [x] ET HUNTING HTTP POST Request XOR Key 08
- [x] ET HUNTING HTTP POST Request XOR Key 09
- [x] ET HUNTING HTTP POST Request XOR Key 0a
- [x] ET HUNTING HTTP POST Request XOR Key 0b
- [x] ET HUNTING HTTP POST Request XOR Key 0c
- [x] ET HUNTING HTTP POST Request XOR Key 0d
- [x] ET HUNTING HTTP POST Request XOR Key 0e
- [x] ET HUNTING HTTP POST Request XOR Key 0f
- [x] ET HUNTING HTTP POST Request XOR Key 10
- [x] ET HUNTING HTTP POST Request XOR Key 11
- [x] ET HUNTING HTTP POST Request XOR Key 12
- [x] ET HUNTING HTTP POST Request XOR Key 13
- [x] ET HUNTING HTTP POST Request XOR Key 14
- [x] ET HUNTING HTTP POST Request XOR Key 15
- [x] ET HUNTING HTTP POST Request XOR Key 16
- [x] ET HUNTING HTTP POST Request XOR Key 17
- [x] ET HUNTING HTTP POST Request XOR Key 18
- [x] ET HUNTING HTTP POST Request XOR Key 19
- [x] ET HUNTING HTTP POST Request XOR Key 1a
- [x] ET HUNTING HTTP POST Request XOR Key 1b
- [x] ET HUNTING HTTP POST Request XOR Key 1c
- [x] ET HUNTING HTTP POST Request XOR Key 1d
- [x] ET HUNTING HTTP POST Request XOR Key 1e
- [x] ET HUNTING HTTP POST Request XOR Key 1f
- [x] ET HUNTING HTTP POST Request XOR Key 20
- [x] ET HUNTING HTTP POST Request XOR Key 21
- [x] ET HUNTING HTTP POST Request XOR Key 22
- [x] ET HUNTING HTTP POST Request XOR Key 23
- [x] ET HUNTING HTTP POST Request XOR Key 24
- [x] ET HUNTING HTTP POST Request XOR Key 25
- [x] ET HUNTING HTTP POST Request XOR Key 26
- [x] ET HUNTING HTTP POST Request XOR Key 27
- [x] ET HUNTING HTTP POST Request XOR Key 28
- [x] ET HUNTING HTTP POST Request XOR Key 29
- [x] ET HUNTING HTTP POST Request XOR Key 2a
- [x] ET HUNTING HTTP POST Request XOR Key 2b
- [x] ET HUNTING HTTP POST Request XOR Key 2c
- [x] ET HUNTING HTTP POST Request XOR Key 2d
- [x] ET HUNTING HTTP POST Request XOR Key 2e
- [x] ET HUNTING HTTP POST Request XOR Key 2f
- [x] ET HUNTING HTTP POST Request XOR Key 30
- [x] ET HUNTING HTTP POST Request XOR Key 31
- [x] ET HUNTING HTTP POST Request XOR Key 32
- [x] ET HUNTING HTTP POST Request XOR Key 33
- [x] ET HUNTING HTTP POST Request XOR Key 34
- [x] ET HUNTING HTTP POST Request XOR Key 35
- [x] ET HUNTING HTTP POST Request XOR Key 36
- [x] ET HUNTING HTTP POST Request XOR Key 37
- [x] ET HUNTING HTTP POST Request XOR Key 38
- [x] ET HUNTING HTTP POST Request XOR Key 39
- [x] ET HUNTING HTTP POST Request XOR Key 3a
- [x] ET HUNTING HTTP POST Request XOR Key 3b
- [x] ET HUNTING HTTP POST Request XOR Key 3c
- [x] ET HUNTING HTTP POST Request XOR Key 3d
- [x] ET HUNTING HTTP POST Request XOR Key 3e

- [x] ET HUNTING HTTP POST Request XOR Key 3f
- [x] ET HUNTING HTTP POST Request XOR Key 40
- [x] ET HUNTING HTTP POST Request XOR Key 41
- [x] ET HUNTING HTTP POST Request XOR Key 42
- [x] ET HUNTING HTTP POST Request XOR Key 43
- [x] ET HUNTING HTTP POST Request XOR Key 44
- [x] ET HUNTING HTTP POST Request XOR Key 45
- [x] ET HUNTING HTTP POST Request XOR Key 46
- [x] ET HUNTING HTTP POST Request XOR Key 47
- [x] ET HUNTING HTTP POST Request XOR Key 48
- [x] ET HUNTING HTTP POST Request XOR Key 49
- [x] ET HUNTING HTTP POST Request XOR Key 4a
- [x] ET HUNTING HTTP POST Request XOR Key 4b
- [x] ET HUNTING HTTP POST Request XOR Key 4c
- [x] ET HUNTING HTTP POST Request XOR Key 4d
- [x] ET HUNTING HTTP POST Request XOR Key 4e
- [x] ET HUNTING HTTP POST Request XOR Key 4f
- [x] ET HUNTING HTTP POST Request XOR Key 50
- [x] ET HUNTING HTTP POST Request XOR Key 51
- [x] ET HUNTING HTTP POST Request XOR Key 52
- [x] ET HUNTING HTTP POST Request XOR Key 53
- [x] ET HUNTING HTTP POST Request XOR Key 54
- [x] ET HUNTING HTTP POST Request XOR Key 55
- [x] ET HUNTING HTTP POST Request XOR Key 56
- [x] ET HUNTING HTTP POST Request XOR Key 57
- [x] ET HUNTING HTTP POST Request XOR Key 58
- [x] ET HUNTING HTTP POST Request XOR Key 59
- [x] ET HUNTING HTTP POST Request XOR Key 5a
- [x] ET HUNTING HTTP POST Request XOR Key 5b
- [x] ET HUNTING HTTP POST Request XOR Key 5c
- [x] ET HUNTING HTTP POST Request XOR Key 5d
- [x] ET HUNTING HTTP POST Request XOR Key 5e
- [x] ET HUNTING HTTP POST Request XOR Key 5f
- [x] ET HUNTING HTTP POST Request XOR Key 60
- [x] ET HUNTING HTTP POST Request XOR Key 61
- [x] ET HUNTING HTTP POST Request XOR Key 62
- [x] ET HUNTING HTTP POST Request XOR Key 63
- [x] ET HUNTING HTTP POST Request XOR Key 64
- [x] ET HUNTING HTTP POST Request XOR Key 65
- [x] ET HUNTING HTTP POST Request XOR Key 66
- [x] ET HUNTING HTTP POST Request XOR Key 67
- [x] ET HUNTING HTTP POST Request XOR Key 68
- [x] ET HUNTING HTTP POST Request XOR Key 69
- [x] ET HUNTING HTTP POST Request XOR Key 6a
- [x] ET HUNTING HTTP POST Request XOR Key 6b
- [x] ET HUNTING HTTP POST Request XOR Key 6c
- [x] ET HUNTING HTTP POST Request XOR Key 6d
- [x] ET HUNTING HTTP POST Request XOR Key 6e
- [x] ET HUNTING HTTP POST Request XOR Key 6f
- [x] ET HUNTING HTTP POST Request XOR Key 70
- [x] ET HUNTING HTTP POST Request XOR Key 71
- [x] ET HUNTING HTTP POST Request XOR Key 72
- [x] ET HUNTING HTTP POST Request XOR Key 73
- [x] ET HUNTING HTTP POST Request XOR Key 74
- [x] ET HUNTING HTTP POST Request XOR Key 75
- [x] ET HUNTING HTTP POST Request XOR Key 76
- [x] ET HUNTING HTTP POST Request XOR Key 77
- [x] ET HUNTING HTTP POST Request XOR Key 78
- [x] ET HUNTING HTTP POST Request XOR Key 79
- [x] ET HUNTING HTTP POST Request XOR Key 7a
- [x] ET HUNTING HTTP POST Request XOR Key 7b
- [x] ET HUNTING HTTP POST Request XOR Key 7c
- [x] ET HUNTING HTTP POST Request XOR Key 7d
- [x] ET HUNTING HTTP POST Request XOR Key 7e
- [x] ET HUNTING HTTP POST Request XOR Key 7f
- [x] ET HUNTING HTTP POST Request XOR Key 80
- [x] ET HUNTING HTTP POST Request XOR Key 81
- [x] ET HUNTING HTTP POST Request XOR Key 82
- [x] ET HUNTING HTTP POST Request XOR Key 83
- [x] ET HUNTING HTTP POST Request XOR Key 84
- [x] ET HUNTING HTTP POST Request XOR Key 85
- [x] ET HUNTING HTTP POST Request XOR Key 86
- [x] ET HUNTING HTTP POST Request XOR Key 87
- [x] ET HUNTING HTTP POST Request XOR Key 88
- [x] ET HUNTING HTTP POST Request XOR Key 89
- [x] ET HUNTING HTTP POST Request XOR Key 8a
- [x] ET HUNTING HTTP POST Request XOR Key 8b
- [x] ET HUNTING HTTP POST Request XOR Key 8c
- [x] ET HUNTING HTTP POST Request XOR Key 8d
- [x] ET HUNTING HTTP POST Request XOR Key 8e
- [x] ET HUNTING HTTP POST Request XOR Key 8f
- [x] ET HUNTING HTTP POST Request XOR Key 90
- [x] ET HUNTING HTTP POST Request XOR Key 91
- [x] ET HUNTING HTTP POST Request XOR Key 92
- [x] ET HUNTING HTTP POST Request XOR Key 93
- [x] ET HUNTING HTTP POST Request XOR Key 94
- [x] ET HUNTING HTTP POST Request XOR Key 95
- [x] ET HUNTING HTTP POST Request XOR Key 96
- [x] ET HUNTING HTTP POST Request XOR Key 97
- [x] ET HUNTING HTTP POST Request XOR Key 98
- [x] ET HUNTING HTTP POST Request XOR Key 99
- [x] ET HUNTING HTTP POST Request XOR Key 9a
- [x] ET HUNTING HTTP POST Request XOR Key 9b
- [x] ET HUNTING HTTP POST Request XOR Key 9c
- [x] ET HUNTING HTTP POST Request XOR Key 9d
- [x] ET HUNTING HTTP POST Request XOR Key 9e
- [x] ET HUNTING HTTP POST Request XOR Key 9f
- [x] ET HUNTING HTTP POST Request XOR Key a0
- [x] ET HUNTING HTTP POST Request XOR Key a1
- [x] ET HUNTING HTTP POST Request XOR Key a2
- [x] ET HUNTING HTTP POST Request XOR Key a3
- [x] ET HUNTING HTTP POST Request XOR Key a4
- [x] ET HUNTING HTTP POST Request XOR Key a5
- [x] ET HUNTING HTTP POST Request XOR Key a6
- [x] ET HUNTING HTTP POST Request XOR Key a7
- [x] ET HUNTING HTTP POST Request XOR Key a8
- [x] ET HUNTING HTTP POST Request XOR Key a9
- [x] ET HUNTING HTTP POST Request XOR Key aa
- [x] ET HUNTING HTTP POST Request XOR Key ab
- [x] ET HUNTING HTTP POST Request XOR Key ac
- [x] ET HUNTING HTTP POST Request XOR Key ad
- [x] ET HUNTING HTTP POST Request XOR Key ae
- [x] ET HUNTING HTTP POST Request XOR Key af
- [x] ET HUNTING HTTP POST Request XOR Key b0
- [x] ET HUNTING HTTP POST Request XOR Key b1
- [x] ET HUNTING HTTP POST Request XOR Key b2
- [x] ET HUNTING HTTP POST Request XOR Key b3
- [x] ET HUNTING HTTP POST Request XOR Key b4
- [x] ET HUNTING HTTP POST Request XOR Key b5
- [x] ET HUNTING HTTP POST Request XOR Key b6
- [x] ET HUNTING HTTP POST Request XOR Key b7
- [x] ET HUNTING HTTP POST Request XOR Key b8
- [x] ET HUNTING HTTP POST Request XOR Key b9
- [x] ET HUNTING HTTP POST Request XOR Key ba
- [x] ET HUNTING HTTP POST Request XOR Key bb
- [x] ET HUNTING HTTP POST Request XOR Key bc
- [x] ET HUNTING HTTP POST Request XOR Key bd
- [x] ET HUNTING HTTP POST Request XOR Key be
- [x] ET HUNTING HTTP POST Request XOR Key bf
- [x] ET HUNTING HTTP POST Request XOR Key c0

- [x] ET HUNTING HTTP POST Request XOR Key c1
- [x] ET HUNTING HTTP POST Request XOR Key c2
- [x] ET HUNTING HTTP POST Request XOR Key c3
- [x] ET HUNTING HTTP POST Request XOR Key c4
- [x] ET HUNTING HTTP POST Request XOR Key c5
- [x] ET HUNTING HTTP POST Request XOR Key c6
- [x] ET HUNTING HTTP POST Request XOR Key c7
- [x] ET HUNTING HTTP POST Request XOR Key c8
- [x] ET HUNTING HTTP POST Request XOR Key c9
- [x] ET HUNTING HTTP POST Request XOR Key ca
- [x] ET HUNTING HTTP POST Request XOR Key cb
- [x] ET HUNTING HTTP POST Request XOR Key cc
- [x] ET HUNTING HTTP POST Request XOR Key cd
- [x] ET HUNTING HTTP POST Request XOR Key ce
- [x] ET HUNTING HTTP POST Request XOR Key cf
- [x] ET HUNTING HTTP POST Request XOR Key d0
- [x] ET HUNTING HTTP POST Request XOR Key d1
- [x] ET HUNTING HTTP POST Request XOR Key d2
- [x] ET HUNTING HTTP POST Request XOR Key d3
- [x] ET HUNTING HTTP POST Request XOR Key d4
- [x] ET HUNTING HTTP POST Request XOR Key d5
- [x] ET HUNTING HTTP POST Request XOR Key d6
- [x] ET HUNTING HTTP POST Request XOR Key d7
- [x] ET HUNTING HTTP POST Request XOR Key d8
- [x] ET HUNTING HTTP POST Request XOR Key d9
- [x] ET HUNTING HTTP POST Request XOR Key da
- [x] ET HUNTING HTTP POST Request XOR Key db
- [x] ET HUNTING HTTP POST Request XOR Key dc
- [x] ET HUNTING HTTP POST Request XOR Key dd
- [x] ET HUNTING HTTP POST Request XOR Key de
- [x] ET HUNTING HTTP POST Request XOR Key df
- [x] ET HUNTING HTTP POST Request XOR Key e0
- [x] ET HUNTING HTTP POST Request XOR Key e1
- [x] ET HUNTING HTTP POST Request XOR Key e2
- [x] ET HUNTING HTTP POST Request XOR Key e3
- [x] ET HUNTING HTTP POST Request XOR Key e4
- [x] ET HUNTING HTTP POST Request XOR Key e5
- [x] ET HUNTING HTTP POST Request XOR Key e6
- [x] ET HUNTING HTTP POST Request XOR Key e7
- [x] ET HUNTING HTTP POST Request XOR Key e8
- [x] ET HUNTING HTTP POST Request XOR Key e9
- [x] ET HUNTING HTTP POST Request XOR Key ea
- [x] ET HUNTING HTTP POST Request XOR Key eb
- [x] ET HUNTING HTTP POST Request XOR Key ec
- [x] ET HUNTING HTTP POST Request XOR Key ed
- [x] ET HUNTING HTTP POST Request XOR Key ee
- [x] ET HUNTING HTTP POST Request XOR Key ef
- [x] ET HUNTING HTTP POST Request XOR Key f0
- [x] ET HUNTING HTTP POST Request XOR Key f1
- [x] ET HUNTING HTTP POST Request XOR Key f2
- [x] ET HUNTING HTTP POST Request XOR Key f3
- [x] ET HUNTING HTTP POST Request XOR Key f4
- [x] ET HUNTING HTTP POST Request XOR Key f5
- [x] ET HUNTING HTTP POST Request XOR Key f6
- [x] ET HUNTING HTTP POST Request XOR Key f7
- [x] ET HUNTING HTTP POST Request XOR Key f8
- [x] ET HUNTING HTTP POST Request XOR Key f9
- [x] ET HUNTING HTTP POST Request XOR Key fa
- [x] ET HUNTING HTTP POST Request XOR Key fb
- [x] ET HUNTING HTTP POST Request XOR Key fc
- [x] ET HUNTING HTTP POST Request XOR Key fd
- [x] ET HUNTING HTTP POST Request XOR Key fe
- [x] ET HUNTING HTTP POST Request XOR Key ff
- [x] ET HUNTING HTTP GET Request XOR e4
- [x] ET HUNTING Possible Fake 404 Credential Phish Landing Page
- [x] ET HUNTING Possible Obfuscator io JavaScript Obfuscation
- [x] ET HUNTING Outbound POST Request with Zipped Directory Traversal Filename
- [x] ET HUNTING Possible Obfuscator io JavaScript Obfuscation Exclusion
- [x] ET HUNTING Suspicious GET Request for .arc File
- [x] ET HUNTING Suspicious GET Request for .i468 File
- [x] ET HUNTING Suspicious GET Request for .i686 File
- [x] ET HUNTING Suspicious GET Request for .mspl File
- [x] ET HUNTING Suspicious GET Request for .arm file File
- [x] ET HUNTING Suspicious GET Request for .ppc File
- [x] ET HUNTING Suspicious GET Request for .spc File
- [x] ET HUNTING Suspicious GET Request for .sh4 File
- [x] ET HUNTING Downloaded Powershell Script Detects AV Product
- [x] ET HUNTING Go-http-client POSTing IP Address and Username
- [x] ET HUNTING Suspicious Windows Installer UA for non-MSI
- [x] ET HUNTING Office UA Retrieving Content on Unusually High Port
- [x] ET HUNTING Windows Commands and Variables in DNS Reply
- [x] ET HUNTING PNG in HTTP POST (Outbound)
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Histories Google Chrome.txt) M1
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Histories Google Chrome.txt) M2
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Histories Firefox.txt) M1
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Histories Firefox.txt) M2
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Bookmarks Firefox.txt) M1
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Bookmarks Firefox.txt) M2
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Cookies Firefox.txt) M1
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Cookies Firefox.txt) M2
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Information.html) M1
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (Information.html) M2
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (ProcessInfo_Log.txt) M2
- [x] ET HUNTING Suspicious Zipped Filename in Outbound POST Request (ProcessInfo_Log.txt) M1
- [x] ET HUNTING 7-zip Executable Requested (GET)
- [x] ET HUNTING Redirect Link in TikTok URL
- [x] ET HUNTING Powershell Get-ComputerInfo Output (WindowsBuildLabEx) - Decimal Encoded
- [x] ET HUNTING Microsoft Powershell Banner Output - Decimal Encoded
- [x] ET HUNTING Microsoft cmd.exe Banner Output - Decimal Encoded
- [x] ET HUNTING Chrome/0 in User-Agent
- [x] ET HUNTING Suspicious Office Template Style Request (GET)
- [x] ET HUNTING RedditSharp UA in POST (POST)
- [x] ET HUNTING Suspicious Empty Accept-Encoding Header
- [x] ET HUNTING File Sharing Related Domain (www .mediafire .com) in DNS Lookup
- [x] ET HUNTING DDoS-Guard Hosted Content
- [x] ET HUNTING Observed Nighthawk 404 Server Response
- [x] ET HUNTING Terse Request for Zip File (GET)
- [ ] ET HUNTING Observed Query to .fyi TLD
- [x] ET HUNTING Observed Query to .beauty TLD
- [ ] ET HUNTING Observed Meterpreter Style Request (GET)
- [x] ET HUNTING HTTP GET Request for sqlite3.dll - Possible Infostealer Activity
- [x] ET HUNTING HTTP GET Request for mozglue.dll - Possible Infostealer Activity

- [x] ET HUNTING HTTP GET Request for freebl3.dll - Possible Infostealer Activity
- [x] ET HUNTING HTTP GET Request for msvcp40.dll - Possible Infostealer Activity
- [x] ET HUNTING HTTP GET Request for nss3.dll - Possible Infostealer Activity
- [x] ET HUNTING HTTP GET Request for softokn3.dll - Possible Infostealer Activity
- [x] ET HUNTING HTTP GET Request for vcruntime140.dll - Possible Infostealer Activity
- [x] ET HUNTING User-Agent with Non Standard Characters
- [x] ET HUNTING Likely Hex Encoded Executable as String - Pipe Separated
- [x] ET HUNTING Likely Hex Encoded Executable as String - Dash Separated
- [x] ET HUNTING Likely Hex Encoded Executable as String - Octothorp Separated
- [x] ET HUNTING Likely Hex Encoded Executable as String - Percent Separated
- [x] ET HUNTING Likely Hex Encoded Executable as String - Double Quote Separated
- [x] ET HUNTING Likely Hex Encoded Executable as String - Single Quote Separated
- [x] ET HUNTING Likely Hex Encoded Executable as String - Tilde Separated
- [x] ET HUNTING Likely Hex Encoded Executable as String - Backtick Separated
- [x] ET HUNTING Likely Hex Encoded Executable as String - Comma Separated
- [ ] ET HUNTING robots Request (set)
- [ ] ET HUNTING robots Request Returning Base64 (Inbound)
- [x] ET HUNTING Curl User-Agent Observed to Telegram
- [x] ET HUNTING Possible Telegram Proxy Site (sendMessage)
- [x] ET HUNTING Possible Telegram Proxy Site (sendDocument)
- [x] ET HUNTING Possible Telegram Proxy Site (getUpdates)
- [x] ET HUNTING HTA Download with PowerShell User-Agent
- [x] ET HUNTING Whoami Command Inbound On High Port
- [x] ET HUNTING PowerShell Command Prompt Outbound On High Port
- [x] ET HUNTING Connectivity Check With Go User-Agent
- [x] ET HUNTING HTTP GET Request for system.data.sqlite.dll - Possible Infostealer Activity
- [x] ET HUNTING HTTP GET Request for newtonsoft.json.dll - Possible Infostealer Activity
- [x] ET HUNTING HTTP GET Request for bouncycastle.crypto.dll - Possible Infostealer Activity
- [x] ET HUNTING HTTP GET Request for sqlite.interop.dll - Possible Infostealer Activity
- [x] ET HUNTING HTTP GET Request for dotnetzip.dll - Possible Infostealer Activity
- [x] ET HUNTING Possible Racoon Stealer Retrieving Google Account Details (GET)
- [x] ET HUNTING Terse DoH Style Query (GET)
- [x] ET HUNTING Gamaredon APT Style jpeg Request (GET)
- [ ] ET HUNTING Gamaredon APT Style Request (GET)
- [x] ET HUNTING Observed DNS Query to autoitscript .com
- [x] ET HUNTING Observed Domain (autoitscript .com) in TLS SNI
- [x] ET HUNTING IPFS Gateway Domain in DNS Lookup (ipfs .w3s .link)
- [x] ET HUNTING IPFS Gateway Domain in DNS Lookup (ipfs .dweb .link)
- [x] ET HUNTING IPFS Gateway Domain in DNS Lookup (gateway .pinata .cloud)
- [x] ET HUNTING Observed IPFS Gateway Domain (ipfs .w3s .link) in TLS SNI
- [x] ET HUNTING Observed IPFS Gateway Domain (ipfs .dweb .link) in TLS SNI
- [x] ET HUNTING Observed IPFS Gateway Domain (gateway .pinata .cloud) in TLS SNI
- [x] ET HUNTING HTTP Request to transfer .sh via Powershell
- [x] ET HUNTING Office User-Agent Requesting Non-Standard Filename
- [x] ET HUNTING HTTP GET Request for PSSQLite.zip - Possible Infostealer Activity
- [x] ET HUNTING Telegram API Request (GET)
- [x] ET HUNTING Possible Snake Header in HTTP Request
- [x] ET HUNTING Possible Successful Generic Phish to webwave .dev Domain 2023-05-24
- [x] ET HUNTING Rejetto HTTP File Sever Response
- [ ] ET HUNTING V8 JavaScript Engine JIT Forcing Observed - Investigate Possible Exploitation M2
- [x] ET HUNTING DropBox User Content Download for payload.bin
- [x] ET HUNTING Possible Node.js REPL Shell Banner - Reverse Shell
- [x] ET HUNTING Possible Node.js REPL Shell Banner - Bind Shell
- [x] ET HUNTING Upload to Links-Server File Sharing Server
- [x] ET HUNTING Possible WikiLoader Activity (GET)
- [x] ET HUNTING Veeam Credential Recovery Script Inbound
- [x] ET HUNTING [ANY.RUN] DARKCLOUD Style External IP Check
- [x] ET HUNTING Redirect via HTTP 300 to URI Shortening Service (rb .gy)
- [x] ET HUNTING Redirect via HTTP 300 to URI Shortening Service (rb .gy) with Fragment Identifier
- [x] ET HUNTING Redirect via HTTP 300 to URI Shortening Service (sprl .in)
- [x] ET HUNTING Redirect via HTTP 300 to URI Shortening Service (alturl .com)
- [x] ET HUNTING WebDAV Retrieving .exe
- [x] ET HUNTING WebDAV Retrieving .dll
- [x] ET HUNTING Base64 Encoded RAR File in HTML Body (Magic Bytes)
- [x] ET HUNTING Base64 Encoded zip-compressed File in HTML Body (Mime Type)
- [x] ET HUNTING Base64 Encoded ISO File in HTML Body (Magic Bytes)
- [x] ET HUNTING Base64 Encoded RAR Compressed File in HTML Body (Mime Type)
- [x] ET HUNTING Base64 Encoded octet-stream File in HTML Body (Mime Type)
- [x] ET HUNTING Base64 Encoded Null Byte Padded File in HTML Body (Magic Bytes)
- [x] ET HUNTING Suspected Gamaredon Template Retrieval
- [x] ET HUNTING MacOS Process List in HTTP POST Request (/sbin/launchd) M1
- [x] ET HUNTING MacOS Process List in HTTP POST Request (/sbin/launchd) M2
- [x] ET HUNTING Suspicious Cisco Privilege Level 15 in HTTP Header (Inbound)
- [x] ET HUNTING Suspicious Cisco Privilege Level 15 in HTTP Header (Outbound)
- [x] ET HUNTING Cisco IOS XE Web Server Auth From Suspicious Username (cisco_tac_admin) (CVE-2023-20198) (Inbound)
- [x] ET HUNTING Cisco IOS XE Web Server Auth From Suspicious Username (cisco_tac_admin) (CVE-2023-20198) (Outbound)
- [x] ET HUNTING HTTP GET Request for AutoItX3
- [x] ET HUNTING curl UA Querying External IP (geoplugin .net)
- [x] ET HUNTING Suspicious HTTP Server Value in Response (Apache Coyote)
- [x] ET HUNTING Suspicious HTTP Server Value in Response (Apache \r\n)
- [x] ET HUNTING Suspicious HTTP Server Value in Response (Apache.)
- [x] ET HUNTING Suspicious HTTP Server Value in Response (CloudFlare)
- [x] ET HUNTING Suspicious HTTP Header in Response (Expired:)
- [x] ET HUNTING Suspicious HTTP Server Value in Response (ngengx)

- [x] ET HUNTING Suspicious HTTP Server Value in Response (Apache64)
- [x] ET HUNTING Suspicious HTTP Server Value in Response (Microsoft - IIS)
- [x] ET HUNTING Redirect to Discord Attachment Download
- [x] ET HUNTING Suspected Malicious Powershell Script (Inbound)
- [x] ET HUNTING 302 Redirect to run .mocky .io
- [x] ET HUNTING Successful PROPFIND Response for Application Media Type
- [x] ET HUNTING WebDAV Retrieving .zip containing .exe
- [x] ET HUNTING WebDAV Retrieving .zip
- [x] ET HUNTING curl in DNS TXT Response
- [x] ET HUNTING wget in DNS TXT Response
- [x] ET HUNTING PDF extension in DNS TXT Response
- [x] ET HUNTING EXE extension in DNS TXT Response
- [x] ET HUNTING vibe.d Library User-Agent
- [x] ET HUNTING Query to IP Check Tool With Minimal Headers (ip .tool .chinaz .com
- [x] ET HUNTING bmp File Request Returning Encoded File
- [x] ET HUNTING Suspicious Request for bd.log
- [x] ET HUNTING Suspicious Request for fs.log
- [x] ET HUNTING External SMB ANDX Request for Outlook Calendar Invite File (.ics) - Possible NTLM Hash Leak Attempt
- [x] ET HUNTING Googlebot User-Agent Observed in Outbound HTTP Request
- [x] ET HUNTING Redirect to Wikipedia with Hackernoon GIF
- [x] ET HUNTING - DNS Response containing multiple DNSSEC RRSIG Entries (Algorithm 14) - Possible CVE-2023-50387 Activity
- [x] ET HUNTING Suspected Andariel/TA430 Related Domain in TLS SNI
- [x] ET HUNTING Suspected Andariel/TA430 Related Domain in TLS SNI

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

- [ ] GPL ICMP undefined code
- [ ] GPL ICMP PING undefined code
- [ ] GPL ICMP Address Mask Reply undefined code
- [ ] GPL ICMP Address Mask Request undefined code
- [ ] GPL ICMP Alternate Host Address undefined code
- [ ] GPL ICMP Datagram Conversion Error
- [ ] GPL ICMP Datagram Conversion Error undefined code
- [ ] GPL ICMP Destination Unreachable undefined code
- [ ] GPL ICMP Echo Reply undefined code
- [ ] GPL ICMP IPV6 I-Am-Here undefined code
- [ ] GPL ICMP IPV6 Where-Are-You undefined code
- [ ] GPL ICMP Information Reply undefined code
- [ ] GPL ICMP Information Request undefined code
- [ ] GPL ICMP Mobile Host Redirect undefined code
- [ ] GPL ICMP Mobile Registration Reply undefined code
- [ ] GPL ICMP Mobile Registration Request undefined code
- [ ] GPL ICMP Parameter Problem Bad Length
- [ ] GPL ICMP Parameter Problem Missing a Required Option
- [ ] GPL ICMP Parameter Problem Unspecified Error
- [ ] GPL ICMP Parameter Problem undefined Code
- [ ] GPL ICMP Photuris Reserved
- [ ] GPL ICMP Photuris Unknown Security Parameters Index
- [ ] GPL ICMP Photuris Valid Security Parameters, But Authentication Failed
- [ ] GPL ICMP Photuris Valid Security Parameters, But Decryption Failed
- [ ] GPL ICMP Photuris undefined code!
- [ ] GPL ICMP Redirect undefined code
- [ ] GPL ICMP Reserved for Security Type 19
- [ ] GPL ICMP Reserved for Security Type 19 undefined code
- [ ] GPL ICMP SKIP undefined code
- [ ] GPL ICMP Source Quench undefined code
- [ ] GPL ICMP Time-To-Live Exceeded in Transit undefined code
- [ ] GPL ICMP Timestamp Reply undefined code
- [ ] GPL ICMP Timestamp Request undefined code
- [ ] GPL ICMP Traceroute undefined code
- [ ] GPL ICMP unassigned type 1 undefined code
- [ ] GPL ICMP unassigned type 2 undefined code
- [ ] GPL ICMP unassigned type 7 undefined code
- [ ] GPL ICMP L3retriever Ping
- [ ] GPL ICMP Large ICMP Packet

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

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

- [x] GPL IMAP Overflow Attempt
- [ ] GPL IMAP partial body buffer overflow attempt
- [x] GPL IMAP EXPLOIT partial body overflow attempt
- [x] GPL IMAP login buffer overflow attempt
- [x] GPL IMAP authenticate overflow attempt
- [ ] GPL IMAP list literal overflow attempt
- [ ] GPL IMAP lsub literal overflow attempt
- [x] GPL IMAP rename overflow attempt
- [x] GPL IMAP find overflow attempt
- [ ] GPL IMAP login literal buffer overflow attempt
- [ ] GPL IMAP partial body.peek buffer overflow attempt
- [ ] GPL IMAP authenticate literal overflow attempt
- [ ] GPL IMAP lsub overflow attempt
- [ ] GPL IMAP create buffer overflow attempt
- [ ] GPL IMAP list overflow attempt
- [ ] GPL IMAP rename literal overflow attempt
- [ ] GPL IMAP create literal buffer overflow attempt
- [x] GPL IMAP auth overflow attempt
- [ ] GPL IMAP login literal format string attempt
- [x] GPL IMAP delete overflow attempt
- [ ] GPL IMAP delete literal overflow attempt
- [x] GPL IMAP copy literal overflow attempt
- [x] GPL IMAP append overflow attempt
- [ ] GPL IMAP examine literal overflow attempt
- [x] GPL IMAP examine overflow attempt
- [ ] GPL IMAP fetch literal overflow attempt
- [x] GPL IMAP fetch overflow attempt
- [ ] GPL IMAP status literal overflow attempt
- [x] GPL IMAP status overflow attempt
- [x] GPL IMAP subscribe literal overflow attempt
- [x] GPL IMAP subscribe overflow attempt
- [x] GPL IMAP unsubscribe literal overflow attempt
- [x] GPL IMAP unsubscribe overflow attempt

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

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

- [x] **emerging-ja3.rules** Hide

- [x] ET JA3 Hash - Metaploit http scanner (tested: 4.11.5 Kali)
- [x] ET JA3 Hash - Metasploit CCS Scanner
- [x] ET JA3 Hash - Metasploit HeartBleed Scanner
- [x] ET JA3 Hash - Metasploit SSL Scanner
- [x] ET JA3 Hash - mitmproxy
- [x] ET JA3 Hash - mitmproxy
- [x] ET JA3 Hash - Nikto (tested 2.1.6 - Kali)
- [x] ET JA3 Hash - Nikto (tested 2.1.6 - Kali)

☑ ET JA3 Hash - Nikto (tested v2.1.6)
☑ ET JA3 Hash - Possible Malware - AnglerEK
☑ ET JA3 Hash - Possible Malware - Boleto Malspam
☑ ET JA3 Hash - Possible Malware - Dridex
☑ ET JA3 Hash - Possible Malware - Eitest/AnglerEK
☑ ET JA3 Hash - Possible Malware - Fake Firefox Font Update
☑ ET JA3 Hash - Possible Malware - FiestaEK
☑ ET JA3 Hash - Possible Malware - Gootkit
☑ ET JA3 Hash - Possible Malware - Malspam
☑ ET JA3 Hash - Possible Malware - Neutrino
☐ ET JA3 Hash - Possible Malware - Neutrino
☑ ET JA3 Hash - Possible Malware - Neutrino
☑ ET JA3 Hash - Possible Malware - NuclearEK
☑ ET JA3 Hash - Possible Malware - RigEK
☑ ET JA3 Hash - Possible Malware - TBot / Skynet Tor Botnet
☐ ET JA3 Hash - Possible Malware - Unknown traffic associated with Dridex
☑ ET JA3 Hash - Possible Malware - USPS Malspam
☐ ET JA3 Hash - Possible Malware - Various Eitest
☑ ET JA3 Hash - Possible Malware - Various Malspam/RigEK
☑ ET JA3 Hash - Possible Malware - Various RigEK/Cryptowall/Dridex
☑ ET JA3 Hash - Possible Superfish
☑ ET JA3 Hash - sqlmap (tested: v1.0-dev kali)
☑ ET JA3 Hash - WPScan (tested: 2.9 Kali)
☑ ET JA3 Hash - [Abuse.ch] Possible Quakbot
☑ ET JA3 Hash - [Abuse.ch] Possible Troldesh Ransomware
☑ ET JA3 Hash - [Abuse.ch] Possible Trickbot
☑ ET JA3 Hash - [Abuse.ch] Possible Dridex
☑ ET JA3 Hash - [Abuse.ch] Possible Adware
☑ ET JA3 Hash - [Abuse.ch] Possible Dridex
☑ ET JA3 Hash - [Abuse.ch] Possible Adware
☑ ET JA3 Hash - [Abuse.ch] Possible Adware
☑ ET JA3 Hash - [Abuse.ch] Possible Adware
☑ ET JA3 Hash - [Abuse.ch] Possible Adware
☑ ET JA3 Hash - [Abuse.ch] Possible Adware
☑ ET JA3 Hash - [Abuse.ch] Possible Adware
☑ ET JA3 Hash - [Abuse.ch] Possible Adware
☑ ET JA3 Hash - [Abuse.ch] Possible Adware
☑ ET JA3 Hash - [Abuse.ch] Possible Adware
☑ ET JA3 Hash - [Abuse.ch] Possible Adware
☑ ET JA3 Hash - [Abuse.ch] Possible Adware
☑ ET JA3 Hash - [Abuse.ch] Possible Adware
☑ ET JA3 Hash - [Abuse.ch] Possible Gozi
☑ ET JA3 Hash - [Abuse.ch] Possible Gozi
☑ ET JA3 Hash - Suspected Meterpreter Reverse Shell M2 (set)
☑ ET JA3 Hash - Trojan.AndroidOS.Jocker.snt 1
☐ ET JA3 HASH - Possible POSHC2 Client CnC
☑ ET JA3 HASH - Possible InnocenceBot CnC
☑ ET JA3 HASH - Possible RustyBuer Server Response
☑ ET JA3 HASH - Possible Rclone Client Response (Mega Storage)
☑ ET JA3 HASH - Possible Nessus Client
☑ ET JA3 HASH - Possible Cobalt Strike Server
☑ ET JA3 HASH - Possible AnchorMail CnC Traffic
☑ ET JA3 HASH - DeimosC2 Agent Activity (set)

☑ ET JA3 Hash - Possible Malware - AnglerEK
☑ ET JA3 Hash - Possible Malware - Boleto Malspam
☑ ET JA3 Hash - Possible Malware - Dridex
☑ ET JA3 Hash - Possible Malware - Eitest Chrome Popup
☑ ET JA3 Hash - Possible Malware - Fake Firefox Font Update
☐ ET JA3 Hash - Possible Malware - Fake Firefox Font Update
☑ ET JA3 Hash - Possible Malware - Gootkit
☐ ET JA3 Hash - Possible Malware - Java Based RAT
☑ ET JA3 Hash - Possible Malware - Malspam
☑ ET JA3 Hash - Possible Malware - Neutrino
☑ ET JA3 Hash - Possible Malware - Neutrino
☑ ET JA3 Hash - Possible Malware - Neutrino
☑ ET JA3 Hash - Possible Malware - RigEK
☑ ET JA3 Hash - Possible Malware - Various Malfams
☑ ET JA3 Hash - Possible Malware - Trickbot
☑ ET JA3 Hash - Possible Malware - USPS Malspam
☑ ET JA3 Hash - Possible Malware - USPS Malspam
☑ ET JA3 Hash - Possible Malware - Various EK
☑ ET JA3 Hash - Possible Malware - Various Malspam/RigEK/Dreambot
☑ ET JA3 Hash - Possible Superfish
☑ ET JA3 Hash - Rapid7 Nexpose
☑ ET JA3 Hash - sqlmap (tested: v1.0.7.0 OS X)
☑ ET JA3 Hash - [Abuse.ch] Possible Trickbot
☑ ET JA3 Hash - [Abuse.ch] Possible Quakbot
☑ ET JA3 Hash - [Abuse.ch] Possible Gootkit
☑ ET JA3 Hash - [Abuse.ch] Possible Adwind
☑ ET JA3 Hash - [Abuse.ch] Possible Dridex
☑ ET JA3 Hash - [Abuse.ch] Possible Adware
☑ ET JA3 Hash - [Abuse.ch] Possible Adware
☑ ET JA3 Hash - [Abuse.ch] Possible Adware
☑ ET JA3 Hash - [Abuse.ch] Possible Adware
☑ ET JA3 Hash - [Abuse.ch] Possible Adware
☑ ET JA3 Hash - [Abuse.ch] Possible Adware
☑ ET JA3 Hash - [Abuse.ch] Possible Torrentlocker
☑ ET JA3 Hash - [Abuse.ch] Possible Trickbot
☑ ET JA3 Hash - [Abuse.ch] Possible Adware
☑ ET JA3 Hash - [Abuse.ch] Possible Adware
☑ ET JA3 Hash - [Abuse.ch] Possible Dridex
☑ ET JA3 Hash - [Abuse.ch] Possible Adware
☑ ET JA3 Hash - [Abuse.ch] Possible Adware
☑ ET JA3 Hash - [Abuse.ch] Possible Ransomware
☑ ET JA3 Hash - [Abuse.ch] Possible Trickbot
☑ ET JA3 Hash - Suspected Meterpreter Reverse Shell M1 (set)
☑ ET JA3 Hash - Suspected Cobalt Strike Malleable C2 M1 (set)
☑ ET JA3 HASH - Possible BAZAR Backdoor CnC
☐ ET JA3 HASH - Possible POSHC2 Server Response
☑ ET JA3 HASH - Possible RustyBuer Client Activity
☑ ET JA3 HASH - Possible Rclone Client Activity
☑ ET JA3 HASH - Possible Rclone Client Response (Mega Storage)
☑ ET JA3 HASH - Possible Cobalt Strike Server
☑ ET JA3 HASH - Possible Cobalt Strike Server
☑ ET JA3 Hash - Remcos 3.x TLS Connection
☑ ET JA3 HASH - DeimosC2 Agent Activity

☑ **emerging-malware.rules** Hide

☑ ET MALWARE IRC Private message on non-standard port
☑ ET MALWARE IRC Channel join on non-standard port
☐ ET MALWARE UPX compressed file download possible malware
☐ ET MALWARE Likely Spambot Web-based Control Traffic
☐ ET MALWARE Bugbear@MM virus via SMTP
☐ ET MALWARE PWS Banker Trojan Sending Report of Infection
☑ ET MALWARE IRC Potential bot scan/exploit command
☐ ET MALWARE IRC Potential DDoS command 1
☐ ET MALWARE Srv.SSA-KeyLogger Checkin Traffic

☑ ET MALWARE IRC DCC chat request on non-standard port
☑ ET MALWARE IRC DNS request on non-standard port
☐ ET MALWARE IE Ilookup Trojan
☐ ET MALWARE HackerDefender Root Kit Remote Connection Attempt Detected
☐ ET MALWARE Possible Bobax trojan infection
☑ ET MALWARE IRC Channel topic scan/exploit command
☐ ET MALWARE IRC Potential bot update/download via http command
☐ ET MALWARE IRC Potential bot command response
☑ ET MALWARE IRC potential reptile commands

- [x] ET MALWARE IRC potential bot commands
- [x] ET MALWARE Torpig Reporting User Activity (x25)
- [ ] ET MALWARE FSG Packed Binary via HTTP Inbound
- [ ] ET MALWARE SickleBot Reporting User Activity
- [ ] ET MALWARE w32agent.dsi Posting Info
- [x] ET MALWARE Haxdoor Reporting User Activity
- [ ] ET MALWARE PassSickle Reporting User Activity
- [x] ET MALWARE Haxdoor Reporting User Activity 2
- [ ] ET MALWARE XP keylogger v2.1 mail report - Inbound
- [ ] ET MALWARE XP keylogger v2.1 mail report - Outbound
- [ ] ET MALWARE Tibs Checkin 2
- [ ] ET MALWARE Generic Spyware Update Download
- [ ] ET MALWARE Backdoor.Hupigon INFECTION - Reporting Host Type
- [x] ET MALWARE Banload Downloader Infection - Sending initial email to owner
- [x] ET MALWARE SC-KeyLog Keylogger Installed - Sending Initial Email Report
- [x] ET MALWARE Banker.Delf Infection variant 4 - Sending Initial Email to Owner
- [ ] ET MALWARE GENERAL Possible Trojan Sending Initial Email to Owner - SUCCESSO
- [ ] ET MALWARE Dialer
- [ ] ET MALWARE - Trojan.Proxy.PPAgent.t (updateb)
- [ ] ET MALWARE Agobot-SDBot Commands
- [ ] ET MALWARE Prg Trojan Server Reply
- [x] ET MALWARE Win32.Lager Trojan Reporting
- [ ] ET MALWARE Win32.Lager Trojan Reporting Spam
- [ ] ET MALWARE W32.Downloader Tibs.jy Reporting to C&C
- [ ] ET MALWARE HackerDefender.HE Root Kit Control Connection
- [ ] ET MALWARE Possible Web-based DDoS-command being issued
- [ ] ET MALWARE Unnamed Generic.Malware http get
- [ ] ET MALWARE Warezov/Stration Communicating with Controller 2
- [ ] ET MALWARE Trojan.Duntek establishing remote connection
- [ ] ET MALWARE Bandook v1.2 Initial Connection and Report
- [ ] ET MALWARE Bandook v1.2 Kill Process Command
- [ ] ET MALWARE Bandook v1.2 Reporting Socks Proxy Off
- [x] ET MALWARE Bandook v1.35 Initial Connection and Report
- [ ] ET MALWARE Bandook v1.35 Keepalive Reply
- [ ] ET MALWARE Bandook v1.35 Create Directory Command Send
- [ ] ET MALWARE Bandook v1.35 Window List Reply
- [ ] ET MALWARE Bandook v1.35 Start Socks5 Proxy Command Send
- [ ] ET MALWARE Bandook v1.35 Get Processes Command Reply
- [ ] ET MALWARE Diazom Trojan User-Agent in Use (cv_v2.0.1)
- [x] ET MALWARE Zlob User Agent - updating (internetsecurity)
- [ ] ET MALWARE Downloader.Small User Agent Detected (NetScafe)
- [x] ET MALWARE Downloader.VB.TX/Backdoor.Win32.DSSdoor!IK Checkin
- [ ] ET MALWARE Clicker.BC User Agent Detected (linkrunner)
- [x] ET MALWARE Dialer-715 Install Checkin
- [ ] ET MALWARE Hupigon User Agent Detected (IE_7.0)
- [ ] ET MALWARE Bandok phoning home (xor by 0xe9 to decode)
- [ ] ET MALWARE Bancos User-Agent Detected vb wininet
- [x] ET MALWARE Banker.Delf User-Agent (hhh)
- [ ] ET MALWARE Downloader.Win32.Agent.bwr CnC Beacon
- [x] ET MALWARE Socks666 Connection Initial Packet
- [x] ET MALWARE Socks666 Successful Connect Packet Packet
- [ ] ET MALWARE Socks666 Checkin Success Packet
- [ ] ET MALWARE Downloader.26001 Url Pattern Detected (lunch_id)
- [ ] ET MALWARE DownLoader.30525 Checkin
- [ ] ET MALWARE Proxy.Win32.Agent.mx (2)
- [x] ET MALWARE Zlob User Agent - updating (Winlogon)
- [ ] ET MALWARE perlb0t/w0rmb0t Response 2
- [ ] ET MALWARE Virtumonde Variant Reporting to Controller via HTTP
- [x] ET MALWARE IRC channel topic misc bot commands
- [x] ET MALWARE Dumador Reporting User Activity
- [ ] ET MALWARE Goldun Reporting User Activity
- [ ] ET MALWARE Goldun Reporting User Activity 2
- [ ] ET MALWARE w32agent.dsi Domain Update
- [ ] ET MALWARE Win32.VB.aie Reporting User Activity
- [ ] ET MALWARE TROJAN BankSnif/Nethelper User-Agent (nethelper)
- [ ] ET MALWARE elitekeylogger v1.0 reporting - Inbound
- [ ] ET MALWARE elitekeylogger v1.0 reporting - Outbound
- [x] ET MALWARE Tibs Checkin
- [ ] ET MALWARE Generic Spambot-Spyware Access
- [ ] ET MALWARE Backdoor.Hupigon Possible Control Connection Being Established
- [x] ET MALWARE Banker.Delf Infection - Sending Initial Email to Owner
- [ ] ET MALWARE Banker.Delf Infection variant 2 - Sending Initial Email to Owner
- [ ] ET MALWARE Banker.Delf Infection variant 3 - Sending Initial Email to Owner
- [ ] ET MALWARE GENERAL Possible Trojan Sending Initial Email to Owner - INFECTADO
- [x] ET MALWARE Torpig Reporting User Activity (wur8)
- [ ] ET MALWARE - Trojan.Proxy.PPAgent.t (updatea)
- [ ] ET MALWARE BOT - potential DDoS command (2)
- [ ] ET MALWARE Possible Warezov/Stration Data Post to Controller
- [x] ET MALWARE Win32.Lager Trojan Initial Checkin
- [x] ET MALWARE Win32.Lager Trojan Reporting (gcu)
- [ ] ET MALWARE IRC pBot PHP Bot Commands
- [x] ET MALWARE W32.Downloader Tibs.jy Reporting to C&C (2)
- [ ] ET MALWARE HackerDefender.HE Root Kit Control Connection Reply
- [ ] ET MALWARE psyBNC IRC Server Connection
- [ ] ET MALWARE Stormy Variant HTTP Request
- [ ] ET MALWARE Snatch Reporting User Activity
- [ ] ET MALWARE Klom.A Connecting to Controller
- [ ] ET MALWARE Bandook v1.2 Get Processes
- [ ] ET MALWARE Bandook v1.2 Reporting Socks Proxy Active
- [ ] ET MALWARE Bandook v1.2 Client Ping Reply
- [ ] ET MALWARE Bandook v1.35 Keepalive Send
- [ ] ET MALWARE Bandook v1.35 Create Registry Key Command Send
- [ ] ET MALWARE Bandook v1.35 Window List Command Send
- [ ] ET MALWARE Bandook v1.35 Get Processes Command Send
- [ ] ET MALWARE Bandook v1.35 Socks5 Proxy Start Command Reply
- [x] ET MALWARE Downloader-5265/Torpig/Anserin/Sinowal Unique UA (MSID)
- [x] ET MALWARE W32.Virut.A joining an IRC Channel
- [x] ET MALWARE Suspicious User Agent Detected (RookIE) - Common with Downloaders
- [x] ET MALWARE Generic.Malware.SFL User-Agent (Rescue/9.11)
- [x] ET MALWARE Backdoor.Irc.MFV User Agent Detected (IRC-U)
- [ ] ET MALWARE Hupigon User Agent Detected (SykO)
- [ ] ET MALWARE Banker.Delf User-Agent (Varlok_11000)
- [x] ET MALWARE Banker.Delf User-Agent (Ms)
- [ ] ET MALWARE Bandook iwebho/BBB-phish trojan leaking user data
- [x] ET MALWARE Banload User-Agent Detected (ExampleDL)
- [x] ET MALWARE Bot Backdoor Checkin/registration Request
- [x] ET MALWARE Poebot Related User Agent (SPM_ID=)
- [x] ET MALWARE Socks666 Connect Command Packet
- [ ] ET MALWARE Socks666 Checkin Packet
- [ ] ET MALWARE Downloader.26001 Url Pattern Detected
- [ ] ET MALWARE General Trojan Checkin by MAC chkmac.php
- [ ] ET MALWARE Proxy.Win32.Agent.mx CnC Beacon
- [ ] ET MALWARE Storm Worm HTTP Request
- [ ] ET MALWARE Win32.Agent.ajx Trojan Reporting to Server
- [x] ET MALWARE Brontok User-Agent Detected (Brontok.A3 Browser)
- [ ] ET MALWARE Downloader.Win32.Agent.cav Url Pattern Detected (ping)

- [ ] ET MALWARE Virtumonde Variant Reporting to Controller via HTTP (2)
- [x] ET MALWARE Zlob Updating via HTTP
- [x] ET MALWARE General Downloader Checkin URL (GUID+)
- [ ] ET MALWARE Win32.SkSocket C&C Connection
- [x] ET MALWARE Hupigon URL Infection Checkin Detected
- [ ] ET MALWARE Downloader.Dluca HTTP Checkin
- [ ] ET MALWARE Win32.Agent.bea C&C connection
- [ ] ET MALWARE Win32.Small.qh/xSock Checkin URL Detected
- [x] ET MALWARE Possible Infection Report Mail - Indy Mail lib and No Message Body - Priority 3
- [ ] ET MALWARE Possible Infection Report Mail - Indy Mail lib and MAC Message Body - Priority 3
- [ ] ET MALWARE Zlob Updating via HTTP (v2)
- [ ] ET MALWARE Win32.Agent.cah Checkin Request
- [x] ET MALWARE Mac Trojan HTTP Checkin (accept-language violation)
- [x] ET MALWARE Win32.Agent.pt User-Agent Detected
- [ ] ET MALWARE E-Jihad 3.0 DNS Activity TCP (1)
- [ ] ET MALWARE E-Jihad 3.0 DNS Activity TCP (3)
- [ ] ET MALWARE E-Jihad 3.0 DNS Activity TCP (5)
- [ ] ET MALWARE E-Jihad 3.0 DNS Activity UDP (2)
- [ ] ET MALWARE E-Jihad 3.0 DNS Activity UDP (4)
- [ ] ET MALWARE E-Jihad 3.0 HTTP Activity 1
- [ ] ET MALWARE E-Jihad 3.0 HTTP Activity 3
- [ ] ET MALWARE E-Jihad 3.0 DDoS HTTP Activity INBOUND
- [x] ET MALWARE Hupigon User Agent Detected (??)
- [ ] ET MALWARE Vanquish Trojan HTTP Checkin
- [ ] ET MALWARE ExplorerHijack Trojan HTTP Checkin
- [ ] ET MALWARE Prg Trojan HTTP POST version 2
- [x] ET MALWARE Storm C&C with typo'd User-Agent (Windoss)
- [ ] ET MALWARE Saturn Proxy Initial Outbound Checkin (404.txt)
- [ ] ET MALWARE Saturn Proxy C&C Activity
- [ ] ET MALWARE Zhelatin Update Detected
- [x] ET MALWARE Lop.gfr/Swizzor HTTP Update/Checkin
- [ ] ET MALWARE Ssppyy.com Surveillance Agent Reporting via Email
- [ ] ET MALWARE Win32.Inject.ql Checkin Post
- [ ] ET MALWARE Metajuan trojan checkin
- [x] ET MALWARE Banker.anv Generally Suspicious User-Agent (CustomExchangeBrowser)
- [x] ET MALWARE Illusion Bot (Lussilon) Checkin
- [x] ET MALWARE Theoreon.com Related Trojan Checkin
- [x] ET MALWARE Downloader General Bot Checking In - Possible Win32.Small.htz related
- [x] ET MALWARE Bzub2 Related RPC/Http Checkin
- [ ] ET MALWARE Delf Keylog FTP Upload
- [x] ET MALWARE Banload HTTP Checkin
- [ ] ET MALWARE Sohanad Checkin via HTTP
- [ ] ET MALWARE Delf Download via HTTP
- [x] ET MALWARE Dialer.MC(vf) HTTP Request - Checkin
- [ ] ET MALWARE Dropper-497 (Yumato) System Stats Report
- [x] ET MALWARE Backdoor.Win32.VB.brg C&C Checkin
- [ ] ET MALWARE Suspicious User-Agent - Possible Trojan Downloader (downloaded)
- [ ] ET MALWARE Delf/Hupigon C&C Channel Version Report
- [ ] ET MALWARE Banker.ili HTTP Checkin
- [x] ET MALWARE Possible Infection Report Mail - Indy Mail lib and Nome do Computador in Body
- [ ] ET MALWARE Downloader.49651 Install Report
- [ ] ET MALWARE Cygo Checkin
- [ ] ET MALWARE Goldun Reporting Install
- [ ] ET MALWARE Universal1337 FTP Upload of Compromised Data
- [ ] ET MALWARE Downloader.MisleadApp Fake Security Product Install
- [ ] ET MALWARE Vundo.dam http Update
- [x] ET MALWARE iebar Spyware User Agent (iebar)
- [ ] ET MALWARE General Downloader or Virut C&C Ack
- [x] ET MALWARE Banker.Delf User-Agent (Mz)
- [ ] ET MALWARE Proxy.Win32.Wopla.ag Server Reply
- [x] ET MALWARE Win32.Small.qh/xSock User-Agent Detected
- [x] ET MALWARE Possible Infection Report Mail - Indy Mail lib and No Message Body - Priority 1
- [ ] ET MALWARE Possible Infection Report Mail - Indy Mail lib and MAC Message Body - Priority 1
- [ ] ET MALWARE Storm Worm ICMP DDOS Traffic
- [x] ET MALWARE Suspicious User-Agent - Matcash related Trojan Downloader (Ismazo Advanced Loader)
- [ ] ET MALWARE Farfli User Agent Detected
- [x] ET MALWARE Hupigon User Agent Detected (RAV1.23)
- [x] ET MALWARE Blackenergy Bot Checkin to C&C
- [ ] ET MALWARE E-Jihad 3.0 DNS Activity TCP (2)
- [ ] ET MALWARE E-Jihad 3.0 DNS Activity TCP (4)
- [ ] ET MALWARE E-Jihad 3.0 DNS Activity UDP (1)
- [ ] ET MALWARE E-Jihad 3.0 DNS Activity UDP (3)
- [ ] ET MALWARE E-Jihad 3.0 DNS Activity UDP (5)
- [ ] ET MALWARE E-Jihad 3.0 HTTP Activity 2
- [ ] ET MALWARE E-Jihad 3.0 DDoS HTTP Activity OUTBOUND
- [ ] ET MALWARE Prg Trojan HTTP POST v1
- [ ] ET MALWARE Basine Trojan Checkin
- [x] ET MALWARE Banker.Delf User-Agent (WINDOWS_LOADS)
- [ ] ET MALWARE Srizbi requesting template
- [x] ET MALWARE TROJ_PROX.AFV POST
- [x] ET MALWARE Nebuler/Dialer.qn HTTP Request - Checkin
- [ ] ET MALWARE Saturn Proxy Checkin Response
- [ ] ET MALWARE Pakes Update Detected
- [x] ET MALWARE Pushdo Update URL Detected
- [ ] ET MALWARE Krunchy/BZub HTTP POST Update
- [x] ET MALWARE Zhelatin npopup Update Detected
- [ ] ET MALWARE Rcash.co.kr Bootup Checkin via HTTP
- [x] ET MALWARE Densmail.com Related Trojan Checkin
- [ ] ET MALWARE Neonaby.com Related Trojan User-Agent (neonabyupdate)
- [x] ET MALWARE Downloader General Bot Checking In via HTTP Post (bot_id push)
- [ ] ET MALWARE Renos/ssd.com HTTP Checkin
- [ ] ET MALWARE Delf HTTP Checkin (1)
- [x] ET MALWARE Kpang.com Related Trojan User-Agent (alertup)
- [x] ET MALWARE LDPinch Checkin (3)
- [ ] ET MALWARE Banload HTTP Checkin Detected
- [ ] ET MALWARE Banker.OPX HTTP Checkin
- [ ] ET MALWARE Suspicious User-Agent - Possible Trojan-Dropper.Win32.Agent.eut (Yhrbg)
- [ ] ET MALWARE Dropper-497 (Yumato) Initial Checkin
- [ ] ET MALWARE Dropper-497 Yumato Reply from server
- [ ] ET MALWARE Suspicious User-Agent - Possible Trojan Downloader (Digital)
- [ ] ET MALWARE Suspicious User-Agent - Possible Trojan Downloader (wnames)
- [ ] ET MALWARE Delf Checkin via HTTP (up)
- [ ] ET MALWARE Medbod UDP Phone Home Packet
- [ ] ET MALWARE Downloader.49651 Checkin
- [ ] ET MALWARE Downloader.49651 Online Report
- [ ] ET MALWARE Banker.ike UDP C&C
- [ ] ET MALWARE Win32.Inject.zy Checkin Post
- [ ] ET MALWARE Universal1337 Email Upload of Compromised Data

- [x] ET MALWARE Perfect Keylogger FTP Initial Install Log Upload
- [ ] ET MALWARE Perfect Keylogger FTP Log Upload
- [ ] ET MALWARE Backdoor.Win32.VB.brg C&C Reporting Version
- [ ] ET MALWARE Backdoor.Win32.VB.brg C&C Kill Command Send
- [ ] ET MALWARE Backdoor.Win32.VB.brg C&C Kill Command Acknowledge
- [ ] ET MALWARE Backdoor.Win32.VB.brg C&C DDoS Outbound
- [ ] ET MALWARE Banker Trojan (General) HTTP Checkin
- [ ] ET MALWARE Emogen Reporting via HTTP
- [ ] ET MALWARE Dropper.Win32.VB.on Keylog/System Info Report via HTTP
- [ ] ET MALWARE Vundo HTTP Pre-Install Checkin
- [ ] ET MALWARE Vundo HTTP Post-Install Checkin
- [x] ET MALWARE Shark Pass Stealer Email Report
- [x] ET MALWARE Banker Trojan (General) HTTP Checkin (vit)
- [x] ET MALWARE Win32.Agent.cyt (Or variant) HTTP POST Checkin
- [ ] ET MALWARE Win32.Agent.cyt (Or variant) HTTP POST Checkin (2)
- [x] ET MALWARE Backdoor.Win32.VB.cfi (related) System Info Upload via FTP
- [ ] ET MALWARE Delf CnC Channel Keepalive Pong
- [ ] ET MALWARE Delf CnC Channel Keepalive Ping
- [x] ET MALWARE Winquickupdates.com/Mycashloads.com Related Trojan Install Report
- [x] ET MALWARE Philis.J ICMP Sweep (Payload Hello World)
- [x] ET MALWARE Turkojan C&C Initial Checkin (ams)
- [x] ET MALWARE Turkojan C&C Info Command (MINFO)
- [x] ET MALWARE Turkojan C&C Info Command Response (MINFO)
- [x] ET MALWARE Turkojan C&C Logs Parse Command (LOGS1)
- [ ] ET MALWARE Turkojan C&C Logs Parse Response Response (LOGS1)
- [x] ET MALWARE Turkojan C&C Keepalive (BAGLANTI)
- [x] ET MALWARE Turkojan C&C Browse Drive Command (BROWSC)
- [ ] ET MALWARE Turkojan C&C Browse Drive Command Response (metin)
- [x] ET MALWARE Turkojan C&C nxt Command (nxt)
- [ ] ET MALWARE Turkojan C&C nxt Command Response (nxt)
- [ ] ET MALWARE Dorf/Win32.Inject.adt C&C Communication Outbound
- [ ] ET MALWARE Dorf/Win32.Inject.adt C&C Communication Inbound
- [x] ET MALWARE LDPinch SMTP Password Report
- [x] ET MALWARE Egspy Infection Report Email
- [ ] ET MALWARE Hupigon CnC Data Post (variant abb)
- [x] ET MALWARE Delf Checkin via HTTP (5)
- [ ] ET MALWARE Egspy Infection Report via HTTP
- [x] ET MALWARE Yahoo550.com Related Downloader/Trojan Checkin
- [ ] ET MALWARE Delf Checkin via HTTP (6)
- [ ] ET MALWARE Banload User-Agent Detected (WebUpdate)
- [ ] ET MALWARE Vundo HTTP Post-Install Checkin (2)
- [x] ET MALWARE Daemonize.ft HTTP Checkin
- [ ] ET MALWARE Downloader.VB.CEJ HTTP Checkin
- [ ] ET MALWARE Delf Checkin via HTTP (7)
- [x] ET MALWARE PRG/wnspoem/Zeus InfoStealer Trojan Config Download
- [ ] ET MALWARE Bobax/Kraken/Oderoor UDP 447 CnC Channel Initial Packet Outbound
- [ ] ET MALWARE Bobax/Kraken/Oderoor UDP 447 CnC Channel Initial Packet Inbound
- [ ] ET MALWARE Bobax/Kraken/Oderoor TCP 447 CnC Channel Initial Packet Inbound
- [ ] ET MALWARE Possible Bobax/Kraken/Oderoor UDP 447 CnC Channel Outbound
- [x] ET MALWARE Likely Bot Username in IRC (XP-..)
- [x] ET MALWARE Likely Bot Nick in IRC (USA +..)
- [ ] ET MALWARE Win32.Lydra.hj HTTP Checkin
- [x] ET MALWARE Common Downloader Access Count Tracking URL
- [x] ET MALWARE Common Downloader Install Count Tracking URL
- [x] ET MALWARE Common Downloader Install Count Tracking URL (partner)
- [ ] ET MALWARE Egspy Install Report via HTTP
- [ ] ET MALWARE RhiFrem Trojan Activity - cmd
- [ ] ET MALWARE RhiFrem Trojan Activity - log
- [ ] ET MALWARE Proxy.Corpes.j Infection Report
- [x] ET MALWARE Win32/FakeXPA Checkin URL
- [ ] ET MALWARE Citi-bank.ru Related Trojan Checkin
- [ ] ET MALWARE Trats.a Post-Infection Checkin
- [x] ET MALWARE Hupigon User Agent Detected (VIP2007)
- [ ] ET MALWARE Ceckno Reporting to Controller
- [ ] ET MALWARE Ceckno Keepalive from Controller
- [x] ET MALWARE Common Downloader Install Report URL
- [x] ET MALWARE Common Downloader Install Report URL (pid - mac)
- [x] ET MALWARE Win32 Cloaker Related Post Infection Checkin
- [x] ET MALWARE SpamTool.Win32.Agent.gy/Grum/Tedroo Or Similar HTTP Checkin
- [x] ET MALWARE Common Downloader Install Report URL (wmid - ucid)
- [ ] ET MALWARE Dropper mdodo.com Related Trojan
- [ ] ET MALWARE Dropper 6dzone.com Related Trojan
- [ ] ET MALWARE Client Visiting Possibly Compromised Site (HaCKeD By BeLa & BodyguarD)
- [x] ET MALWARE Optix Pro Trojan/Keylogger Reporting Installation via Email
- [x] ET MALWARE Optix Pro Trojan/Keylogger Reporting Installation via HTTP-Email Post
- [ ] ET MALWARE Looked.P/Gamania/Delf #109/! Style CnC Checkin Response from Server
- [ ] ET MALWARE Asprox-style Message ID
- [ ] ET MALWARE Asprox phishing email detected
- [x] ET MALWARE Generic Spambot (often Tibs) Post-Infection Checkin (justcount.net likely)
- [x] ET MALWARE Common Downloader Install Report URL (farfly checkin)
- [ ] ET MALWARE Fake.Googlebar or Softcash.org Related Post-Infection Checkin
- [ ] ET MALWARE Pass Stealer FTP Upload
- [x] ET MALWARE ProxyBot Phone Home Traffic
- [x] ET MALWARE Cashout Proxy Bot reg_DST
- [x] ET MALWARE Knockbot Proxy Checkin
- [ ] ET MALWARE Winspywareprotect.com Fake AV/Anti-Spyware Install Checkin
- [x] ET MALWARE Banload HTTP Checkin Detected (envia.php)
- [ ] ET MALWARE Hupigon CnC Communication (variant bysj)
- [ ] ET MALWARE Pointpack.kr Related Trojan Checkin
- [ ] ET MALWARE Common Spambot HTTP Checkin
- [ ] ET MALWARE DNS Changer HTTP Post Checkin
- [ ] ET MALWARE Banker.JU Related HTTP Post-infection Checkin
- [x] ET MALWARE DMSpammer HTTP Post Checkin
- [ ] ET MALWARE Bifrose Connect to Controller
- [x] ET MALWARE Bifrose Response from Controller
- [ ] ET MALWARE Hitpop Checkin
- [ ] ET MALWARE Win32/Kryptik.AR Variant Winifixer.com Related Checkin URL
- [ ] ET MALWARE 3alupKo/Win32.Socks.n Related Checkin URL
- [ ] ET MALWARE Banload HTTP Checkin Detected (quem=)
- [ ] ET MALWARE RLPacked Binary - Likely Hostile
- [ ] ET MALWARE Win32.Onlinegames.ajok CnC Packet to Server
- [ ] ET MALWARE Win32.Onlinegames.ajok CnC Packet from Server

- [x] ET MALWARE Codesoft PW Stealer Email Report Outbound
- [ ] ET MALWARE Win32.Small.wpx or Related Downloader Posting Data
- [x] ET MALWARE Win32.Small.AB or related Post-infection checkin
- [ ] ET MALWARE Zalupko/Koceg/Mandaph manda.php Checkin
- [x] ET MALWARE xpsecuritycenter.com Fake AntiVirus GET-Install Checkin
- [ ] ET MALWARE Steam Pass Stealer FTP Upload
- [ ] ET MALWARE Beizhu/Womble/Vipdataend Controller Keepalive
- [ ] ET MALWARE Keypack.co.kr Related Trojan User-Agent Detected
- [ ] ET MALWARE Themida Packed Binary - Likely Hostile
- [ ] ET MALWARE Swizzor Checkin
- [ ] ET MALWARE CoreFlooder.Q C&C Checkin
- [x] ET MALWARE Steam Steal0r
- [x] ET MALWARE Playtech Downloader Online Gaming Checkin
- [ ] ET MALWARE Unknown Keylogger checkin
- [x] ET MALWARE RegHelper Installation
- [x] ET MALWARE Swizzor Checkin (kgen_up)
- [ ] ET MALWARE PoisonIvy Key Exchange with CnC Response
- [x] ET MALWARE Piptea.a Related Trojan Checkin (2)
- [ ] ET MALWARE Zlob HTTP Checkin
- [ ] ET MALWARE 3alupKo/Win32.Socks.n Related Checkin URL (3)
- [ ] ET MALWARE Fullspace.cc or Related Checkin (1)
- [x] ET MALWARE contacy.info Trojan Checkin (User agent clk_jdfhid)
- [x] ET MALWARE RemoteSpy.com Upload Detected
- [ ] ET MALWARE Trojan-Dropper.Win32.Small.avu HTTP Checkin
- [ ] ET MALWARE PWS.Gamania Checkin
- [ ] ET MALWARE Coreflood/AFcore Trojan Infection
- [x] ET MALWARE Win32 Dialer Variant
- [ ] ET MALWARE Coreflood/AFcore Trojan Infection (2)
- [ ] ET MALWARE Donbot Connect to CnC
- [x] ET MALWARE Rouge Security Software Win32.BHO.egw
- [ ] ET MALWARE HotLan.C Spambot C&C download command
- [x] ET MALWARE Banload POST Checkin (dados)
- [ ] ET MALWARE thespybot.com installation download detected
- [ ] ET MALWARE Dialer.Win32.E-Group.n Checkin
- [ ] ET MALWARE Antispywareexpert.com Fake AS Install Checkin
- [ ] ET MALWARE Backdoor.Win32.VB.fdi Bot Reporting to Controller
- [ ] ET MALWARE Suspicious User-Agent - Possible Trojan Downloader (\xa2\xa2HttpClient)
- [ ] ET MALWARE Hupigon.AZG Checkin
- [ ] ET MALWARE Keylogger Infection Report via POST
- [ ] ET MALWARE Proxy.Win32.Fackemo.g/Katusha/FakeAlert Checkin
- [ ] ET MALWARE Infected System Looking up chr.santa-inbox.com CnC Server
- [x] ET MALWARE Bravix Checkin
- [ ] ET MALWARE PECompact2 Packed Binary - Sometimes Hostile
- [x] ET MALWARE Banito/Agent.pb Pass Stealer Email Report Outbound
- [ ] ET MALWARE Viruscatch.co.kr/Win32.Small.hvd Mysql Command and Control Connection (user viruscatch)
- [x] ET MALWARE Nbar.co.kr Related Trojan Checkin
- [ ] ET MALWARE Visual Shock Keylogger Reporting Idle to Controller
- [ ] ET MALWARE Cinmus.Checkin 2
- [x] ET MALWARE Tibs Trojan Downloader
- [x] ET MALWARE Spy-Net Trojan Connection
- [ ] ET MALWARE Torpig Infection Reporting
- [ ] ET MALWARE Generic PSW Agent server reply
- [ ] ET MALWARE Delf Key Checkin (Clicker.Win32.Delf.afl)
- [ ] ET MALWARE Likely eCard Malware Laden Email Inbound
- [ ] ET MALWARE Backdoor.Win32.Assasin.20.C Control Session Server Reply
- [ ] ET MALWARE Gimmiv.A.dll Infection
- [x] ET MALWARE Hitpop.AG/Pophot.az HTTP Checkin
- [ ] ET MALWARE Banload Gadu-Gadu CnC Message Detected
- [x] ET MALWARE FraudLoad.aww HTTP CnC Post
- [x] ET MALWARE Perfect Keylogger FTP Initial Install Log Upload (Null obfuscated)
- [x] ET MALWARE Banker/Banbra Variant POST via x-www-form-urlencoded
- [x] ET MALWARE Lop.gfr/Swizzor HTTP Update/Checkin (usually host-domain-lookup.com related)
- [x] ET MALWARE KLog Nick Keylogger Checkin
- [x] ET MALWARE Lost Door Checkin
- [x] ET MALWARE Dialer.Trojan Activity
- [x] ET MALWARE SC-KeyLog Keylogger Installed - Sending Log Email Report
- [ ] ET MALWARE Pakes/Cutwail/Kobcka Checkin Detected High Ports
- [x] ET MALWARE Donkeyp2p Update Detected
- [ ] ET MALWARE LD Pinch Checkin (HTTP POST on port 82)
- [ ] ET MALWARE Keylogger Crack by bahman
- [x] ET MALWARE Virtumod/Agent.ufv/Virtumonde Get Request
- [ ] ET MALWARE PoisonIvy Key Exchange with CnC Init
- [x] ET MALWARE Piptea.a Related Trojan Checkin (1)
- [ ] ET MALWARE Piptea.a Related Trojan Checkin (3)
- [ ] ET MALWARE 3alupKo/Win32.Socks.n Related Checkin URL (2)
- [ ] ET MALWARE Zlob Initial Check-in Version 2 (confirm.php?sid=)
- [x] ET MALWARE Fullspace.cc or Related Checkin (2)
- [ ] ET MALWARE Obitel trojan calling home
- [x] ET MALWARE LDPinch SMTP Password Report with mail client The Bat!
- [ ] ET MALWARE Win32.Dialer.buv Sending Information Home
- [x] ET MALWARE Razy Variant Checkin
- [x] ET MALWARE Possible Windows executable sent when remote host claims to send a Text File
- [ ] ET MALWARE Rootkit.Win32.Clbd.cz Checkin
- [ ] ET MALWARE Keylogger.ane Checkin
- [ ] ET MALWARE Donbot Report to CnC
- [ ] ET MALWARE Backdoor Possible Backdoor.Cow Varient (Backdoor.Win32.Agent.lam) C&C traffic
- [ ] ET MALWARE HotLan.C Spambot Trojan Activity
- [ ] ET MALWARE Trojan-PSW.Win32.Nilage.crg Checkin
- [x] ET MALWARE FakeAV Win32/Antivirus2008 CnC Beacon
- [ ] ET MALWARE Pushdo Checkin
- [ ] ET MALWARE Trojan-PWS.Win32.VB.tr Checkin Detected
- [ ] ET MALWARE VirtualProtect Packed Binary - Likely Hostile
- [ ] ET MALWARE Win32/Antivirus2008 Fake AV Install Report
- [ ] ET MALWARE Win32.Agent.zrm/Infostealer.Bancos Checkin
- [ ] ET MALWARE Stpage Checkin (nomodem)
- [x] ET MALWARE Virusremover2008.com Checkin
- [ ] ET MALWARE Hupigon.dkxh Checkin to CnC
- [x] ET MALWARE Social-bos.biz related trojan checkin (trackid=hex)
- [x] ET MALWARE Trojan.Win32.Buzus Checkin
- [x] ET MALWARE Win32.Crypt.nc Checkin
- [ ] ET MALWARE Trojan Sinowal/Torpig Phoning Home
- [ ] ET MALWARE Visual Shock Keylogger Reporting to Controller
- [ ] ET MALWARE Cinmus.Checkin 1
- [x] ET MALWARE PlayMP3z.biz Related Spyware/Trojan Install Report
- [ ] ET MALWARE Keylogger PRO GOLD Post
- [ ] ET MALWARE Spy-Net Trojan Connection (2)
- [ ] ET MALWARE Zbot/Zeus HTTP POST
- [x] ET MALWARE Zbot/Zeus or Related Infection Checkin
- [ ] ET MALWARE Backdoor.Win32.Agent.fvt Checkin
- [ ] ET MALWARE Backdoor.Win32.Assasin.20.C Control Session Start
- [ ] ET MALWARE Backdoor.Win32.Assasin.20.C Control Channel Client Reply
- [x] ET MALWARE Gimmiv Infection Ping Outbound

- [ ] ET MALWARE Gimmiv Infection Ping Inbound
- [x] ET MALWARE Conficker/KernelBot/MS08-067 related Trojan Checkin
- [x] ET MALWARE Conficker/MS08-067 Worm Traffic Outbound
- [ ] ET MALWARE Autorun.qvi Related HTTP Get on Off Port
- [ ] ET MALWARE Insidebar.co.kr Related Infection Checkin
- [ ] ET MALWARE DNS Changer.bnm/Downloader.bnm CnC Channel Start
- [ ] ET MALWARE DNS Changer.bnm/Downloader.bnm Second CnC Channel Start
- [ ] ET MALWARE Trojan-PWS.Win32.Small.gs Passwords leak over FTP
- [x] ET MALWARE Virtumonde Variant Reporting to Controller via HTTP (3)
- [ ] ET MALWARE MEREDROP/micr0s0fts.cn Related Checkin
- [ ] ET MALWARE Trojan.Delf-5496 Checkin Error
- [ ] ET MALWARE Trojan.Delf-5496 File Manager Access Report
- [ ] ET MALWARE Spyguarder.com Fake AV Install Report
- [ ] ET MALWARE DNSChanger.AT or related Infection Checkin Post
- [x] ET MALWARE TDSServ or Tidserv variant Checkin
- [ ] ET MALWARE UpackbyDwing binary in HTTP Download Possibly Hostile
- [ ] ET MALWARE Win32.Small.yml or Related HTTP Checkin
- [ ] ET MALWARE Trojan.Win32.Small.yml client command
- [x] ET MALWARE Mac User-Agent Typo INBOUND Likely Hostile
- [ ] ET MALWARE Pointfree.co.kr Trojan/Spyware Infection Checkin
- [ ] ET MALWARE Vundo Variant reporting to Controller via HTTP (1)
- [ ] ET MALWARE Trojan-GameThief.Win32.OnLineGames infection report
- [ ] ET MALWARE VMProtect Demo version Packed Binary - Likely Hostile
- [x] ET MALWARE Downadup/Conficker A or B Worm reporting
- [ ] ET MALWARE Vipdataend C&C Traffic - Status OK (variant 2)
- [ ] ET MALWARE Hupigon System Stats Report (I-variant)
- [ ] ET MALWARE TROJ_INJECT.NI Update Request
- [ ] ET MALWARE Delfsnif/Buzus.fte Remote Response
- [x] ET MALWARE Password Stealer - User-Agent (Ucheck)
- [ ] ET MALWARE Password Stealer (PSW.Win32.Magania Family) GET
- [x] ET MALWARE Parite Setup Connection (tqzn.com related)
- [x] ET MALWARE Comfoo Outbound Communication
- [x] ET MALWARE General Banker.PWS POST Checkin
- [ ] ET MALWARE Bifrose Response from Controller (PING PONG)
- [x] ET MALWARE Overtoolbar.net Backdoor ICMP Checkin Response
- [ ] ET MALWARE Psyb0t joining an IRC Channel
- [ ] ET MALWARE Possible Vundo EXE Download Attempt
- [x] ET MALWARE Conficker.b Shellcode
- [ ] ET MALWARE Crypt.CFI.Gen Checkin
- [ ] ET MALWARE Possible KEYPLUG/Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 4)
- [ ] ET MALWARE Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 16)
- [ ] ET MALWARE Zbot/Zeus Dropper Infection - /loads.php
- [x] ET MALWARE Fake AV Downloader.Onestage/FakeAlert.ZR User-Agent (AV1)
- [ ] ET MALWARE PcClient Backdoor Checkin Packet 1
- [x] ET MALWARE General Win32 Backdoor Checkin POST Packet 1
- [ ] ET MALWARE LDPinch Reporting infection via Email
- [x] ET MALWARE Banker/Banbra Related HTTP Post-infection Checkin
- [x] ET MALWARE General Trojan Downloader
- [ ] ET MALWARE Tigger.a/Syzor Checkin
- [ ] ET MALWARE Win32.Hupigon Control Server Response
- [x] ET MALWARE Bredolab Downloader Communicating With Controller (1)
- [ ] ET MALWARE Bredolab Check In
- [ ] ET MALWARE Trojan.Win32.Regrun.ro FTP connection detected
- [x] ET MALWARE Suspicious Accept-Language HTTP Header zh-cn likely Kernelbot/Conficker Trojan Related
- [x] ET MALWARE Possible Rar'd Malware sent when remote host claims to send an Image
- [ ] ET MALWARE Mcboo.com/Bundlext.com related Trojan Checkin URL
- [x] ET MALWARE Brontok/Joseray User-Agent Detected (Joseray.A3 Browser)
- [ ] ET MALWARE DNS Changer.bnm/Downloader.bnm CnC Channel Start Response
- [ ] ET MALWARE DNS Changer.bnm/Downloader.bnm Second CnC Channel Traffic
- [x] ET MALWARE Downloader Win32.Small.agoy Checkin
- [x] ET MALWARE Koobface Trojan HTTP Post Checkin
- [x] ET MALWARE Perfect Keylogger Install Email Report
- [ ] ET MALWARE Trojan.Delf-5496 Egg Request
- [x] ET MALWARE Trojan.Delf-5496 New Infection Report
- [ ] ET MALWARE Backdoor.Win32/PcClient.ZL Checkin
- [x] ET MALWARE Lop_com or variant Checkin (9kgen_up)
- [x] ET MALWARE dlink router access attempt
- [ ] ET MALWARE UpackbyDwing binary in HTTP (2) Possibly Hostile
- [ ] ET MALWARE Trojan.Win32.Small.yml client registration
- [ ] ET MALWARE Win32.Small.yml or Related HTTP Command
- [x] ET MALWARE Waledac Beacon Traffic Detected
- [ ] ET MALWARE onmuz.com Infection Activity
- [ ] ET MALWARE Vundo Variant reporting to Controller via HTTP (2)
- [ ] ET MALWARE Win32/Korklic.A
- [x] ET MALWARE Zlob User Agent (securityinternet)
- [ ] ET MALWARE Vipdataend C&C Traffic Checkin variant 2
- [x] ET MALWARE 404 Response with an EXE Attached - Likely Malware Drop
- [x] ET MALWARE Asprox Form Submission to C&C
- [x] ET MALWARE Backdoor Lanfiltrator Checkin
- [ ] ET MALWARE VMProtect Packed Binary Inbound via HTTP - Likely Hostile
- [ ] ET MALWARE Generic Banker Trojan Downloader Config to client
- [ ] ET MALWARE Tigger.a/Syzor Control Checkin
- [ ] ET MALWARE Downadup/Conficker A Worm reporting
- [ ] ET MALWARE Win32/Monkif Downloader Checkin
- [ ] ET MALWARE Bifrose Connect to Controller (PING PONG)
- [x] ET MALWARE Overtoolbar.net Backdoor ICMP Checkin Request
- [x] ET MALWARE Koobface Checkin via POST
- [ ] ET MALWARE Possible Vundo Trojan Variant reporting to Controller
- [ ] ET MALWARE Conficker.a Shellcode
- [x] ET MALWARE Alman Dropper Checkin
- [ ] ET MALWARE Possible KEYPLUG/Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 1)
- [ ] ET MALWARE Possible KEYPLUG/Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 5)
- [ ] ET MALWARE Rogue A/V Win32/FakeXPA GET Request
- [x] ET MALWARE Farfli HTTP Checkin Activity
- [x] ET MALWARE PWSteal.Bancos Generic Banker Trojan SCR Download
- [ ] ET MALWARE PcClient Backdoor Checkin
- [x] ET MALWARE General Win32 Backdoor Checkin POST
- [ ] ET MALWARE CoreFlooder C&C Checkin (2)
- [ ] ET MALWARE Boaxxe HTTP POST Checkin
- [ ] ET MALWARE Small.zon checkin
- [ ] ET MALWARE Metafisher/Bzub/Cimuz/Tanspy Reporting User Activity
- [ ] ET MALWARE Urlzone/Bebloh Communication with Controller
- [ ] ET MALWARE Bredolab Downloader Communicating With Controller (2)
- [x] ET MALWARE Virut Counter/Check-in

- [ ] ET MALWARE Bredolab Downloader Response Binaries from Controller
- [ ] ET MALWARE Personal Defender 2009 - trash.py
- [ ] ET MALWARE Patcher/Bankpatch V2 Communication with Controller
- [x] ET MALWARE Gozi check-in / update
- [x] ET MALWARE Murlo Trojan Checkin
- [x] ET MALWARE Virut Family GET
- [x] ET MALWARE Zbot/Beomok/PSW - HTTP POST
- [x] ET MALWARE Atya Dropper Possible Rootkit - HTTP GET
- [ ] ET MALWARE BANLOAD Downloader GET Checkin
- [ ] ET MALWARE Virut Counter/Check-in
- [ ] ET MALWARE Generic Info Stealer - HTTP POST
- [x] ET MALWARE Fasec/FakeAV Alert/Keylogger/Dropper/DNSChanger Possible Rootkit - HTTP GET
- [x] ET MALWARE APT1 WEBC2-UGX Related Pingbed/Downbot User-Agent (Windows+NT+5.x)
- [ ] ET MALWARE FAKE/ROGUE AV HTTP Post
- [ ] ET MALWARE Qhosts Trojan Check-in
- [x] ET MALWARE Gaboc Trojan Check-in
- [x] ET MALWARE Win32/Nubjub.A HTTP Check-in
- [x] ET MALWARE Sality - Fake Opera User-Agent
- [x] ET MALWARE Sality - Fake Opera User-Agent (Opera/8.89)
- [ ] ET MALWARE BackDoor-EGB Check-in
- [ ] ET MALWARE Downloader Infostealer - GET Checkin
- [x] ET MALWARE Generic Downloader - HTTP POST
- [ ] ET MALWARE FAKE/ROGUE AV Encoded data= HTTP POST
- [x] ET MALWARE Yoda's Protector Packed Binary - VERY Likely Hostile
- [ ] ET MALWARE Navipromo related update
- [x] ET MALWARE Win32.Runner/Bublik Checkin
- [x] ET MALWARE Fraudload/FakeAlert/FakeVimes Downloader - POST
- [x] ET MALWARE Oficla Downloader Activity Observed
- [x] ET MALWARE Luder.B User-Agent (Mozilla/4.0 (SPGK)) - GET
- [x] ET MALWARE Win32.Virut - GET
- [ ] ET MALWARE KillAV/Dropper/Mdrop/Hupigon - HTTP GET
- [x] ET MALWARE Trojan.MyDNS DNSChanger - HTTP POST
- [x] ET MALWARE Win32.VB.tdq - Fake User-Agent
- [ ] ET MALWARE Win32/Wombot.A checkin Possible Bruteforcer for Web Forms and Accounts - HTTP POST
- [ ] ET MALWARE Banker Trojan CnC Hello Command
- [x] ET MALWARE Possible Windows executable sent when remote host claims to send html content
- [x] ET MALWARE Banker.Delf User-Agent (MzApp)
- [ ] ET MALWARE Likely Fake Antivirus Download Antivirus_21.exe
- [ ] ET MALWARE Likely TDSS Download (codec.exe)
- [ ] ET MALWARE Likely Infostealer exe Download
- [ ] ET MALWARE Likely Fake Antivirus Download AntivirusPlus.exe
- [x] ET MALWARE Hiloti/Mufanom Downloader Checkin
- [ ] ET MALWARE Palevo/BFBot/Mariposa client join attempt
- [x] ET MALWARE Drop.Agent.bfsv HTTP Activity (UsER-AgENt)
- [ ] ET MALWARE DHL Spam Inbound
- [x] ET MALWARE Koobface C&C availability check
- [ ] ET MALWARE Koobface fetch C&C command detected
- [ ] ET MALWARE Glacial Dracon C&C Communication
- [x] ET MALWARE Tibs/Harnig Downloader Activity
- [x] ET MALWARE DownloaderExchanger/Cbeplay Variant Checkin
- [ ] ET MALWARE Opachki Link Hijacker Traffic Redirection
- [ ] ET MALWARE WindowsEnterpriseSuite FakeAV check-in HEAD
- [x] ET MALWARE WindowsEnterpriseSuite FakeAV get_product_domains.php
- [ ] ET MALWARE Personal Defender 2009 - prinimalka.py
- [ ] ET MALWARE Koobface BLACKLABEL
- [ ] ET MALWARE Patcher/Bankpatch Module Download Request
- [ ] ET MALWARE Swizzor Family GET
- [ ] ET MALWARE NoBo Downloader Dropper GET
- [x] ET MALWARE TSPY_BANKER.IDV/Infostealer.Bancos Module Download
- [ ] ET MALWARE Trash Family - HTTP POST
- [x] ET MALWARE Common Trojan HTTP GET Logging
- [x] ET MALWARE FAKE AV HTTP CnC Post
- [x] ET MALWARE Win32/Sisron/BackDoor.Cybergate.1 Checkin
- [x] ET MALWARE Bancos/Banker Info Stealer Post
- [x] ET MALWARE Sality - Fake Opera User-Agent
- [ ] ET MALWARE Downloader Possible AV KILLER
- [x] ET MALWARE Generic Win32.Autorun HTTP Post
- [ ] ET MALWARE s4t4n1c Trojan Check-in
- [x] ET MALWARE Urlzone/Bebloh Trojan Check-in
- [ ] ET MALWARE Win32/Pasta Downloader - GET Checkin to Fake GIF
- [x] ET MALWARE Generic Downloader Checkin - HTTP GET
- [x] ET MALWARE Gamania Trojan Check-in
- [ ] ET MALWARE Keylogger Pro Update Check
- [ ] ET MALWARE PCFlashbang.com Spyware Checkin (PCFlashBangA)
- [x] ET MALWARE Banker PWS/Infostealer HTTP GET Checkin
- [x] ET MALWARE FAKE/ROGUE AV/Security Application Checkin
- [ ] ET MALWARE Unkown Trojan User-Agent (5.1 ...)
- [x] ET MALWARE Win32.Hupigon.dkwt Related Checkin
- [ ] ET MALWARE Banker/Bancos/Infostealer Possible Rootkit - HTTP HEAD Request
- [ ] ET MALWARE Monkif/DlKroha Trojan Activity HTTP Outbound
- [x] ET MALWARE Screenblaze SCR Related Backdoor - GET
- [x] ET MALWARE PoisonIvy RAT/Backdoor follow on POST Data PUSH Packet
- [x] ET MALWARE Swizzor-based Downloader - Invalid User-Agent (Mozilla/4.0 (compatible MSIE 7.0 na .NET CLR 2.0.50727 .NET CLR 3.0.4506.2152 .NET CLR 3.5.30729))
- [ ] ET MALWARE AVKiller with Backdoor checkin
- [ ] ET MALWARE Downloader.Win32.Delf followon POST Data PUSH Packet
- [ ] ET MALWARE Virut/Virutas/Virtob/QQHelper Dropper Family - HTTP GET
- [x] ET MALWARE Banker Trojan CnC AddNew Command
- [ ] ET MALWARE Win32/Winwebsec User-Agent Detected
- [x] ET MALWARE Possible Windows executable sent when remote host claims to send HTML/CSS Content
- [ ] ET MALWARE Potential Gemini Malware Download
- [ ] ET MALWARE Likely Fake Antivirus Download ws.exe
- [ ] ET MALWARE Likely TDSS Download (pcdef.exe)
- [x] ET MALWARE Likely Fake Antivirus Download InternetAntivirusPro.exe
- [ ] ET MALWARE SafeFighter Fake Scanner Installation in Progress
- [ ] ET MALWARE Bredolab Infection - Windows Key
- [ ] ET MALWARE Palevo/BFBot/Mariposa server join acknowledgement
- [ ] ET MALWARE Possible Win32/Agent.QBY CnC Post
- [x] ET MALWARE Koobface HTTP Request (2)
- [ ] ET MALWARE Koobface C&C availability check successful
- [ ] ET MALWARE Nanspy Bot Checkin
- [ ] ET MALWARE Daonol C&C Communication
- [ ] ET MALWARE Silon Encrypted Data POST to C&C
- [ ] ET MALWARE Possible Fake-Rean Installer Activity (Malwareurl.com Top 30)
- [ ] ET MALWARE W32.Koblu
- [x] ET MALWARE WindowsEnterpriseSuite FakeAV check-in GET
- [x] ET MALWARE Obitel Downloader Request

- [ ] ET MALWARE WindowsEnterpriseSuite FakeAV Reporting via POST initial check-in
- [ ] ET MALWARE Eleonore Exploit Pack activity
- [ ] ET MALWARE Sinowal/Torpig Checkin
- [x] ET MALWARE Asprox Data Post to C&C
- [ ] ET MALWARE Opachki Link Hijacker HTTP Header Injection
- [x] ET MALWARE Dosenjo/Kvadr Proxy Trojan Activity
- [ ] ET MALWARE Chorns/Poisonlvy related Backdoor Initial Connection
- [ ] ET MALWARE Ultimate HAckerz Team User-Agent (Made by UltimateHackerzTeam) - Likely Trojan Report
- [ ] ET MALWARE - Possible Zeus/Perkesh (.bin) configuration download
- [x] ET MALWARE Fake AV GET
- [ ] ET MALWARE Possible Storm Variant HTTP Post (S)
- [ ] ET MALWARE Potential Gemini/Fake AV Download URL Detected
- [ ] ET MALWARE Potential Fake AV GET installer_1.exe
- [ ] ET MALWARE Potential Fake AV Download (download/install.php)
- [x] ET MALWARE FakeAV FakeSmoke HTTP POST check-in
- [x] ET MALWARE Potential FakeAV HTTP GET Check-IN (/check)
- [x] ET MALWARE Likely FakeAV/Fakeinit/FraudLoad Checkin
- [x] ET MALWARE Likely FakeAV/Fakeinit/FraudLoad Checkin
- [ ] ET MALWARE Lethic Spambot CnC Initial Connect Bot Response
- [ ] ET MALWARE Lethic Spambot CnC Connect Command (port 25 specifically)
- [ ] ET MALWARE Lethic Spambot CnC Bot Transaction Relay
- [ ] ET MALWARE Aurora Backdoor (C&C) client connection to CnC
- [x] ET MALWARE Likely Koobface Beaconing (getexe)
- [ ] ET MALWARE Oficla Russian Malware Bundle C&C instruction response with runurl
- [x] ET MALWARE Oficla Checkin (1)
- [x] ET MALWARE Sasfis Botnet Client Reporting Back to Controller After Command Execution
- [ ] ET MALWARE Knockbot Proxy Response From Controller
- [ ] ET MALWARE Bredavi Configuration Update Response
- [ ] ET MALWARE smain?scout=acxc Generic Download landing
- [ ] ET MALWARE WScript/VBScript XMLHTTP downloader likely malicious get?src=
- [ ] ET MALWARE Pragma hack Detected Outbound - Likely Infected Source
- [x] ET MALWARE BlackEnergy v2.x HTTP Request with Encrypted Variables
- [x] ET MALWARE Generic Downloader checkin (3)
- [ ] ET MALWARE Arucer Command Execution
- [ ] ET MALWARE Arucer WRITE FILE command
- [ ] ET MALWARE Arucer NOP Command
- [ ] ET MALWARE Arucer YES Command
- [ ] ET MALWARE Arucer DEL FILE Command
- [ ] ET MALWARE Vobfus/Changeup/Chinky Download Command
- [x] ET MALWARE Fruspam polling for IP likely infected
- [ ] ET MALWARE Eleonore Exploit Pack activity variant May 2010
- [x] ET MALWARE IRC Potential bot update/download via ftp command
- [ ] ET MALWARE Nine Ball Infection ya.ru Post
- [ ] ET MALWARE Cosmu Process Dump Report
- [x] ET MALWARE Downloader.Win32.Small CnC Beacon
- [x] ET MALWARE Rogue.Win32/Winwebsec Checkin
- [ ] ET MALWARE Trojan.Win32.FraudPack.aweo
- [x] ET MALWARE Stuxnet index.php
- [x] ET MALWARE Sality Variant Downloader Activity (2)
- [ ] ET MALWARE FakeAV SetupSecure Download Attempt SetupSecure
- [x] ET MALWARE Sinowal/sinonet/mebroot/Torpig infected host checkin
- [ ] ET MALWARE Stupid Stealer C&C Communication (2)
- [ ] ET MALWARE wisp backdoor detected reporting
- [x] ET MALWARE WindowsEnterpriseSuite FakeAV Reporting via POST
- [ ] ET MALWARE Banload Checkin
- [ ] ET MALWARE W32.SillyFDC Checkin
- [ ] ET MALWARE Generic Trojan Checkin (double Content-Type headers)
- [x] ET MALWARE W32/Scar Downloader Request
- [ ] ET MALWARE FakeAV Reporting - POST often to resolution|borders.php
- [ ] ET MALWARE Chorns/Poisonlvy related Backdoor Keep Alive
- [ ] ET MALWARE Fake/Rogue AV Landing Page Encountered
- [x] ET MALWARE Syrutrk/Gibon/Bredolab Checkin
- [x] ET MALWARE Generic Trojan Checkin (UA VBTagEdit)
- [ ] ET MALWARE Possible Storm Variant HTTP Post (U)
- [ ] ET MALWARE Potential Fake AV GET installer.1.exe
- [x] ET MALWARE Dropper Checkin (often scripts.dlv4.com related)
- [x] ET MALWARE Vundo User-Agent Check-in
- [ ] ET MALWARE Bebloh C&C HTTP POST
- [x] ET MALWARE FakeAV Landing Page (aid sid)
- [x] ET MALWARE Likely FakeAV/Fakeinit/FraudLoad Checkin
- [x] ET MALWARE Lethic Spambot CnC Initial Connect
- [ ] ET MALWARE Lethic Spambot CnC Connect Command
- [ ] ET MALWARE Lethic Spambot CnC Bot Command Confirmation
- [ ] ET MALWARE Likely Fake Antivirus Download Setup_2012.exe
- [ ] ET MALWARE Aurora Backdoor (C&C) connection CnC response
- [ ] ET MALWARE Gootkit Checkin User-Agent (Gootkit HTTP Client)
- [ ] ET MALWARE Oficla Russian Malware Bundle C&C instruction response
- [ ] ET MALWARE Oficla Russian Malware Bundle C&C instruction response (2)
- [x] ET MALWARE Zalupko/Koceg/Mandaph HTTP Checkin (2)
- [x] ET MALWARE Knockbot Proxy Response From Controller (empty command)
- [ ] ET MALWARE Java Downloader likely malicious payload download src=xrun
- [ ] ET MALWARE Torpig Related Fake User-Agent (Apache (compatible...))
- [x] ET MALWARE Incorrectly formatted User-Agent string (dashes instead of semicolons) Likely Hostile
- [ ] ET MALWARE Blackenergy Bot Checkin to C&C (2)
- [x] ET MALWARE BlackEnergy v2.x Plugin Download Request
- [x] ET MALWARE Win32.Tdss User Agent Detected (Mozzila)
- [ ] ET MALWARE Arucer DIR Listing
- [ ] ET MALWARE Arucer READ FILE Command
- [ ] ET MALWARE Arucer FIND FILE Command
- [ ] ET MALWARE Arucer ADD RUN ONCE Command
- [x] ET MALWARE Dropper Checkin 2 (often scripts.dlv4.com related)
- [x] ET MALWARE Unruy Downloader Checkin
- [ ] ET MALWARE Trojan-Dropper.Win32.Flystud
- [ ] ET MALWARE Unknown Malware Download Request
- [x] ET MALWARE Generic Checkin - MSCommonInfoEx
- [ ] ET MALWARE Outbound AVISOSVB MSSQL Request
- [ ] ET MALWARE Trojan-Downloader Win32.Genome.avan
- [x] ET MALWARE Win32/Chekafe.A or Related Infection Checkin
- [x] ET MALWARE Trojan.Win32.Cosmu.xet CnC Beacon
- [ ] ET MALWARE Butterfly/Mariposa Bot Join Acknowledgment
- [x] ET MALWARE Win32/Keatep.B Checkin
- [x] ET MALWARE Sality Variant Downloader Activity (3)
- [x] ET MALWARE Sinowal/sinonet/mebroot/Torpig infected host POSTing process list
- [ ] ET MALWARE Stupid Stealer C&C Communication (1)
- [x] ET MALWARE indux.php check-in
- [x] ET MALWARE FakeYak or Related Infection Checkin 1

- [ ] ET MALWARE FakeYak or Related Infection Checkin 2
- [ ] ET MALWARE Yoyo-DDoS Bot Download and Launch Executable Message From CnC Server
- [ ] ET MALWARE Yoyo-DDoS Bot HTTP Flood Attack Inbound
- [ ] ET MALWARE Win32/Small.gen!AQ Communication with Controller
- [ ] ET MALWARE FAKEAV client requesting image - sector.hdd.png
- [ ] ET MALWARE Daurso Checkin
- [ ] ET MALWARE FAKEAV scanner page enocuntered - .hdd_icon
- [x] ET MALWARE IMDDOS Botnet User-Agent IAMDDOS
- [x] ET MALWARE IMDDOS Botnet User-Agent YTDDOS
- [x] ET MALWARE Meredrop/Nusump Checkin
- [ ] ET MALWARE Downloader.Win32.Zlob.bgs Checkin(2)
- [ ] ET MALWARE Executable Download named to be FQDN
- [x] ET MALWARE Shiz or Rohimafo Reporting Listening Socket to CnC Server
- [ ] ET MALWARE nte Binary Download Attempt (multiple malware variants served)
- [x] ET MALWARE DNSTrojan FakeAV Dropper Activity Observed (2)
- [x] ET MALWARE Zeus Bot Connectivity Check
- [ ] ET MALWARE Yoyo-DDoS Bot Download and Launch Executable Message From CnC Server
- [ ] ET MALWARE Shiz/Rohimafo Binary Download Request
- [x] ET MALWARE carberp check in
- [ ] ET MALWARE Fake AV CnC Checkin cycle_report
- [x] ET MALWARE Xilcter/Zeus related malware dropper reporting in
- [ ] ET MALWARE Win32/Comotor.A!dll Reporting 2
- [ ] ET MALWARE Carberp CnC Reply no tasks
- [ ] ET MALWARE Likely Hostile HTTP Header GET structure
- [ ] ET MALWARE Feodo Banking Trojan Account Details Post
- [x] ET MALWARE Possible Fake AV Checkin
- [ ] ET MALWARE FAKEAV CryptMEN - Landing Page Download Contains .hdd_icon
- [x] ET MALWARE Rogue AV Downloader concat URI
- [x] ET MALWARE Suspicious bot.exe Request
- [x] ET MALWARE Suspicious flash_player.exe Download
- [ ] ET MALWARE FAKEAV Gemini systempack exe download
- [x] ET MALWARE Darkness DDoS Bot Checkin
- [ ] ET MALWARE Win32.Krap.ar Infection URL Request
- [ ] ET MALWARE Trojan.BackDoor-DRV.gen.c Reporting-2
- [ ] ET MALWARE Storm/Waledac 3.0 Checkin 1
- [x] ET MALWARE Potential Blackhole Exploit Pack Binary Load Request
- [ ] ET MALWARE Possible Worm W32.Svich or Other Infection Request for setting.ini
- [x] ET MALWARE Possible Worm W32.Svich or Other Infection Request for setting.doc
- [ ] ET MALWARE Malware Related msndown
- [x] ET MALWARE Winsoft.E Checkin 2
- [x] ET MALWARE Spy Banker Outbound Communication Attempt
- [ ] ET MALWARE FAKEAV Gemini softupdate*.exe download
- [x] ET MALWARE x0Proto Client Info
- [x] ET MALWARE x0Proto Ping
- [x] ET MALWARE W32/Goolbot.E Checkin UA Detected iamx
- [ ] ET MALWARE USPS Inbound SPAM
- [ ] ET MALWARE SpyEye Post_Express_Label ftpgrabber check-in
- [ ] ET MALWARE Win32 Troxen Reporting
- [x] ET MALWARE W32 Bamital or Backdoor.Win32.Shiz CnC Communication
- [ ] ET MALWARE Night Dragon CnC Beacon Inbound
- [x] ET MALWARE Night Dragon CnC Traffic Outbound 2
- [ ] ET MALWARE Night Dragon Dropper Download Command
- [x] ET MALWARE Generic Trojan with /? and Indy Library User-Agent
- [x] ET MALWARE Fake Opera 8.11 UA related to Trojan Activity
- [ ] ET MALWARE IRS Inbound SMTP Malware
- [ ] ET MALWARE Yoyo-DDoS Bot Execute DDoS Command From CnC Server
- [ ] ET MALWARE Yoyo-DDoS Bot Execute SYN Flood Command Message From CnC Server
- [ ] ET MALWARE Yoyo-DDoS Bot HTTP Flood Attack Outbound
- [ ] ET MALWARE FAKEAV landing page - sector.hdd.png no-repeat
- [ ] ET MALWARE Daurso FTP Credential Theft Reported
- [ ] ET MALWARE Antivirus2010 Checkin port 8082
- [x] ET MALWARE IMDDOS Botnet User-Agent STORMDDOS
- [x] ET MALWARE IMDDOS Botnet User-Agent kav
- [x] ET MALWARE IMDDOS Botnet User-Agent i am ddos
- [ ] ET MALWARE Downloader.Win32.Zlob.bgs Checkin(1)
- [ ] ET MALWARE Executable Download named to be .com FQDN
- [x] ET MALWARE Knock.php Shiz or Rohimafo CnC Server Contact URL
- [ ] ET MALWARE JAR Download From Crimepack Exploit Kit
- [x] ET MALWARE DNSTrojan FakeAV Dropper Activity Observed (1)
- [x] ET MALWARE Avzhan DDOS Bot Outbound Hardcoded Malformed GET Request Denial Of Service Attack Detected
- [ ] ET MALWARE Potential-Hiloti/FakeAV site access
- [ ] ET MALWARE Avzhan DDOS Bot Inbound Hardcoded Malformed GET Request Denial Of Service Attack Detected
- [x] ET MALWARE Shiz/Rohimafo Checkin
- [x] ET MALWARE Carberp checkin task
- [x] ET MALWARE MUROFET/Licat Trojan
- [x] ET MALWARE Win32/Comotor.A!dll Reporting 1
- [x] ET MALWARE Carberp file download
- [x] ET MALWARE SpyEye C&C Check-in URI
- [x] ET MALWARE Bredolab CnC URL Detected
- [x] ET MALWARE TDSS/TDL/Alureon MBR rootkit Checkin
- [ ] ET MALWARE FAKEAV Gemini - JavaScript Redirection To Scanning Page
- [ ] ET MALWARE FAKEAV CryptMEN - Random Named DeObfuscation JavaScript File Download
- [x] ET MALWARE X-Tag Zeus Mitmo user agent
- [x] ET MALWARE Ponmocup C2 Post-infection Checkin
- [ ] ET MALWARE Suspicious executable download adobe-flash.v
- [ ] ET MALWARE Suspicious invoice.scr Download Request
- [ ] ET MALWARE Trojan.Spy.YEK MAC and IP POST
- [x] ET MALWARE Trojan.BackDoor-DRV.gen.c Reporting-1
- [ ] ET MALWARE Waledac 2.0/Storm Worm 3.0 GET request detected
- [x] ET MALWARE Storm/Waledac 3.0 Checkin 2
- [x] ET MALWARE Carberp CnC request POST /set/task.html
- [x] ET MALWARE Possible Worm W32.Svich or Other Infection Request for setting.xls
- [ ] ET MALWARE FAKEAV CryptMEN pack.exe Payload Download
- [x] ET MALWARE Winsoft.E Checkin 1
- [x] ET MALWARE Winsoft.E Checkin 3
- [x] ET MALWARE Win32/Banbra Banking Trojan Communication
- [x] ET MALWARE x0Proto Init
- [x] ET MALWARE x0Proto Pong
- [x] ET MALWARE x0Proto Download Cmd
- [ ] ET MALWARE MUROFET/Licat Trojan Checkin Forum
- [ ] ET MALWARE SpyEye HTTP Library Checkin
- [ ] ET MALWARE Spy.Win32.Agent.bijs Reporting 2
- [ ] ET MALWARE Spy.Win32.Agent.bijs Reporting 1
- [x] ET MALWARE Night Dragon CnC Beacon Outbound
- [ ] ET MALWARE Night Dragon CnC Traffic Inbound 2
- [ ] ET MALWARE Night Dragon CMD Shell
- [ ] ET MALWARE Night Dragon Server Auth to Bot
- [x] ET MALWARE Rootkit TDSS/Alureon Checkin 2
- [ ] ET MALWARE FAKEAV download (AntiSpyWareSetup.exe)
- [ ] ET MALWARE IRS Inbound SPAM

- [x] ET MALWARE Possible TDSS User-Agent CMD
- [ ] ET MALWARE Possible Neosploit Toolkit download
- [ ] ET MALWARE Tatanga Checkin
- [x] ET MALWARE Potential FakePAV Checkin
- [ ] ET MALWARE Win32.Vilsel.akd Reporting
- [x] ET MALWARE Downloader.Win32.Banload Reporting
- [ ] ET MALWARE UPS Inbound bad attachment v.6
- [ ] ET MALWARE Possible Eleonore Exploit pack download
- [ ] ET MALWARE Downloader Win32.Agent.FakeAV.AVG 2
- [x] ET MALWARE Possible JKDDOS download ddos.exe
- [ ] ET MALWARE Possible JKDDOS download 1691.exe
- [x] ET MALWARE Possible JKDDOS download cl.exe
- [ ] ET MALWARE DHL Spam Inbound
- [ ] ET MALWARE Excel with Embedded .emf object downloaded
- [x] ET MALWARE Driveby Exploit Attempt Often to Install Monkif
- [ ] ET MALWARE Hiloti loader installed successfully response
- [x] ET MALWARE Hiloti loader requesting payload URL
- [ ] ET MALWARE Generic Win32 Banker Trojan CheckIn
- [ ] ET MALWARE Downloader.small Generic Checkin
- [ ] ET MALWARE Best Spyware Scanner FaveAV Download
- [x] ET MALWARE Slugin.A PatchTimeCheck.dat Request
- [x] ET MALWARE Win32.FakeAV.chhq Checkin
- [ ] ET MALWARE Chinese Bootkit Checkin
- [ ] ET MALWARE Malicious JAR olig
- [x] ET MALWARE SpyEye Checkin version 1.3.25 or later
- [ ] ET MALWARE Win32/Injector.DKUN Variant Response
- [ ] ET MALWARE FakeAV BestAntivirus2011 Download
- [x] ET MALWARE BestAntivirus2011 Fake AV reporting
- [x] ET MALWARE Known Hostile Domain .ntkrnlpa.info Lookup
- [ ] ET MALWARE Trojan-GameThief.Win32.OnLineGames.bnye Checkin
- [x] ET MALWARE Possible Hiloti DNS Checkin Message explorer_exe
- [x] ET MALWARE Ponmocup C2 Sending Data to Controller 1
- [x] ET MALWARE Spoofed MSIE 7 User-Agent Likely Ponmocup
- [x] ET MALWARE Delf Alms backdoor checkin
- [ ] ET MALWARE Trojan-Downloader.Win32.Small Checkin
- [ ] ET MALWARE Vinself Backdoor Checkin
- [ ] ET MALWARE Gozi posting form data
- [x] ET MALWARE JKDDOS Bot CnC Phone Home Message
- [x] ET MALWARE Dropper.Win32.Agent.bpxo Checkin
- [ ] ET MALWARE Backdoor Win32/Begman.A Checkin
- [x] ET MALWARE Generic Dropper/Clicker Checkin
- [ ] ET MALWARE Generic adClicker Checkin
- [x] ET MALWARE Backdoor.Win32.ZZSlash/Redosdru.E checkin
- [ ] ET MALWARE Trojan.Vaklik.kku Checkin Response
- [x] ET MALWARE W32.Qakbot Request for Compromised FTP Sites
- [ ] ET MALWARE W32.Qakbot .cb File Extention FTP Upload
- [x] ET MALWARE Possible FakeAV Binary Download (Security)
- [ ] ET MALWARE WebToolbar.Win32.WhenU.r Reporting
- [x] ET MALWARE DLoader File Download Request Activity
- [x] ET MALWARE DonBot Checkin
- [x] ET MALWARE Possible Tracur.Q HTTP Communication
- [x] ET MALWARE Win32.Meredrop Checkin
- [x] ET MALWARE Zeus Bot GET to Google checking Internet connectivity
- [x] ET MALWARE Backdoor.Win32.DarkComet Keepalive Inbound
- [x] ET MALWARE Win32.Vilsel Checkin
- [ ] ET MALWARE FakeAV FakeAlert.Rena.n Checkin Flowbit set
- [ ] ET MALWARE Backdoor.Win32.Gbod.dv Checkin
- [x] ET MALWARE Gozi Communication 2
- [x] ET MALWARE Trojan-Banker.Win32.Agent Checkin
- [ ] ET MALWARE Backdoor Win32/IRCbot.FJ Cnc connection dns lookup
- [ ] ET MALWARE IRS Inbound SPAM variant 3
- [ ] ET MALWARE USPS SPAM Inbound possible spyeye trojan
- [x] ET MALWARE Suspicious Download Setup_ exe
- [x] ET MALWARE TrojanDownloader Win32/Harnig.gen-P Reporting
- [ ] ET MALWARE Downloader.Win32.Agent.bqkb Reporting
- [ ] ET MALWARE UPS Inbound bad attachment v.5
- [ ] ET MALWARE Post Express Inbound bad attachment
- [ ] ET MALWARE Downloader Win32.Agent.FakeAV.AVG 1
- [ ] ET MALWARE Possible JKDDOS download 500.exe
- [ ] ET MALWARE Possible JKDDOS download desyms.exe
- [ ] ET MALWARE Possible JKDDOS download wm.exe
- [ ] ET MALWARE DHL Spam Inbound
- [ ] ET MALWARE FakeAV InstallInternetDefender Download
- [ ] ET MALWARE Monkif Checkin
- [ ] ET MALWARE Monkif CnC response in fake JPEG
- [x] ET MALWARE Hiloti loader installed successfully request
- [ ] ET MALWARE Win32/Rimecud.B Activity
- [x] ET MALWARE Win32/Virut.BN Checkin
- [x] ET MALWARE BlackshadesRAT Reporting
- [ ] ET MALWARE PWS-Banker.gen.b Reporting
- [ ] ET MALWARE Unknown Malware PatchPathNewS3.dat Request
- [x] ET MALWARE FakeAV Check-in purporting to be MSIE with invalid terse HTTP headers
- [x] ET MALWARE GET to Google with specific HTTP lib likely Cycbot/ Bifrose/Kryptic checking Internet connection
- [ ] ET MALWARE HTTP Request to a Malware Related Numerical .cn Domain
- [ ] ET MALWARE FakeAV InstallInternetProtection Download
- [x] ET MALWARE Internet Protection FakeAV checkin
- [x] ET MALWARE Win32/FakeSysdef Rogue AV Checkin
- [x] ET MALWARE Known Hostile Domain citi-bank.ru Lookup
- [x] ET MALWARE Known Hostile Domain ilo.brenz .pl Lookup
- [x] ET MALWARE Backdoor.Win32.Vertexbot.A User-Agent (VERTEXNET)
- [ ] ET MALWARE DNS Query for Possible FakeAV Domain
- [x] ET MALWARE Ponmocup C2 Sending Data to Controller 2
- [x] ET MALWARE Spoofed MSIE 8 User-Agent Likely Ponmocup
- [ ] ET MALWARE Win32/Rimecud download
- [x] ET MALWARE Backdoor.Win32.Xyligan Checkin
- [ ] ET MALWARE Clicker.Win32.AutoIt.ai Checkin
- [x] ET MALWARE Backdoor.Win32.Poison.AU checkin
- [x] ET MALWARE Known Skunkx DDOS Bot User-Agent Cyberdog
- [x] ET MALWARE Dropper.Win32.Agent.ahju Checkin
- [ ] ET MALWARE Possible TDSS Trojan GET with xxxx_ string
- [x] ET MALWARE Suspicious Email Attachment Possibly Related to Mydoom.L@mm
- [x] ET MALWARE Kazy/Kryptor/Cycbot Trojan Checkin
- [ ] ET MALWARE Trojan.Vaklik.kku Checkin Request
- [x] ET MALWARE W32.Qakbot Update Request
- [x] ET MALWARE W32.Qakbot Webpage Infection Routine POST
- [ ] ET MALWARE W32.Qakbot Seclog FTP Upload
- [x] ET MALWARE Secure-Soft.Stealer Checkin
- [x] ET MALWARE Java EXE Download by Vulnerable Version - Likely Driveby
- [ ] ET MALWARE DLoader PWS Module Data Upload Activity
- [ ] ET MALWARE MacShield FakeAV CnC Communication
- [ ] ET MALWARE Dropper.MSIL.Agent.ate Checkin
- [x] ET MALWARE Large DNS Query possible covert channel
- [x] ET MALWARE Backdoor.Win32.Fynloski.A/DarkRat Checkin Outbound
- [ ] ET MALWARE VBKrypt.cmtp Login to Server
- [ ] ET MALWARE Vilsel.ayjv Checkin (aid)
- [ ] ET MALWARE FakeAV FakeAlertRena.n Checkin Response from Server
- [x] ET MALWARE Generic Bot Checkin
- [x] ET MALWARE Ponmocup Redirection from infected Website to Trojan-Downloader
- [x] ET MALWARE Win32.Renos/Artro Trojan Checkin M1
- [ ] ET MALWARE Unknown Dropper HTTP POST Check-in

- [x] ET MALWARE Win32.Genome Initial Checkin
- [ ] ET MALWARE Trojan/Hacktool.Sniffer Initial Checkin
- [x] ET MALWARE Win32/Rodecap CnC Checkin
- [x] ET MALWARE Win32/Fosniw CnC Checkin Style 2
- [x] ET MALWARE Trojan Internet Connectivity Check
- [x] ET MALWARE Backdoor.Meciv Checkin
- [x] ET MALWARE Win32/Sefnit Initial Checkin
- [ ] ET MALWARE Palevo (OUTBOUND)
- [x] ET MALWARE Ruskill/Palevo CnC PONG
- [x] ET MALWARE Yandexbot Request Outbound
- [ ] ET MALWARE Guagua Trojan Update Checkin
- [x] ET MALWARE DarkComet-RAT init connection
- [x] ET MALWARE DarkComet-RAT Client Keepalive
- [x] ET MALWARE Papras Banking Trojan Checkin
- [ ] ET MALWARE Win32/Cycbot Initial Checkin to CnC
- [x] ET MALWARE Possible Ponmocup Driveby Download
- [ ] ET MALWARE Google Warning Infected Local User
- [ ] ET MALWARE Ruskill CnC Download Command 2
- [x] ET MALWARE FakeAV Landing Page
- [x] ET MALWARE Bifrose Client Checkin
- [ ] ET MALWARE FakeAV/Application JPDesk/Delf checkin
- [x] ET MALWARE Win32.Pamesg/ArchSMS.HL CnC Checkin
- [ ] ET MALWARE Zeus Bot Request to CnC 2
- [ ] ET MALWARE Connectivity Check of Unknown Origin 2
- [x] ET MALWARE Executable Download Purporting to be JavaScript likely 2nd stage Infection
- [ ] ET MALWARE HTran/SensLiceld.A Checkin 2 (unicode)
- [ ] ET MALWARE FakeAV Checkin
- [x] ET MALWARE KeyloggerOnline Keylogger Checkin (sleep)
- [x] ET MALWARE Win32/Oliga Fake User Agent
- [x] ET MALWARE FakeAV User-Agent XML
- [x] ET MALWARE W32/Nolja Trojan User-Agent (FileNolja)
- [x] ET MALWARE Downbot/Shady Rat Remote Shell Connection
- [x] ET MALWARE Fakealert.Rena CnC Checkin 2
- [ ] ET MALWARE W32/Siscos CnC Checkin
- [x] ET MALWARE W32/FakeAlert Fake Security Tool Checkin
- [x] ET MALWARE W32/Hupigon.B User Agent TSDownload
- [ ] ET MALWARE W32/Pandex Trojan Dropper Initial Checkin
- [x] ET MALWARE Backdoor.Win32/Momibot Ping Checkin
- [ ] ET MALWARE Suspicious User Agent ksdl_1_0
- [ ] ET MALWARE FakeAV Landing Page Checking firewall status
- [ ] ET MALWARE FakeAV FakeAlertRena.n Checkin NO Response from Server
- [x] ET MALWARE Win32.Shiz.fxm/Agent-TBT Checkin
- [ ] ET MALWARE W32/DirtJumper CnC Server Providing DDOS Targets
- [x] ET MALWARE W32/Mnless Checkin
- [x] ET MALWARE Win32/TrojanDownloader.Chekafe.D User-Agent my_check_data On Off HTTP Port
- [x] ET MALWARE Troxen Downloader Checkin
- [ ] ET MALWARE Win32/VB.HV Checkin
- [x] ET MALWARE DNS query for Morto RDP worm related domain jaifr.com
- [ ] ET MALWARE DNS query for Morto RDP worm related domain jifr.co.cc
- [ ] ET MALWARE Best Pack Exploit Pack Binary Load Request
- [ ] ET MALWARE DNS query for Morto RDP worm related domain qfsl.co.cc
- [ ] ET MALWARE DNS query for Morto RDP worm related domain jifr.co.be
- [x] ET MALWARE Win32/Dynamer Trojan Dropper User-Agent VB Http
- [x] ET MALWARE W32/Lalus Trojan Downloader User Agent (Message Center)
- [ ] ET MALWARE Win32.Genome Download.php HTTP Request
- [ ] ET MALWARE Trojan/Hacktool.Sniffer Successful Install Message
- [x] ET MALWARE Win32/Fosniw MacTryCnt CnC Style Checkin
- [x] ET MALWARE Win32.FakeAV POST datan.php
- [x] ET MALWARE Backdoor.Esion CnC Checkin
- [x] ET MALWARE Gh0st Remote Access Trojan Encrypted Session To CnC Server
- [ ] ET MALWARE W32/IRCBrute Checkin 2
- [x] ET MALWARE Ruskill/Palevo Download Command
- [x] ET MALWARE Ruskill/Palevo KCIK IRC Command
- [x] ET MALWARE Avzhan DDoS Bot User-Agent MyIE
- [ ] ET MALWARE Win32/Nekill Checkin
- [x] ET MALWARE DarkComet-RAT server join acknowledgement
- [x] ET MALWARE Win32.Jadtre Retrieving Cfg File
- [ ] ET MALWARE Win32/Cycbot Pay-Per-Install Executable Download
- [x] ET MALWARE Win32.Glupteba/ClIEcker CnC Checkin
- [ ] ET MALWARE Phoenix Landing Page Obfuscated Javascript 2
- [ ] ET MALWARE Ruskill CnC Download Command 1
- [ ] ET MALWARE Ruskill Reporting on Local Scans
- [x] ET MALWARE PoisonIvy.E Keepalive to CnC
- [x] ET MALWARE Win32.FakeAV.Rean Checkin
- [x] ET MALWARE Win32/Sisproc Variant POST to CnC Server
- [ ] ET MALWARE PSW.Win32.Ruftar.lon File Stealer FTP File Upload
- [ ] ET MALWARE Connectivity Check of Unknown Origin 1
- [ ] ET MALWARE Connectivity Check of Unknown Origin 3
- [x] ET MALWARE HTran/SensLiceld.A response to infected host
- [ ] ET MALWARE windows_security_update Fake AV download
- [x] ET MALWARE KeyloggerOnline Keylogger Checkin (kill)
- [x] ET MALWARE KeyloggerOnline Keylogger Checkin (go https)
- [x] ET MALWARE FakeAV oms.php Data Post
- [x] ET MALWARE W32/Nolja Trojan Downloader Initial Checkin
- [ ] ET MALWARE W32/Alunik User Agent Detected
- [x] ET MALWARE W32/Sality Executable Pack Digital Signature ASCII Marker
- [ ] ET MALWARE Fakealert.Rena CnC Checkin 1
- [ ] ET MALWARE Accept-encode HTTP header with UA indicating infected host
- [ ] ET MALWARE Suspicious User Agent 3653Client
- [x] ET MALWARE W32/Skintrim CnC Checkin
- [x] ET MALWARE Backdoor.Win32/Momibot Checkin
- [x] ET MALWARE Win32/Winshow User Agent
- [ ] ET MALWARE Bancos.DV MSSQL CnC Connection Outbound
- [ ] ET MALWARE FakeAV FakeAlert.Rena or similar Checkin Flowbit Set 2
- [x] ET MALWARE User-Agent in Referer Field - Likely Malware
- [x] ET MALWARE Dirt Jumper/Russkill3 Checkin
- [x] ET MALWARE EXE Download When Server Claims To Send Audio File - Must Be Win32
- [x] ET MALWARE W32/NetShare User-Agent
- [ ] ET MALWARE Win32/TrojanDownloader.Chekafe.D Initial Checkin
- [x] ET MALWARE NgrBot IRC CnC Channel Join
- [x] ET MALWARE DNS query for Morto RDP worm related domain qfsl.net
- [x] ET MALWARE DNS query for Morto RDP worm related domain jaifr.net
- [x] ET MALWARE Zeus Bot GET to Bing checking Internet connectivity
- [ ] ET MALWARE DNS query for Morto RDP worm related domain qfsl.co.be
- [x] ET MALWARE DNS query for Morto RDP worm related domain jifr.info
- [x] ET MALWARE W32/Badlib Connectivity Check To Department of Defense Intelligence Information Systems
- [x] ET MALWARE W32/Lalus Trojan Downloader Checkin
- [ ] ET MALWARE Win32/CazinoSilver Checkin

- [ ] ET MALWARE W32/Bancos Reporting
- [ ] ET MALWARE Potential DNS Command and Control via TXT queries
- [x] ET MALWARE Driveby Loader Request List.php
- [ ] ET MALWARE Spyeye Data Exfiltration 0
- [ ] ET MALWARE Spyeye Data Exfiltration 2
- [ ] ET MALWARE Spyeye Data Exfiltration 4
- [ ] ET MALWARE Spyeye Data Exfiltration 6
- [ ] ET MALWARE Spyeye Data Exfiltration 8
- [ ] ET MALWARE Backdoor.Win32.Fynloski.A Command Request
- [x] ET MALWARE VirTool.Win32/VBInject.gen!DM Checkin
- [ ] ET MALWARE BKDR_BTMINE.MNR BitCoin Miner Retrieving New IP Addresses From Server
- [x] ET MALWARE BKDR_BTMINE.MNR BitCoin Miner Server Checkin
- [ ] ET MALWARE TROJ_VB.FJP Generic Dowbnloader Connectivity Check to Google
- [ ] ET MALWARE Win32.Unknown.UDP.edsm CnC traffic
- [ ] ET MALWARE Potentially Unwanted Program Storm3-607.exe Download Reporting
- [x] ET MALWARE Shady RAT Put File Command
- [x] ET MALWARE Shady RAT Relay Command
- [ ] ET MALWARE Unknown Exploit Pack Binary Load Request (server_privileges.php)
- [x] ET MALWARE Win32.Riberow.A (mkdir)
- [ ] ET MALWARE Win32.Riberow.A (touch)
- [ ] ET MALWARE Win32.Parite Checkin SQL Database
- [ ] ET MALWARE ZeroAccess/Max++ Rootkit C&C Activity 2
- [x] ET MALWARE Shylock Module Server Response
- [x] ET MALWARE Trojan Downloader User-Agent (NOPE)
- [x] ET MALWARE Trojan Downloader User-Agent (Tiny)
- [x] ET MALWARE Suspicious User-Agent (WindowsNT) With No Separating Space
- [x] ET MALWARE Win32/OnLineGames GetMyIP Style Checkin
- [ ] ET MALWARE Zeus/Aeausuc P2P Variant Retrieving Peers List
- [ ] ET MALWARE Double HTTP/1.1 Header Outbound - Likely Infected or Hostile Traffic
- [x] ET MALWARE Backdoor.Win32.Aldibot.A Checkin
- [ ] ET MALWARE Possible German Governmental Backdoor/R2D2.A 2
- [ ] ET MALWARE Bundestrojaner (W32/R2D2 BTrojan) Outbound SRV-1
- [ ] ET MALWARE W32/Einstein CnC Checkin
- [ ] ET MALWARE Backdoor.Win32.Prosti Checkin
- [x] ET MALWARE Win32.Cerberus RAT Checkin Outbound
- [x] ET MALWARE Win32.Cerberus RAT Client pong
- [ ] ET MALWARE Win32.Scar.dvov Searchstar.co.kr related Checkin
- [x] ET MALWARE Zentom FakeAV Checkin
- [ ] ET MALWARE Dropper.Win32.Npkon Client Checkin
- [x] ET MALWARE Bifrose/Cycbot Checkin
- [ ] ET MALWARE Win32.Trojan.SuspectCRC FakeAV Checkin
- [x] ET MALWARE Jorik FakeAV GET
- [x] ET MALWARE Tatanga/Win32.Kexject.A Checkin
- [ ] ET MALWARE SecurityDefender exe Download Likely FakeAV Install
- [x] ET MALWARE Kazy/Kryptor/Cycbot Trojan Checkin 2
- [x] ET MALWARE W32/Fullstuff Initial Checkin
- [x] ET MALWARE Backdoor.Win32.Svlk Client Checkin
- [ ] ET MALWARE Backdoor.Win32.Svlk Client Ping
- [ ] ET MALWARE Suspicious User Agent GeneralDownloadApplication
- [ ] ET MALWARE Suspicious User Agent GetFile
- [ ] ET MALWARE Suspicious User Agent banderas
- [x] ET MALWARE P2P Zeus or ZeroAccess Request To CnC
- [x] ET MALWARE Request for utu.dat Likely Ponmocup checkin
- [ ] ET MALWARE PoisonIvy.Emp Keepalive to CnC
- [ ] ET MALWARE PoisonIvy.Eu3 Keepalive to CnC
- [x] ET MALWARE Win32.Fareit.A/Pony Downloader Checkin
- [x] ET MALWARE FakeAV.EGZ Checkin 1
- [ ] ET MALWARE Potential DNS Command and Control via TXT queries
- [x] ET MALWARE TR/Spy.Gen checkin via dns ANY query
- [ ] ET MALWARE Driveby Loader Request sn.php
- [ ] ET MALWARE Spyeye Data Exfiltration 1
- [ ] ET MALWARE Spyeye Data Exfiltration 3
- [ ] ET MALWARE Spyeye Data Exfiltration 5
- [ ] ET MALWARE Spyeye Data Exfiltration 7
- [ ] ET MALWARE Spyeye Data Exfiltration 9
- [ ] ET MALWARE Backdoor.Win32.Fynloski.A Command Response
- [x] ET MALWARE BKDR_BTMINE.MNR BitCoin Miner Retrieving Server IP Addresses
- [x] ET MALWARE BKDR_BTMINE.MNR BitCoin Miner Retrieving New Malware From Server
- [x] ET MALWARE W32/iGrabber Info Stealer FTP Upload
- [x] ET MALWARE W32/Gagolino Banking Trojan Reporting to CnC
- [ ] ET MALWARE Fivfrom Downloader (Unitrix)
- [x] ET MALWARE Shady RAT Get File Command
- [x] ET MALWARE Shady RAT Retrieve and Execute Command
- [x] ET MALWARE Shady RAT Send Status Result
- [x] ET MALWARE Win32.Riberow.A (listdir)
- [x] ET MALWARE Win32.Riberow.A (fsize)
- [x] ET MALWARE Win32.Riberow.A (postit3)
- [x] ET MALWARE ZeroAccess/Max++ Rootkit C&C Activity 1
- [x] ET MALWARE Shylock Module Data POST
- [ ] ET MALWARE Agent-TMF Checkin
- [x] ET MALWARE Trojan Downloader User-Agent BGroom
- [ ] ET MALWARE Win32/Wapomi.AD Variant Checkin
- [ ] ET MALWARE Win32/Daemonize Trojan Proxy Initial Checkin
- [x] ET MALWARE Suspicious User-Agent (GenericHttp/VER_STR_COMMA)
- [x] ET MALWARE Trojan-Dropper.Win32.StartPage.dvm or Mebromi Bios Rootkit CnC Count Checkin
- [x] ET MALWARE Backdoor.Win32.Aldibot.A User-Agent (Aldi Bot)
- [ ] ET MALWARE Possible German Governmental Backdoor/R2D2.A 1
- [ ] ET MALWARE Bundestrojaner (W32/R2D2 BTrojan) Inbound SRV-1
- [ ] ET MALWARE Win32.Swisyn Reporting
- [ ] ET MALWARE Win32.Dropper.Wlock Checkin
- [ ] ET MALWARE USPS Spam/Trojan Executable Download
- [x] ET MALWARE Win32.Cerberus RAT Checkin Response
- [x] ET MALWARE Win32.Cerberus RAT Server ping
- [ ] ET MALWARE W32.Duqu UA and Filename Requested
- [x] ET MALWARE Cnzz.cn Related Dropper Checkin
- [ ] ET MALWARE Dropper.Win32.Npkon Server Responce
- [x] ET MALWARE Win32.PEx.Delphi.1151005043 Post-infection Checkin
- [x] ET MALWARE Cycbot POST
- [x] ET MALWARE Dooptroop Dropper Checkin
- [ ] ET MALWARE Trojan.Kryptik/proscan.co.kr Checkin
- [x] ET MALWARE AntiVirus exe Download Likely FakeAV Install
- [ ] ET MALWARE Win32/Sefbov.E Reporting
- [ ] ET MALWARE W32/Koobface Variant Initial Checkin
- [ ] ET MALWARE Backdoor.Win32.Svlk Server Reply
- [ ] ET MALWARE W32/Yaq Checkin
- [ ] ET MALWARE Win32.BlackControl Retrieving IP Information
- [ ] ET MALWARE W32/Rimecud User Agent beat
- [x] ET MALWARE ZAccess/Sirefef/MAX++/Jorik/Smadow Checkin
- [ ] ET MALWARE P2P Zeus Response From CnC
- [x] ET MALWARE Win32/Dofoil.L Checkin
- [ ] ET MALWARE PoisonIvy.Eu2 Keepalive to CnC
- [ ] ET MALWARE PoisonIvy.Eu4 Keepalive to CnC
- [ ] ET MALWARE Win32.Zbot.chas/Unruy.H Covert DNS CnC Channel TXT Response
- [x] ET MALWARE FakeAV.EGZ Checkin 2

- [ ] ET MALWARE PWS.TIBIA Checkin or Data Post
- [ ] ET MALWARE Win32/Rimecud.A User-Agent (needit)
- [ ] ET MALWARE Win32/Rimecud.A User-Agent (counters)
- [x] ET MALWARE Win32.Sality User-Agent (DEBUT.TMP)
- [x] ET MALWARE Suspicious UA Mozilla / 4.0
- [ ] ET MALWARE TDSS DNS Based Internet Connectivity Check
- [x] ET MALWARE W32/Kazy User-Agent (Windows NT 5.1 \; v.) space infront of semi-colon
- [ ] ET MALWARE VBKrypt.dytr Checkin
- [x] ET MALWARE Backdoor.Win32.Sykipot Put
- [x] ET MALWARE Smokeloader getgrab Command
- [x] ET MALWARE Smokeloader getsock Command
- [ ] ET MALWARE Zeus Checkin Header Pattern
- [ ] ET MALWARE Gootkit Scanner User-Agent Outbound
- [ ] ET MALWARE Agent.UGP!tr/Cryptor/Graftor Dropper Requesting exe
- [ ] ET MALWARE SpyEye Checkin version 1.3.25 or later 2
- [ ] ET MALWARE Win32/Hilgild!gen.A CnC Communication
- [ ] ET MALWARE PoisonIvy.Eu5 Keepalive from CnC
- [x] ET MALWARE Trojan Downloader.Bancos Reporting
- [ ] ET MALWARE TROJAN Win32.OnlineGames.Bft Reporting
- [x] ET MALWARE Suspicious user agent (V32)
- [x] ET MALWARE Blackshades Payload Download Command
- [ ] ET MALWARE Zeus POST Request to CnC - cookie variation
- [x] ET MALWARE Win32.UFRStealer.A issuing MKD command FTP
- [ ] ET MALWARE Win32/Injector.MUD Variant Reporting
- [ ] ET MALWARE Delf/Troxen/Zema Reporting 2
- [ ] ET MALWARE Cythosia V2 DDoS WebPanel Hosted Locally
- [x] ET MALWARE Win32/Nuclear Checkin
- [ ] ET MALWARE Zeus/Reveton checkin to /images.rar
- [ ] ET MALWARE PoisonIvy.Ehy Keepalive to CnC
- [ ] ET MALWARE Suspicious executable download possible Trojan NgrBot
- [x] ET MALWARE Bifrose/Cycbot Checkin 2
- [x] ET MALWARE Suspicious User-Agent MyAgrent
- [ ] ET MALWARE W32/Mentory CnC Server Providing File Info Details
- [x] ET MALWARE Win32/Cryptrun.B Connectivity check
- [x] ET MALWARE Win32.MSUpdater C&C traffic GET
- [x] ET MALWARE W32/VPEYE Trojan Downloader User-Agent (VP-EYE Downloader)
- [ ] ET MALWARE TLD4 Purple Haze Variant Initial CnC Request for Ad Servers
- [ ] ET MALWARE Sykipot SSL Certificate subject emailAddress detected
- [x] ET MALWARE MSUpdater POST checkin to CnC
- [ ] ET MALWARE Delf/Troxen/Zema controller responding to client
- [x] ET MALWARE Zeus POST Request to CnC sk1 and bn1 post parameters
- [ ] ET MALWARE QDIGIT Trojan Protocol detected
- [ ] ET MALWARE UPDATE Protocol Trojan Communication detected on non-http ports
- [x] ET MALWARE IP2B Trojan Communication Protocol detected
- [x] ET MALWARE Backdoor Win32.Idicaf/Atraps
- [ ] ET MALWARE Karagany/Kazy Obfuscated Payload Download
- [x] ET MALWARE UPDATE Protocol Trojan Communication detected on http ports 2
- [x] ET MALWARE W32.Duptwux/Ganelp FTP Username - onthelinux
- [ ] ET MALWARE Sefnit Checkin 5
- [ ] ET MALWARE Trojan.Win32.NfLog Checkin (TTip)
- [x] ET MALWARE Backdoor.Win32.RShot Checkin
- [x] ET MALWARE Backdoor.Win32.RShot Ping Outbound
- [x] ET MALWARE Win32/Cutwail.BE Checkin 2
- [ ] ET MALWARE W32/Rovnix Downloading Config File From CnC
- [ ] ET MALWARE PWS.TIBIA Checkin or Data Post 2
- [ ] ET MALWARE TR/Rimecud.aksa User-Agent (indy)
- [ ] ET MALWARE Win32/Rimecud.A User-Agent (giftz)
- [ ] ET MALWARE Win32.Sality User-Agent (Internet Explorer 5.01)
- [ ] ET MALWARE Zeus POST Request to CnC - URL agnostic
- [ ] ET MALWARE W32/Jorik DDOS Instructions From CnC Server
- [x] ET MALWARE Fake Variation of Mozilla 4.0 - Likely Trojan
- [x] ET MALWARE Backdoor.Win32.Sykipot Checkin
- [x] ET MALWARE Backdoor.Win32.Sykipot Get Config Request
- [x] ET MALWARE Smokeloader getproxy Command
- [x] ET MALWARE Smokeloader getload Command
- [x] ET MALWARE Gootkit Checkin User-Agent 2
- [ ] ET MALWARE Likely CryptMEN FakeAV Download vclean
- [ ] ET MALWARE Win32.PowerPointer checkin
- [x] ET MALWARE Double HTTP/1.1 Header Inbound - Likely Hostile Traffic
- [ ] ET MALWARE PoisonIvy.Eu5 Keepalive to CnC
- [ ] ET MALWARE Trojan-Clicker.Win32.VB.gnf Reporting
- [x] ET MALWARE Trojan.Win32.A.FakeAV Reporting
- [x] ET MALWARE TROJAN Win32-WebSec Reporting
- [ ] ET MALWARE Downloader.Win32.Nurech Checkin UA
- [ ] ET MALWARE Zeus Bot GET to Google checking Internet connectivity using proxy
- [ ] ET MALWARE PoisonIvy.Eu6 Keepalive to CnC
- [x] ET MALWARE Dooptroop CnC Beacon
- [ ] ET MALWARE Delf/Troxen/Zema Reporting 1
- [x] ET MALWARE Suspicious User-Agent build - possibly Delf/Troxen/Zema
- [x] ET MALWARE W32/Lici Initial Checkin
- [x] ET MALWARE W32/Jiwerks.A Checkin
- [x] ET MALWARE Query to Known CnC Domain msnsolution.nicaze.net
- [ ] ET MALWARE Win32/Spy.Banker Reporting Via SMTP
- [ ] ET MALWARE Gozi Checkin to CnC
- [x] ET MALWARE W32/DelfInject.A CnC Checkin 2
- [x] ET MALWARE W32/Mentory CnC Server Providing Update Details
- [ ] ET MALWARE TROJAN ClickCounter Connectivity Check
- [x] ET MALWARE Win32/Cryptrun.B/MSUpdater C&C traffic 1
- [x] ET MALWARE W32/118GotYourNo Reporting to CnC
- [ ] ET MALWARE Dapato/Cleaman Checkin
- [ ] ET MALWARE Sykipot SSL Certificate serial number detected
- [x] ET MALWARE MSUpdater alt checkin to CnC
- [x] ET MALWARE MSUpdater Connectivity Check to Google
- [ ] ET MALWARE Delf/Troxen/Zema controller delivering clickfraud instructions
- [ ] ET MALWARE TSPY_SPCESEND.A Checkin
- [ ] ET MALWARE UPDATE Protocol Trojan Communication detected on http ports
- [x] ET MALWARE LURK Trojan Communication Protocol detected
- [x] ET MALWARE BB Trojan Communication Protocol detected
- [ ] ET MALWARE NfLog Checkin
- [x] ET MALWARE UPDATE Protocol Trojan Communication detected on non-http ports 2
- [x] ET MALWARE Fareit/Pony Downloader Checkin 3
- [ ] ET MALWARE Sefnit Checkin 4
- [ ] ET MALWARE W32/Pasta.IK Checkin
- [x] ET MALWARE Query for Known Hostile *test.3322.org.cn Domain
- [x] ET MALWARE Backdoor.Win32.RShot HTTP Checkin
- [x] ET MALWARE Win32/Cutwail.BE Checkin 1
- [x] ET MALWARE W32/Rovnix Activity
- [x] ET MALWARE Trustezeb Checkin to CnC

- [x] ET MALWARE Java Archive sent when remote host claims to send an image
- [x] ET MALWARE Smart Fortress FakeAV/Kryptik.ABNC Checkin
- [x] ET MALWARE W32/Koobface Variant Checkin Attempt
- [x] ET MALWARE W32/Backdoor.BlackMonay Checkin
- [ ] ET MALWARE W32/LockScreen Scareware Geolocation Request
- [x] ET MALWARE W32/NSIS.TrojanDownloader Second Stage Download Instructions from Server
- [x] ET MALWARE Kelihos/Hlux GET jucheck.exe from CnC
- [x] ET MALWARE Yayih.A Checkin
- [x] ET MALWARE W32/Coced.PasswordStealer User-Agent 5.0
- [ ] ET MALWARE RevProxy ClientHello
- [ ] ET MALWARE W32/ProxyChanger.InfoStealer Checkin
- [ ] ET MALWARE Backdoor.Win32.Riern.K Checkin Off Port
- [ ] ET MALWARE Win32/Protux.B Download Update
- [ ] ET MALWARE W32.Blocker Checkin
- [x] ET MALWARE Suspicious User-Agent (Post)
- [x] ET MALWARE Possible Zeus .ru CnC Domain Generation Algorithm (DGA) Lookup Detected
- [ ] ET MALWARE Trojan-Spy.Win32.Zbot.djrm Checkin
- [x] ET MALWARE FakeAV.dfze/FakeAV!IK Checkin
- [x] ET MALWARE Fareit/Pony Downloader Checkin 2
- [ ] ET MALWARE Infostealer.Banprox Proxy.pac Download
- [x] ET MALWARE IRC Bot Download http Command
- [ ] ET MALWARE DwnLdr-JMZ Downloading Binary
- [ ] ET MALWARE Win32.Datamaikon Checkin
- [x] ET MALWARE Win32.Datamaikon Checkin myAgent
- [ ] ET MALWARE HTTP Request to Zaletelly CnC Domain atserverxx.info
- [x] ET MALWARE OSX/Flashback.K/I reporting successful infection
- [x] ET MALWARE OSX/Flashback.K/I reporting failed infection
- [ ] ET MALWARE W32/Taidoor.Backdoor Command Request CnC Checkin
- [x] ET MALWARE Metasploit Meterpreter stdapi_* Command Request
- [x] ET MALWARE Metasploit Meterpreter stdapi_* Command Response
- [x] ET MALWARE OSX/Flashback.K/I User-Agent
- [x] ET MALWARE Pony Downloader HTTP Library MSIE 5 Win98
- [x] ET MALWARE OS X Backdoor Checkin
- [ ] ET MALWARE HTTP Request to a known malware domain (regicsgf.net)
- [x] ET MALWARE DNS Query for a known malware domain (sektori.org)
- [ ] ET MALWARE Win32.Winwebsec.B Checkin
- [x] ET MALWARE Hoax.Win32.BadJoke/DownLoader1.57593 Checkin
- [x] ET MALWARE Mac Flashback Checkin 1
- [ ] ET MALWARE Mac Flashback Checkin 3
- [x] ET MALWARE Win32/Nitol.B Checkin
- [x] ET MALWARE W32/Downvision.A Initial Checkin
- [x] ET MALWARE Jembot PHP Webshell (system command)
- [ ] ET MALWARE W32/Sogu Remote Access Trojan Social Media Embedded CnC Channel
- [ ] ET MALWARE FireEye.STX RAT Checkin
- [x] ET MALWARE Possible Variant.Kazy.53640 Malformed Client Hello SSL 3.0 (Cipher_Suite length greater than Client_Hello Length)
- [ ] ET MALWARE Maljava Dropper for Windows
- [x] ET MALWARE ConstructorWin32/Agent.V
- [ ] ET MALWARE W32/SpyBanker Infection Confirmation Email
- [ ] ET MALWARE W32/Simbot.Backdoor Checkin
- [ ] ET MALWARE Boatz Checkin
- [x] ET MALWARE Backdoor.Win32.PEx.942728546 Checkin
- [ ] ET MALWARE Win32/Kryptik.ABUD Checkin
- [x] ET MALWARE W32/TCYWin.Downloader User-Agent
- [ ] ET MALWARE W32/SelfStarterInternet.InfoStealer Checkin
- [x] ET MALWARE RegSubsDat Checkin
- [ ] ET MALWARE ZeuS Clickfraud List Delivered To Client
- [x] ET MALWARE Trojan.Win32.Genome.aetqe Checkin
- [x] ET MALWARE SMTP Subject Line Contains C Path and EXE Possible Trojan Reporting Execution Path/Binary Name
- [ ] ET MALWARE Peed Checkin
- [x] ET MALWARE W32/SCKeyLog.InfoStealer Installation Confirmation Via SMTP
- [ ] ET MALWARE W32/Kazy Checkin
- [x] ET MALWARE Win32/Protux.B POST checkin
- [x] ET MALWARE Lookup of Algorithm Generated Zeus CnC Domain (DGA)
- [x] ET MALWARE Backdoor.Graybird Checkin
- [x] ET MALWARE W32/GamesForum.InfoStealer Reporting to CnC
- [ ] ET MALWARE Generic Dropper User-Agent (XXXwww)
- [ ] ET MALWARE Cridex.B/Feodo Checkin
- [x] ET MALWARE Backdoor.Win32.Ixeshe
- [ ] ET MALWARE SpyEye Checkin version 1.3.25 or later 3
- [ ] ET MALWARE FakeAV Landing Page - Initializing Protection System
- [x] ET MALWARE LuckyCat/TROJ_WIMMIE Checkin
- [ ] ET MALWARE DwnLdr-JMZ Downloading Binary 2
- [ ] ET MALWARE Win32.Datamaikon Checkin NewAgent
- [ ] ET MALWARE HTTP Request to Zaletelly CnC Domain zaletellyxx.be
- [x] ET MALWARE DNS Request for Zaletelly CnC Domain
- [x] ET MALWARE OSX/Flashback.K/I reporting successful infection 2
- [x] ET MALWARE OSX/Flashback.K first execution checkin
- [x] ET MALWARE W32/Taidoor.Backdoor CnC Checkin With Default Substitute MAC Address Field
- [x] ET MALWARE Metasploit Meterpreter core_channel_* Command Request
- [x] ET MALWARE Metasploit Meterpreter core_channel_* Command Response
- [ ] ET MALWARE Modified Metasploit Jar
- [x] ET MALWARE Pony Downloader check-in response STATUS-IMPORT-OK
- [x] ET MALWARE W32/UltimateDefender.FakeAV Checkin
- [ ] ET MALWARE DNS Query for a known malware domain (regicsgf.net)
- [ ] ET MALWARE Italian Spam Campaign ZIP with EXE Containing Many Underscores
- [x] ET MALWARE Likely Infected HTTP POST to PHP with User-Agent of HTTP Client
- [x] ET MALWARE FlashBack Mac OSX malware Checkin
- [x] ET MALWARE Mac Flashback Checkin 2
- [x] ET MALWARE Win32/Nitol.A Checkin
- [x] ET MALWARE Trojan.Win32.Yakes.pwo Checkin
- [x] ET MALWARE Jembot PHP Webshell (file upload)
- [ ] ET MALWARE Win32/Usteal.B Checkin
- [ ] ET MALWARE PoisonIvy.Es11 Keepalive to CnC
- [x] ET MALWARE Possible Variant.Kazy.53640 Malformed Client Hello SSL 3.0 (Session_Id length greater than Client_Hello Length)
- [x] ET MALWARE FakeM RAT CnC Beacon
- [ ] ET MALWARE Maljava Dropper for OS X
- [x] ET MALWARE Win32/Ponmocup.A Checkin
- [ ] ET MALWARE W32/Backdoor.BAT.Agent.W User Botnet
- [ ] ET MALWARE W32/Downloader/Agent.dxh.1 Reporting to CnC
- [x] ET MALWARE Medfos/Midhos Checkin

- [ ] ET MALWARE Suspicious Icon http header in response seen with Medfos/Midhos downloader
- [ ] ET MALWARE Snap Bot Checkin
- [ ] ET MALWARE Snap Bot Receiving DDoS Command
- [x] ET MALWARE W32/Mepaow.Backdoor Initial Checkin to Intermediary Pre-CnC
- [x] ET MALWARE Win32/Comrerop Checkin to FTP server
- [ ] ET MALWARE Trojan.BAT.Qhost Response from Controller
- [x] ET MALWARE W32/SpyBanker Infection Confirmation Email 2
- [x] ET MALWARE Bebloh connectivity check
- [ ] ET MALWARE W32/Syndicasec.Backdoor Client POST CMD result
- [x] ET MALWARE VBS/Wimmie.A Set
- [ ] ET MALWARE Unknown java_ara Bin Download
- [x] ET MALWARE W32/Renos.Downloader User Agent zeroup
- [x] ET MALWARE Possible SKyWIper/Win32.Flame POST
- [ ] ET MALWARE Possible Feodo/Cridex Traffic Detected
- [ ] ET MALWARE Flamer WuSetupV module traffic 2
- [x] ET MALWARE FakeAvCn-A Checkin 3
- [ ] ET MALWARE Self Signed SSL Certificate (Reaserch)
- [x] ET MALWARE W32/Bakcorox.A ProxyBot CnC Server Connection
- [ ] ET MALWARE Win32/Bicololo.Dropper ne_unik CnC Server Response
- [ ] ET MALWARE Capfire4 Checkin (update machine status)
- [x] ET MALWARE Backdoor Win32/Hupigon.CK Server Checkin
- [x] ET MALWARE Backdoor Win32/Hupigon.CK Server Idle
- [x] ET MALWARE W32/Nutiliers.A Downloader CnC Checkin - Request Encrypted Response
- [x] ET MALWARE Zbot CnC POST /common/versions.php
- [x] ET MALWARE Zbot CnC POST /common/timestamps.php
- [ ] ET MALWARE Pushbot server response
- [x] ET MALWARE W32/Numnet.Downloader CnC Checkin 1
- [ ] ET MALWARE W32/Zusy Gettime Checkin
- [x] ET MALWARE Cridex Post to CnC
- [x] ET MALWARE Win32/Pift Checkin 1
- [x] ET MALWARE Win32/Pift DNS TXT CnC Lookup ppift.net
- [x] ET MALWARE ZeroAccess Outbound udp traffic detected
- [ ] ET MALWARE ProxyBox -ProxyBotCommand - CHECK_ME
- [x] ET MALWARE ProxyBox - HTTP CnC - POST 1-letter.php
- [x] ET MALWARE ProxyBox - HTTP CnC - get_servers.php
- [x] ET MALWARE ProxyBox - ProxyBotCommand - I_AM
- [x] ET MALWARE Urlzone/Bebloh/Bublik Checkin /was/vas.php
- [ ] ET MALWARE Pakes2 - Server Hello
- [ ] ET MALWARE Pakes2 - Checkin - /test.php
- [ ] ET MALWARE HTTP Request to RunForestRun DGA Domain 16-alpha.waw.pl
- [ ] ET MALWARE Generic - ProxyJudge Reverse Proxy Scoring Activity
- [ ] ET MALWARE Karagany checkin (sid5 2)
- [ ] ET MALWARE Trojan Cridex checkin
- [x] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL certificate detected (Likely Shylock/URLzone/Gootkit/Zeus Panda C2)
- [x] ET MALWARE W32/Lile.A DoS Outbound
- [ ] ET MALWARE FinFisher Malware Connection Initialization
- [ ] ET MALWARE DNS Query Gauss Domain *.gowin7.com
- [x] ET MALWARE DNS Query Gauss Domain *.bestcomputeradvisor.com
- [ ] ET MALWARE DNS Query Gauss Domain *.dataspotlight.net
- [ ] ET MALWARE DOCHTML C&C http directive in HTML comments
- [ ] ET MALWARE DNS Query Gauss Domain *.datajunction.org
- [ ] ET MALWARE Shamoon/Wiper/DistTrack Checkin
- [ ] ET MALWARE Rogue.Win32/Winwebsec Install
- [ ] ET MALWARE NeoSploit - Version Enumerated - Java
- [x] ET MALWARE Trojan.JS.QLP Checkin
- [x] ET MALWARE Mirage Campaign checkin
- [ ] ET MALWARE DNS Query to Unknown CnC DGA Domain palauone.com 09/20/12
- [x] ET MALWARE Smoke Loader Checkin r=gate
- [ ] ET MALWARE Snap Bot Receiving Download Command
- [x] ET MALWARE Win32.HLLW.Autoruner USA_Load UA
- [ ] ET MALWARE W32/HupigonUser.Backdoor Rabclib UA Checkin
- [ ] ET MALWARE Trojan.BAT.Qhost - SET
- [ ] ET MALWARE W32/Votwup.Backdoor Checkin
- [ ] ET MALWARE Kazy/Kryptic Checkin with Opera/9 User-Agent
- [x] ET MALWARE Win32/MultiPasswordRecovery.A cs-crash PWS
- [ ] ET MALWARE ZeuS Ransomware win_unlock
- [ ] ET MALWARE VBS/Wimmie.A Checkin
- [x] ET MALWARE Rogue.Win32/Winwebsec Install 2
- [ ] ET MALWARE Possible SKyWIper/Win32.Flame UA
- [ ] ET MALWARE Virus.Win32.Sality.aa Checkin
- [ ] ET MALWARE Flamer WuSetupV module traffic 1
- [x] ET MALWARE FakeAvCn-A Checkin 1
- [ ] ET MALWARE W32.Gimemo/Aldibot CnC POST
- [ ] ET MALWARE Self Signed SSL Certificate (John Doe)
- [ ] ET MALWARE Unknown Java Malicious Jar /eeltff.jar
- [x] ET MALWARE Capfire4 Checkin (register machine)
- [x] ET MALWARE Backdoor Win32/Hupigon.CK Client Checkin
- [ ] ET MALWARE Backdoor Win32/Hupigon.CK Client Idle
- [ ] ET MALWARE W32/Scar CnC Checkin
- [x] ET MALWARE W32/Armageddon CnC Checkin
- [x] ET MALWARE Zbot CnC GET /lost.dat
- [ ] ET MALWARE Pushbot User-Agent
- [ ] ET MALWARE W32/Icoo CnC Checkin
- [x] ET MALWARE W32/Numnet.Downloader CnC Checkin 2
- [ ] ET MALWARE Incognito - Malicious PDF Requested - /getfile.php
- [x] ET MALWARE Generic - 8Char.JAR Naming Algorithm
- [x] ET MALWARE Win32/Pift Checkin 2
- [x] ET MALWARE ZeroAccess udp traffic detected
- [ ] ET MALWARE W32/OnlineGame.DaGame Variant CnC Checkin
- [x] ET MALWARE ProxyBox - HTTP CnC - .com.tw/check_version.php
- [x] ET MALWARE ProxyBox - HTTP CnC - getiplist.php
- [x] ET MALWARE ProxyBox - HTTP CnC - botinfo.php
- [ ] ET MALWARE ProxyBox - ProxyBotCommand - FORCE_AUTHENTICATION*
- [ ] ET MALWARE .HTM being served from WP 1-flash-gallery Upload DIR (likely malicious)
- [x] ET MALWARE Lethic - Client Alive
- [ ] ET MALWARE Win32.Agent2.fher Related User-Agent (Microsoft Internet Updater)
- [ ] ET MALWARE DNS Query to RunForestRun DGA Domain 16-alpha.waw.pl
- [ ] ET MALWARE Karagany checkin (sid5 1)
- [ ] ET MALWARE ZeroAccess HTTP GET request
- [ ] ET MALWARE Pakes2 - EXE Download Request
- [x] ET MALWARE Trojan.Win32.Jorik.Totem.vg HTTP request
- [ ] ET MALWARE MP-FormGrabber Checkin
- [x] ET MALWARE FinFisher Malware Connection Handshake
- [ ] ET MALWARE DNS Query Gauss Domain *.secuurity.net
- [ ] ET MALWARE DNS Query Gauss Domain *.dotnetadvisor.info
- [x] ET MALWARE DNS Query Gauss Domain *.guest-access.net
- [ ] ET MALWARE Smardf/Boaxxe GET to cc.php3
- [x] ET MALWARE Urlzone/Bebloh/Bublik Checkin /was/uid.php
- [ ] ET MALWARE Backdoor.Briba Checkin
- [x] ET MALWARE Possible Metasploit Java Payload
- [ ] ET MALWARE NeoSploit - Version Enumerated - null
- [ ] ET MALWARE Dapato Checkin 8
- [ ] ET MALWARE SSL Cert Used In Unknown Exploit Kit
- [ ] ET MALWARE DNS Query to Unknown CnC DGA Domain traindiscover.com 09/20/12

- [ ] ET MALWARE DNS Query to Unknown CnC DGA Domain manymanyd.com 09/20/12
- [x] ET MALWARE ZeroAccess Checkin
- [ ] ET MALWARE DNS Query to Unknown CnC DGA Domain sleeveblouse.com 09/20/12
- [ ] ET MALWARE DNS Query to Unknown CnC DGA Domain (adbullion .com) 09/26/12
- [ ] ET MALWARE Fake Anti-Hacking Tool
- [x] ET MALWARE Trojan Downloader GetBooks UA
- [x] ET MALWARE Ransom.Win32.Birele.gsg Checkin
- [x] ET MALWARE Win32.Fareit.A/Pony Downloader Checkin (2)
- [ ] ET MALWARE Mini-Flame v 4.x C2 HTTP request
- [x] ET MALWARE Backdoor.Win32.Pushdo.s Checkin
- [x] ET MALWARE DNS Query Sinkhole Domain Various Families (Possible Infected Host)
- [ ] ET MALWARE GeckaSeka User-Agent
- [ ] ET MALWARE Zeus/Citadel Control Panel Access (Inbound)
- [ ] ET MALWARE Citadel API Access IFramer Controller (Inbound)
- [ ] ET MALWARE Citadel API Access VNC Controller (Inbound)
- [ ] ET MALWARE Citadel API Access Bot Controller (Inbound)
- [ ] ET MALWARE Smoke Loader C2 Response
- [x] ET MALWARE Georgian Targeted Attack - Trojan Checkin
- [x] ET MALWARE Georbot initial checkin
- [x] ET MALWARE System Progressive Detection FakeAV (INTEL)
- [x] ET MALWARE Potentially Unwanted Program RebateInformerSetup.exe Download Reporting
- [ ] ET MALWARE Backdoor.ADDNEW (DarKDdoser) CnC 2
- [ ] ET MALWARE Known Reveton Domain HTTP whatwillber.com
- [ ] ET MALWARE Unknown FakeAV - /get/*.crp
- [x] ET MALWARE Andromeda Check-in Response
- [ ] ET MALWARE Win32/Kuluoz.B CnC 2
- [x] ET MALWARE Lyposit Ransomware Checkin 1
- [x] ET MALWARE WORM_VOBFUS Checkin 1
- [x] ET MALWARE WORM_VOBFUS Checkin Generic
- [ ] ET MALWARE W32/Quarian HTTP Proxy Header
- [x] ET MALWARE SmokeBot grab data plaintext
- [x] ET MALWARE Kelihos.K Executable Download DGA
- [ ] ET MALWARE W32/Prinimalka Get Task CnC Beacon
- [ ] ET MALWARE W32/Prinimalka Prinimalka.py Script In CnC Beacon
- [ ] ET MALWARE W32.Daws/Sanny CnC POST
- [ ] ET MALWARE TROJAN Unk_Banker - Check In
- [x] ET MALWARE FakeAV checkin
- [x] ET MALWARE Unknown - Loader - Check .exe Updated
- [x] ET MALWARE DNS Reply Sinkhole - Microsoft - 199.2.137.0/24
- [ ] ET MALWARE FakeAV Download antivirus-installer.exe
- [x] ET MALWARE W32/Downloader.FakeFlashPlayer Status.Php CnC Beacon
- [ ] ET MALWARE W32/Downloader.FakeFlashPlayer Kelimeid CnC Beacon
- [x] ET MALWARE CFR DRIVEBY CVE-2012-4792 DNS Query for C2 domain
- [x] ET MALWARE Request for fake postal receipt from e-mail link
- [ ] ET MALWARE PoisonIvy.2013Jan04 server response
- [x] ET MALWARE Generic -POST To file.php w/Extended ASCII Characters
- [x] ET MALWARE FakeAV security_scanner.exe
- [x] ET MALWARE W32/Tobfy.Ransomware Invalid URI CnC Request
- [x] ET MALWARE W32/Zemra.DDoS.Bot Variant CnC Beacon
- [x] ET MALWARE W32/Iyus.H work_troy.php CnC Request
- [ ] ET MALWARE W32/Karagany.Downloader CnC Beacon
- [x] ET MALWARE Red October/Win32.Digitalia Checkin cgi-bin/nt/th
- [x] ET MALWARE Red October/Win32.Digitalia Checkin cgi-bin/dllhost/ac
- [x] ET MALWARE Red October/Win32.Digitalia Checkin cgi-bin/ms/flush
- [x] ET MALWARE Red October/Win32.Digitalia Checkin cgi-bin/win/cab
- [ ] ET MALWARE DNS Query to Unknown CnC DGA Domain whatandwhyeh.com 09/20/12
- [ ] ET MALWARE DNS Query to Unknown CnC DGA Domain bktwenty.com 09/20/12
- [ ] ET MALWARE DNS Query to Unknown CnC DGA Domain (defmaybe .com) 09/25/12
- [ ] ET MALWARE SSL Cert Used In Unknown Exploit Kit
- [ ] ET MALWARE Pincav.cjvb Checkin
- [x] ET MALWARE Zbot UA
- [ ] ET MALWARE Winlock.6870 SSL Cert
- [x] ET MALWARE Dorkbot GeoIP Lookup to wipmania
- [ ] ET MALWARE Mini-Flame v 5.x C2 HTTP request
- [x] ET MALWARE Taidoor Checkin
- [x] ET MALWARE Win32/Fujacks Activity
- [ ] ET MALWARE Zeus/Citadel Control Panel Access (Outbound)
- [ ] ET MALWARE Citadel API Access Iframer Controller (Outbound)
- [ ] ET MALWARE Citadel API Access VNC Controller (Outbound)
- [ ] ET MALWARE Citadel API Access Bot Controller (Outbound)
- [ ] ET MALWARE Citadel API Access Video Controller (Inbound)
- [ ] ET MALWARE SSL Cert Used In Unknown Exploit Kit
- [x] ET MALWARE Georbot requesting update
- [x] ET MALWARE Georbot checkin
- [x] ET MALWARE System Progressive Detection FakeAV (AMD)
- [ ] ET MALWARE Backdoor.ADDNEW (DarKDdoser) CnC 1
- [x] ET MALWARE Backdoor.ADDNEW (DarKDdoser) CnC 3
- [x] ET MALWARE DNS Query Known Reveton Domain whatwillber.com
- [x] ET MALWARE Win32/TrojanDownloader.Wauchos.A CnC Activity
- [ ] ET MALWARE Win32/Kuluoz.B CnC
- [ ] ET MALWARE Win32/Kuluoz.B CnC 3
- [x] ET MALWARE Lyposit Ransomware Checkin 2
- [x] ET MALWARE WORM_VOBFUS Requesting exe
- [x] ET MALWARE Win32/Kuluoz.B Request
- [x] ET MALWARE Win32/Necurs
- [x] ET MALWARE Win32/Trojan.Agent.AXMO CnC Beacon
- [x] ET MALWARE Faked Russian Opera UA without Accept - probable downloader
- [ ] ET MALWARE W32/Prinimalka Configuration Update Request
- [x] ET MALWARE W32.Daws/Sanny CnC Initial Beacon
- [ ] ET MALWARE Linux/Chapro.A Malicious Apache Module CnC Beacon
- [x] ET MALWARE SmokeLoader - Init 0x
- [x] ET MALWARE W32/Dexter Infostealer CnC POST
- [x] ET MALWARE DNS Reply Sinkhole - Microsoft - 131.253.18.11-12
- [ ] ET MALWARE DNS Reply Sinkhole - Microsoft - 207.46.90.0/24
- [ ] ET MALWARE W32/Downloader.FakeFlashPlayer Clientregister.php CnC Beacon
- [ ] ET MALWARE W32/Downloader.FakeFlashPlayer Bitensiteler CnC Beacon
- [x] ET MALWARE Stabuniq Checkin
- [x] ET MALWARE Sakula/Mivast RAT CnC Beacon 1
- [ ] ET MALWARE PoisonIvy.2013Jan04 victim beacon
- [x] ET MALWARE ProxyBox - HTTP CnC - proxy_info.php
- [x] ET MALWARE Generic -POST To gate.php w/Extended ASCII Characters (Likely Zeus Derivative)
- [x] ET MALWARE W32/Tobfy.Ransomware CnC Request - status.php
- [x] ET MALWARE Midhos/Medfos downloader
- [x] ET MALWARE W32/Iyus.H Initial CnC Beacon
- [x] ET MALWARE W32/Downloader Secondary Download Request - W32/Hupigon.Backdoor Likely Secondary Payload
- [ ] ET MALWARE BroBot POST
- [x] ET MALWARE Red October/Win32.Digitalia Checkin cgi-bin/nt/sk
- [x] ET MALWARE Red October/Win32.Digitalia Checkin cgi-bin/ms/check
- [x] ET MALWARE Red October/Win32.Digitalia Checkin cgi-bin/win/wcx
- [x] ET MALWARE Andromeda Checkin

- [x] ET MALWARE Possible Red October proxy CnC 1
- [x] ET MALWARE Possible Red October proxy CnC 2
- [x] ET MALWARE Possible Red October proxy CnC 3
- [x] ET MALWARE Win32/Emold.C Checkin
- [ ] ET MALWARE Unknown POST of Windows PW Hashes to External Site
- [ ] ET MALWARE Unknown POST of System Info
- [ ] ET MALWARE PoisonIvy Variant Jan 24 2013
- [ ] ET MALWARE PoisonIvy Variant Jan 24 2013
- [x] ET MALWARE W32/Bilakip.A Downloader API Ping CnC Beacon
- [x] ET MALWARE W32/Bilakip.A Downloader Viruslist Download For Populating FakeAV
- [x] ET MALWARE Win32/Xtrat.A Checkin
- [x] ET MALWARE Mashigoom/Tranwos/RevProxy ClickFraud - hello
- [ ] ET MALWARE RevProxy - ClickFraud - MIDUIDEND
- [x] ET MALWARE Simda.C Checkin
- [x] ET MALWARE W32/DownloaderAgent.fajk Successful Infection CnC Beacon
- [x] ET MALWARE W32/DownloaderAgent.fajk Second Stage Download List Requested
- [x] ET MALWARE Linux/SSHDoor.A Reporting Backdoor CnC Beacon
- [x] ET MALWARE W32/StartPage.eba Dropper Checkin
- [x] ET MALWARE Suspicious user-agent (f**king)
- [x] ET MALWARE ZeuS Post to C&C footer.php
- [x] ET MALWARE W32/SecVerif.Downloader Initial Checkin
- [x] ET MALWARE W32/SecVerif.Downloader Second Stage Download Request
- [x] ET MALWARE W32/Jabberbot.A Trednet XMPP CnC Beacon
- [x] ET MALWARE W32/Beebus HTTP POST CnC Beacon
- [x] ET MALWARE W32/ServStart.Variant CnC Beacon
- [x] ET MALWARE Request for fake postal receipt from e-mail link
- [x] ET MALWARE Umbra/Multibot Loader User-Agent (umbra)
- [x] ET MALWARE Umbra/MultiBot Plugin access
- [x] ET MALWARE Win32/Toby.N Multilocker Checkin
- [x] ET MALWARE Win32/Toby.N Multilocker Request
- [x] ET MALWARE Win32/Toby.N Multilocker Image Request
- [x] ET MALWARE Trojan.APT.9002 CnC Traffic
- [x] ET MALWARE W32/FloatingCloud.Banker CnC Beacon
- [x] ET MALWARE PDF 0day Communication - agent UA Feb 14 2013
- [x] ET MALWARE W32/Vundo.Downloader Reporting User Website Session Information
- [x] ET MALWARE Win32/Vundo.OD Checkin
- [x] ET MALWARE Win32.Zbot.ivgw Downloading EXE
- [ ] ET MALWARE Backdoor.Win32.Likseput.B Checkin 2
- [ ] ET MALWARE Shady Rat/HTran style HTTP Header Pattern Request UHCa and Google MSIE UA
- [x] ET MALWARE Win32/Tosct.B UA Mandiant APT1 Related
- [x] ET MALWARE Likseput.B Checkin
- [x] ET MALWARE Backdoor.Win32/Likseput.A Checkin Windows Vista/7/8
- [x] ET MALWARE Win32/COOKIEBAG Cookie APT1 Related
- [x] ET MALWARE WEBC2-TABLE Checkin 1 - APT1 Related
- [x] ET MALWARE WEBC2-TABLE Checkin 2 - APT1 Related
- [x] ET MALWARE WEBC2-TABLE Checkin 3 - APT1 Related
- [x] ET MALWARE WEBC2-TABLE Checkin Response - Embedded CnC APT1 Related
- [x] ET MALWARE Win32/Namsoth.A Checkin/NEWSREELS APT1 Related
- [x] ET MALWARE SEASALT HTTP Checkin
- [x] ET MALWARE SEASALT Client Checkin
- [x] ET MALWARE SEASALT Server Response
- [x] ET MALWARE STARSYPOUND Client Checkin
- [ ] ET MALWARE STARSYPOUND Client Checkin
- [x] ET MALWARE SWORD Sending Sword Marker
- [x] ET MALWARE TABMSGSQL/Sluegot.C Checkin
- [x] ET MALWARE WARP Win32/Barkiofork.A
- [x] ET MALWARE WEBC2-ADSPACE Server Response
- [x] ET MALWARE WEBC2-AUSOV Checkin Response - Embedded CnC APT1 Related
- [x] ET MALWARE Backdoor.Win32/Likseput.A Checkin
- [x] ET MALWARE WEBC2-QBP Checkin Response 1 - Embedded CnC APT1 Related
- [x] ET MALWARE WEBC2-CLOVER Checkin APT1 Related
- [x] ET MALWARE WEBC2-CLOVER Download UA
- [x] ET MALWARE WEBC2-DIV UA
- [x] ET MALWARE Possible WEBC2-GREENCAT Response - Embedded CnC APT1 Related
- [x] ET MALWARE WEBC2-KT3 Intial Connection Beacon APT1 Related
- [x] ET MALWARE WEBC2-KT3 Intial Connection Beacon Server Response APT1 Related
- [x] ET MALWARE WEBC2-RAVE UA
- [x] ET MALWARE Win32/Small.XR Checkin 2 WEBC2-CSON APT1 Related
- [ ] ET MALWARE WEBC2-CSON Checkin - APT1 Related
- [x] ET MALWARE Win32.Sluegot.A Checkin WEBC2-YAHOO APT1 Related
- [x] ET MALWARE Fake Virtually SSL Cert APT1
- [ ] ET MALWARE Fake IBM SSL Cert APT1
- [x] ET MALWARE EMAIL SSL Cert APT1
- [x] ET MALWARE LAME SSL Cert APT1
- [x] ET MALWARE NS SSL Cert APT1
- [x] ET MALWARE SERVER SSL Cert APT1
- [x] ET MALWARE SUR SSL Cert APT1
- [x] ET MALWARE FAKE AOL SSL Cert APT1
- [x] ET MALWARE FAKE YAHOO SSL Cert APT1
- [x] ET MALWARE WEBC2-UGX User-Agent (Windows+NT+5.x) APT1
- [x] ET MALWARE WEBC2-UGX Embedded CnC Response APT1
- [x] ET MALWARE CommentCrew UGX Backdoor initial connection
- [x] ET MALWARE CommentCrew downloader without user-agent string exe download without User Agent
- [x] ET MALWARE CommentCrew Possible APT c2 communications get system
- [x] ET MALWARE CommentCrew Possible APT c2 communications html return 1
- [x] ET MALWARE CommentCrew Possible APT c2 communications sleep
- [x] ET MALWARE CommentCrew Possible APT c2 communications sleep2
- [x] ET MALWARE CommentCrew Possible APT c2 communications sleep3
- [x] ET MALWARE CommentCrew Possible APT c2 communications sleep5
- [x] ET MALWARE CommentCrew Possible APT c2 communications download client.png
- [x] ET MALWARE CommentCrew Possible APT crabdance backdoor base64 head 2
- [x] ET MALWARE CommentCrew Possible APT crabdance backdoor base64 head
- [x] ET MALWARE CommentCrew Possible APT backdoor stage 2 download base64 update.gif
- [x] ET MALWARE CommentCrew Possible APT backdoor download logo.png
- [x] ET MALWARE CommentCrew Possible APT c2 communications get command client key
- [x] ET MALWARE CBeplay Downloading Design
- [x] ET MALWARE Gimemo Ransomware Checkin
- [x] ET MALWARE W32/Caphaw Requesting Additional Modules From CnC
- [x] ET MALWARE W32/Caphaw CnC Configuration File Request
- [x] ET MALWARE W32/Zbot.Variant Fake MSIE 6.0 UA
- [x] ET MALWARE Gimemo Activity
- [x] ET MALWARE W32/Asprox php.dll.crp POST CnC Beacon

- [x] ET MALWARE W32/Asprox CnC Beacon
- [x] ET MALWARE W32/Asprox Passgrub POST CnC Beacon
- [x] ET MALWARE W32/Asprox.FakeAV Affiliate Second Stage Download Location Request
- [x] ET MALWARE W32/Asprox.FakeAV Affiliate Download Location Response - Likely Pay-Per-Install For W32/Papras.Spy or W32/ZeroAccess
- [x] ET MALWARE W32/TrojanSpy.MSIL Fetch Time CnC Beacon
- [x] ET MALWARE W32/TrojanSpy.MSIL Get New MAC CnC Beacon
- [x] ET MALWARE W32/TrojanSpy.MSIL Set Done Day CnC Beacon
- [x] ET MALWARE W32/TrojanSpy.MSIL Fetch Header CnC Beacon
- [x] ET MALWARE Java Download non Jar file
- [x] ET MALWARE Win32/Fareit Checkin 2
- [x] ET MALWARE W32/Trustezeb.C CnC Beacon
- [x] ET MALWARE Win32/Urausy.C Checkin
- [x] ET MALWARE Win32/Urausy.C Checkin 2
- [x] ET MALWARE W32/LetsGo.APT Sleep CnC Beacon
- [x] ET MALWARE APT_NGO_wuaclt C2 Check-in
- [x] ET MALWARE APT_NGO_wuaclt
- [x] ET MALWARE Dorkbot Loader Payload Request
- [x] ET MALWARE APT_NGO_wuaclt PDF file
- [x] ET MALWARE RevProxy Java Settings
- [x] ET MALWARE Backdoor.Win32.Xtrat Checkin 2
- [ ] ET MALWARE DNS Query Sykipot Domain peocity.com
- [x] ET MALWARE DNS Query Sykipot Domain rusview.net
- [ ] ET MALWARE DNS Query Sykipot Domain skyruss.net
- [ ] ET MALWARE DNS Query Sykipot Domain commanal.net
- [ ] ET MALWARE DNS Query Sykipot Domain natareport.com
- [ ] ET MALWARE DNS Query Sykipot Domain photogellrey.com
- [ ] ET MALWARE DNS Query Sykipot Domain photogalaxyzone.com
- [x] ET MALWARE DNS Query Sykipot Domain insdet.com
- [ ] ET MALWARE DNS Query Sykipot Domain creditrept.com
- [ ] ET MALWARE DNS Query Sykipot Domain pollingvoter.org
- [ ] ET MALWARE DNS Query Sykipot Domain dfasonline.com
- [ ] ET MALWARE DNS Query Sykipot Domain hudsoninst.com
- [ ] ET MALWARE DNS Query Sykipot Domain wsurveymaster.com
- [ ] ET MALWARE DNS Query Sykipot Domain nhrasurvey.org
- [ ] ET MALWARE DNS Query Sykipot Domain pdi2012.org
- [ ] ET MALWARE DNS Query Sykipot Domain nceba.org
- [ ] ET MALWARE DNS Query Sykipot Domain linkedin-blog.com
- [ ] ET MALWARE DNS Query Sykipot Domain aafbonus.com
- [ ] ET MALWARE DNS Query Sykipot Domain milstars.org
- [ ] ET MALWARE DNS Query Sykipot Domain vatdex.com
- [ ] ET MALWARE DNS Query Sykipot Domain insightpublicaffairs.org
- [ ] ET MALWARE DNS Query Sykipot Domain applesea.net
- [ ] ET MALWARE DNS Query Sykipot Domain appledmg.net
- [ ] ET MALWARE DNS Query Sykipot Domain appleintouch.net
- [ ] ET MALWARE DNS Query Sykipot Domain seyuieyahooapis.com
- [ ] ET MALWARE DNS Query Sykipot Domain appledns.net
- [ ] ET MALWARE DNS Query Sykipot Domain emailserverctr.com
- [ ] ET MALWARE DNS Query Sykipot Domain dailynewsjustin.com
- [ ] ET MALWARE DNS Query Sykipot Domain hi-tecsolutions.org
- [ ] ET MALWARE DNS Query Sykipot Domain slashdoc.org
- [ ] ET MALWARE DNS Query Sykipot Domain photosmagnum.com
- [ ] ET MALWARE DNS Query Sykipot Domain resume4jobs.net
- [ ] ET MALWARE DNS Query Sykipot Domain searching-job.net
- [ ] ET MALWARE DNS Query Sykipot Domain servagency.com
- [ ] ET MALWARE DNS Query Sykipot Domain gsasmartpay.org
- [ ] ET MALWARE DNS Query Sykipot Domain tech-att.com
- [x] ET MALWARE W32/GameThief Initial CnC Beacon
- [x] ET MALWARE W32/Depyot.Downloader CnC Beacon
- [x] ET MALWARE Galock Ransomware Check-in
- [x] ET MALWARE Galock Ransomware Command
- [x] ET MALWARE [CrowdStrike] ANCHOR PANDA - Adobe Gh0st Beacon
- [x] ET MALWARE [CrowdStrike] ANCHOR PANDA Torn RAT Beacon Message Header Local
- [x] ET MALWARE [CrowdStrike] ANCHOR PANDA Torn RAT Beacon Message
- [x] ET MALWARE Win32/Delfinject Check-in
- [x] ET MALWARE Win32/Enchanim Checkin
- [x] ET MALWARE Zeus User-Agent(z00sAgent)
- [x] ET MALWARE W32/BaneChant.APT Winword.pkg Redirect
- [x] ET MALWARE W32/BaneChant.APT Data Exfiltration POST to CnC
- [x] ET MALWARE W32/BaneChant.APT Initial CnC Beacon
- [x] ET MALWARE Revoyem Ransomware Check-in
- [x] ET MALWARE Revoyem Ransomware Activity
- [x] ET MALWARE W32/Citadel Infection or Config URL Request
- [x] ET MALWARE W32/Citadel File.php CnC POST
- [x] ET MALWARE W32/Citadel Content.php CnC POST
- [x] ET MALWARE W32/Citadel Pro File.php CnC POST
- [x] ET MALWARE Possible W32/Citadel Download From CnC Server Self Referenced /files/ attachment
- [x] ET MALWARE W32/Citadel Conf.bin Download From CnC Server
- [x] ET MALWARE W32/NSISDL.Downloader CnC Server Response
- [ ] ET MALWARE RansomCrypt Intial Check-in
- [x] ET MALWARE RansomCrypt Getting Template
- [x] ET MALWARE W32/Nymaim Checkin M2
- [x] ET MALWARE Win32/Redyms.A Checkin
- [x] ET MALWARE Backdoor.Win32.Dorkbot.AR Join IRC channel
- [x] ET MALWARE Win32/Enchanim Check-in Response
- [x] ET MALWARE Win32/Enchanim Process List Dump
- [x] ET MALWARE Win32/Enchanim C2 Injection Download
- [x] ET MALWARE Win32/Enchanim C2 Client Check-in
- [x] ET MALWARE Mutter Backdoor Checkin
- [x] ET MALWARE Linux Backdoor Linux/Cdorked.A Redirect 1
- [ ] ET MALWARE Possible Linux/Cdorked.A Incoming Command
- [ ] ET MALWARE TROJ_NAIKON.A SSL Cert
- [x] ET MALWARE Medfos Connectivity Check
- [x] ET MALWARE Known Sinkhole Response Header
- [x] ET MALWARE Cookies/Cookiebag Checkin
- [x] ET MALWARE Win32/Urausy.C Checkin 3
- [ ] ET MALWARE Greencat SSL Certificate
- [x] ET MALWARE Linux Backdoor Linux/Cdorked.A Redirect 2
- [x] ET MALWARE Linux Backdoor Linux/Cdorked.A Redirect 3
- [ ] ET MALWARE Variant.Zusy.45802 Checkin
- [x] ET MALWARE DEEP PANDA Checkin 1
- [ ] ET MALWARE DEEP PANDA Checkin 2
- [x] ET MALWARE DEEP PANDA Checkin 3
- [x] ET MALWARE Suspicious Fake Opera 10 User-Agent
- [ ] ET MALWARE Unknown Checkin
- [ ] ET MALWARE Alina Checkin
- [x] ET MALWARE Alina User-Agent(Alina)
- [x] ET MALWARE Trojan-Downloader.Win32.AutoIt.mj Checkin
- [x] ET MALWARE Worm.Win32.Ngrbot.lof Join IRC channel
- [x] ET MALWARE Possible Linux/Cdorked.A CnC
- [x] ET MALWARE Embedded Android Dalvik Executable File With Fake Windows Executable Header - Possible AV Bypass Attempt
- [ ] ET MALWARE Embedded ZIP/APK File With Fake Windows Executable Header - Possible AV Bypass Attempt
- [x] ET MALWARE Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative)
- [x] ET MALWARE Hangover Campaign Keylogger Checkin
- [x] ET MALWARE Hangover Campaign Keylogger 2 checkin
- [x] ET MALWARE Trojan.Win32.VB.cefz Checkin
- [x] ET MALWARE Backdoor.Win32.Agent.bjjv Checkin
- [x] ET MALWARE TrojanSpy.KeyLogger.acqh User-Agent(EMSFRTCBVD)
- [x] ET MALWARE Trojan-Spy.Win32.KeyLogger.acuj Checkin

- [x] ET MALWARE Backdoor.Win32.Pushdo.s Checkin
- [x] ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(FMBVDFRESCT)
- [x] ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(DSMBVCTFRE)
- [x] ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(MBESCVDFRT)
- [x] ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(TCBFRVDEMS)
- [x] ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(DEMOMAKE)
- [x] ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(DEMO)
- [x] ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(UPHTTP)
- [x] ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(sendFile)
- [x] ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(vbusers)
- [x] ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(folderwin)
- [x] ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(smaal)
- [x] ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(nento)
- [x] ET MALWARE TrojanSpy.KeyLogger Hangover Campaign User-Agent(bugmaal)
- [x] ET MALWARE Trojan.BlackRev Registering Client
- [x] ET MALWARE Trojan.BlackRev Download Executable
- [ ] ET MALWARE Trojan-Spy.Win32.Agent.byhm User-Agent (EMSCBVDFRT)
- [ ] ET MALWARE Trojan.Win32.FresctSpy.A User-Agent (MBVDFRESCT)
- [x] ET MALWARE Trojan.BlackRev Registration Rev3
- [x] ET MALWARE Trojan.BlackRev Get Command Rev3
- [x] ET MALWARE W32/Briba CnC POST Beacon
- [x] ET MALWARE W32/KeyLogger.ACQH!tr Checkin
- [x] ET MALWARE Backdoor.Win32.VB.Alsci/Dragon Eye RAT Checkin (sending user info)
- [x] ET MALWARE Trojan.Win32.Antavmu.guw Checkin
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic
- [x] ET MALWARE Spy/Infostealer.Win32.Embed.A Client Traffic
- [x] ET MALWARE W32/Safe User Agent Fantasia
- [x] ET MALWARE Variant.Kazy.174106 Checkin
- [x] ET MALWARE Vobfus Check-in
- [x] ET MALWARE ISRStealer Checkin
- [x] ET MALWARE Possible Win32.Bicololo Checkin
- [x] ET MALWARE Win32.Bicololo Response 1
- [x] ET MALWARE Win32.Bicololo Response 2
- [x] ET MALWARE Possible Backdoor.Linux.Tsunami Outbound HTTP request
- [x] ET MALWARE Possible Win32/Hupigon ip.txt with a Non-Mozilla UA
- [x] ET MALWARE Backdoor.Win32.Trup.CX Checkin 1
- [x] ET MALWARE System Progressive Detection FakeAV (AuthenticAMD)
- [x] ET MALWARE System Progressive Detection FakeAV (GenuineIntel)
- [ ] ET MALWARE Trojan.Win32/Mutopy.A Checkin
- [x] ET MALWARE W32/Symmi Remote File Injector Initial CnC Beacon
- [x] ET MALWARE Win32/Travnet.A Checkin
- [x] ET MALWARE Possible Win32/Travnet.A Internet Connection Check (microsoft.com)
- [x] ET MALWARE Karagany encrypted binary (3)
- [x] ET MALWARE KeyBoy Backdoor Login
- [ ] ET MALWARE KeyBoy Backdoor SysInfo Response header
- [ ] ET MALWARE KeyBoy Backdoor File Manager Response Header
- [ ] ET MALWARE KeyBoy Backdoor File Download Response Header
- [ ] ET MALWARE KeyBoy Backdoor File Upload Response Header
- [x] ET MALWARE Alina Server Response Code
- [ ] ET MALWARE Connection to AnubisNetworks Sinkhole IP (Possible Infected Host)
- [ ] ET MALWARE Connection to Georgia Tech Sinkhole IP (Possible Infected Host)
- [ ] ET MALWARE Connection to 1&1 Sinkhole IP (Possible Infected Host)
- [ ] ET MALWARE Connection to Zinkhole Sinkhole IP (Possible Infected Host)
- [ ] ET MALWARE Connection to Dr Web Sinkhole IP(Possible Infected Host)
- [ ] ET MALWARE Connection to Fitsec Sinkhole IP (Possible Infected Host)
- [ ] ET MALWARE Connection to Microsoft Sinkhole IP (Possbile Infected Host)
- [ ] ET MALWARE Connection to a cert.pl Sinkhole IP (Possible Infected Host)
- [x] ET MALWARE Win32/Tobfy.S
- [x] ET MALWARE KimJongRAT cnc exe pull
- [x] ET MALWARE TripleNine RAT Checkin
- [x] ET MALWARE Unknown Webserver Backdoor
- [ ] ET MALWARE Unknown Webserver Backdoor Domain (google-analytcs)
- [x] ET MALWARE Activity related to APT.Seinup Checkin 1
- [x] ET MALWARE Possible Drive DDoS Check-in
- [x] ET MALWARE Drive Receiving GET DDoS instructions
- [x] ET MALWARE Drive Receiving POST1 DDoS instructions
- [x] ET MALWARE Drive Receiving POST2 DDoS instructions
- [x] ET MALWARE Drive Receiving IP DDoS instructions
- [x] ET MALWARE Drive Receiving IP2 DDoS instructions
- [x] ET MALWARE Drive Receiving UDP DDoS instructions
- [ ] ET MALWARE PoisonIvy [victim beacon]
- [ ] ET MALWARE PoisonIvy [server response]
- [ ] ET MALWARE AryaN IRC bot CnC1
- [ ] ET MALWARE AryaN IRC bot CnC2
- [ ] ET MALWARE AryaN IRC bot Download and Execute Scheduled file command
- [ ] ET MALWARE AryaN IRC bot Flood command
- [ ] ET MALWARE AryaN IRC bot Botkill command
- [x] ET MALWARE Pony Loader default URI struct
- [x] ET MALWARE Win32/Comisproc Checkin
- [x] ET MALWARE VBulletin Backdoor CMD inbound
- [x] ET MALWARE VBulletin Backdoor C2 URI Structure
- [ ] ET MALWARE VBulletin Backdoor C2 Domain
- [x] ET MALWARE W32.Berbew Check-in
- [x] ET MALWARE Cryptmen FakAV page Title
- [x] ET MALWARE Win32/Kelihos.F exe Download 2
- [ ] ET MALWARE Win32/Kelihos.F Checkin
- [x] ET MALWARE Generic - POST To .php w/Extended ASCII Characters
- [x] ET MALWARE SmokeLoader Checkin
- [x] ET MALWARE Comfoo Checkin
- [ ] ET MALWARE StealRat Checkin
- [x] ET MALWARE CBReplay Checkin
- [x] ET MALWARE CBReplay.P Ransomware
- [ ] ET MALWARE W32/StealRat.SpamBot Configuration File Request
- [ ] ET MALWARE W32/StealRat.SpamBot CnC Server Configuration File Response
- [x] ET MALWARE W32/StealRat.SpamBot Email Template Request
- [x] ET MALWARE Win32.Rovnix.I Checkin

- [x] ET MALWARE ATTACKER IRCBot - net user - PRIVMSG Command
- [x] ET MALWARE ATTACKER IRCBot - net localgroup - PRIVMSG Command
- [x] ET MALWARE ATTACKER IRCBot - net add PRIVMSG Command
- [x] ET MALWARE ATTACKER IRCBot - netsh - PRIVMSG Command
- [x] ET MALWARE ATTACKER IRCBot - ipconfig - PRIVMSG Command
- [x] ET MALWARE ATTACKER IRCBot - reg - PRIVMSG Command
- [x] ET MALWARE ATTACKER IRCBot - The command completed successfully - PRIVMSG Response
- [x] ET MALWARE ATTACKER IRCBot - PRIVMSG Response - Directory Listing
- [x] ET MALWARE ATTACKER IRCBot - PRIVMSG Response - net command output
- [x] ET MALWARE ATTACKER IRCBot - PRIVMSG Response - ipconfig command output
- [ ] ET MALWARE Possible CritX/SafePack/FlashPack Jar Download
- [ ] ET MALWARE Possible CritX/SafePack/FlashPack EXE Download
- [x] ET MALWARE ATTACKER IRCBot - PRIVMSG Response - Directory Listing *nix
- [x] ET MALWARE Win32/Cridex Checkin
- [x] ET MALWARE W32/DirCrypt.Ransomware CnC Checkin
- [x] ET MALWARE FortDisco Reporting Status
- [x] ET MALWARE Possible FortDisco Reporting Hacked Accounts
- [x] ET MALWARE Win32/Pift DNS TXT CnC Lookup ppidn.net
- [x] ET MALWARE China Chopper Command Struct
- [x] ET MALWARE PRISM Backdoor
- [x] ET MALWARE DDoS.Win32.Agent.bay Covert Channel (VERSONEX and Mr.Black)
- [x] ET MALWARE Yayih.A Checkin 2
- [x] ET MALWARE Yayih.A Checkin 3
- [x] ET MALWARE W32/Spy.KeyLogger.OCI CnC Checkin
- [x] ET MALWARE Proxychecker Lookup
- [x] ET MALWARE Trojan Related Lame Updater User-Agent
- [x] ET MALWARE Win32.Troj.Cidox Checkin
- [ ] ET MALWARE PoisonIvy.admin@388 Keepalive to CnC
- [ ] ET MALWARE PoisonIvy.th3bug Keepalive to CnC
- [ ] ET MALWARE PoisonIvy.keaidestone Keepalive to CnC
- [ ] ET MALWARE PoisonIvy.suzuki Keepalive to CnC
- [ ] ET MALWARE PoisonIvy.happyyongzi Keepalive to CnC
- [ ] ET MALWARE PoisonIvy.key@123 Keepalive to CnC
- [ ] ET MALWARE PoisonIvy.gwx@123 Keepalive to CnC
- [ ] ET MALWARE PoisonIvy.wwwst@Admin Keepalive to CnC
- [ ] ET MALWARE PoisonIvy.xiaoxiaohuli Keepalive to CnC
- [ ] ET MALWARE PoisonIvy.smallfish Keepalive to CnC
- [ ] ET MALWARE PoisonIvy.XGstone Keepalive to CnC
- [x] ET MALWARE Win32/Napolar.A Getting URL
- [x] ET MALWARE Possible Win32/Napolar.A URL Response
- [ ] ET MALWARE Possible Avatar RootKit Yahoo Group Search
- [x] ET MALWARE Bitcoin variant Checkin
- [ ] ET MALWARE Win32/Neurevt.A/Betabot checkin
- [x] ET MALWARE Win64/Vabushky.A Malicious driver download
- [ ] ET MALWARE Drive DDoS Tool get command received key=okokokjjk
- [ ] ET MALWARE Drive DDoS Tool long command received key=okokokjjk
- [ ] ET MALWARE Drive DDoS Tool smart command received key=okokokjjk
- [ ] ET MALWARE Drive DDoS Tool post1 command received key=okokokjjk
- [ ] ET MALWARE Drive DDoS Tool post2 command received key=okokokjjk
- [ ] ET MALWARE Drive DDoS Tool byte command received key=okokokjjk
- [ ] ET MALWARE Drive DDoS Tool byte command received key=okokokjjk
- [x] ET MALWARE Trojan.Dirtjump Checkin
- [x] ET MALWARE Possible APT-12 Related C2
- [ ] ET MALWARE Possible Sweet Orange Payload Download Aug 28 2013
- [x] ET MALWARE Likely Bot Nick in IRC ([country|so version|CPU])
- [ ] ET MALWARE Gh0st_Apple Checkin
- [x] ET MALWARE EvilGrab/Vidgrab Checkin
- [x] ET MALWARE Bladabindi/njrat CnC Keep-Alive (INBOUND)
- [x] ET MALWARE Bladabindi/njrat CnC Keep-Alive (OUTBOUND)
- [x] ET MALWARE Bladabindi/njrat CnC Checkin
- [x] ET MALWARE Bladabindi/njrat CnC Command (File Manager)
- [ ] ET MALWARE Bladabindi/njrat CnC Command Response (File Manager)
- [ ] ET MALWARE Bladabindi/njrat CnC Command (Remote Desktop)
- [x] ET MALWARE Bladabindi/njrat CnC Command Response (Remote Desktop)
- [ ] ET MALWARE Bladabindi/njrat CnC Command (Remote Cam)
- [ ] ET MALWARE Bladabindi/njrat CnC Command Response (Remote Cam)
- [x] ET MALWARE Bladabindi/njrat CnC Command (Remote Shell)
- [x] ET MALWARE Bladabindi/njrat CnC Command Response (Process listing)
- [x] ET MALWARE Bladabindi/njrat CnC Command (Kill Process)
- [x] ET MALWARE Bladabindi/njrat CnC Command (Registry)
- [ ] ET MALWARE Bladabindi/njrat CnC Command (Keylogger)
- [x] ET MALWARE Bladabindi/njrat CnC Command (Get Passwords)
- [x] ET MALWARE Bladabindi/njrat CnC Command Response (Get Passwords)
- [x] ET MALWARE Waledac FACEPUNCH Traffic Detected
- [x] ET MALWARE ZeroAccess P2P Module v6 Reporting
- [x] ET MALWARE W32/Hesperus.Banker Tr-mail Variant Sending Data To CnC
- [x] ET MALWARE W32/Hesperus.Banker Nlog.php Variant Sending Data To CnC
- [x] ET MALWARE Win32/Dipverdle.A Activity
- [x] ET MALWARE W32/Zzinfor.A Retrieving Instructions From CnC Server
- [x] ET MALWARE W32/Downloader.Mevade.FBV CnC Beacon
- [x] ET MALWARE Gh0st Trojan CnC 2
- [x] ET MALWARE APT.Agtid callback
- [x] ET MALWARE Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1
- [x] ET MALWARE Worm.VBS.ayr Checkin 2
- [ ] ET MALWARE Worm.VBS.ayr CnC command (/iam-ready)
- [x] ET MALWARE Worm.VBS.ayr CnC command (is-enum-driver)
- [x] ET MALWARE Worm.VBS.ayr CnC command (is-enum-folder)
- [x] ET MALWARE Worm.VBS.ayr CnC command (is-enum-process)
- [x] ET MALWARE Worm.VBS.ayr CnC command (is-cmd-shell)
- [ ] ET MALWARE Worm.VBS.ayr CnC command response
- [x] ET MALWARE DATA-BROKER BOT Activity
- [x] ET MALWARE OSX/Leverage.A Checkin
- [x] ET MALWARE Hiloti/Mufanom CnC Response
- [ ] ET MALWARE Possible FortDisco POP3 Site list download
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 3
- [x] ET MALWARE Mevade Checkin
- [ ] ET MALWARE SSH Connection on 443 - Mevade Banner
- [x] ET MALWARE Citadel Activity POST
- [x] ET MALWARE CryptoLocker EXE Download
- [x] ET MALWARE Chthonic Checkin
- [x] ET MALWARE Possible W32/KanKan tools.ini Request
- [x] ET MALWARE Possible W32/KanKan Update officeaddinupdate.xml Request

- [x] ET MALWARE Possible Kelihos.F EXE Download Common Structure
- [x] ET MALWARE Backdoor.Egobot Checkin
- [x] ET MALWARE W32/Kegotip CnC Beacon
- [x] ET MALWARE Athena DDoS Bot Checkin
- [x] ET MALWARE Linux/Ssemgrvd sshd Backdoor HTTP CNC 2
- [x] ET MALWARE FakeAV Install
- [x] ET MALWARE W32/InstallMonster.Downloader Checkin
- [ ] ET MALWARE Fredcot campaign payload download
- [x] ET MALWARE Possible Schneebly Posting ScreenShot
- [x] ET MALWARE W32/Citadel.Arx Varient CnC Beacon 2
- [x] ET MALWARE Possible Stitur Secondary Download
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 4
- [ ] ET MALWARE Possible Fake Codec Download
- [x] ET MALWARE PlugX Checkin
- [x] ET MALWARE Trojan.BlackRev Botnet Monitor Request CnC Beacon
- [x] ET MALWARE Trojan.BlackRev V1.Botnet HTTP Login POST Flood Traffic Outbound
- [x] ET MALWARE PWS Win32/Lmir.BMQ checkin
- [x] ET MALWARE Downloader (P2P Zeus dropper UA)
- [x] ET MALWARE Trojan.Dropper.Win32.Dapato.braa.AMN CnC traffic
- [x] ET MALWARE Solarbot Check-in
- [ ] ET MALWARE Trojan-Downloader Win32.Genome.AV server response
- [x] ET MALWARE Darkness DDoS Common Intial Check-in Response wtf
- [x] ET MALWARE Possible Upatre Downloader SSL certificate
- [x] ET MALWARE Possible Zbot Activity Common Download Struct
- [x] ET MALWARE Vawtrak/NeverQuest Checkin
- [x] ET MALWARE W32/Ke3chang.Snake.APT Campaign CnC Beacon
- [x] ET MALWARE W32/Ke3chang.BMW.APT Campaign CnC Beacon
- [x] ET MALWARE W32/Ke3chang.MyWeb.APT Eourdegh Campaign CnC Beacon
- [x] ET MALWARE W32/Liftoh.Downloader Images CnC Beacon
- [x] ET MALWARE W32/Liftoh.Downloader Get Final Payload Request
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 6
- [x] ET MALWARE Kuluoz/Asprox Activity
- [ ] ET MALWARE Win32/Urausy.C Checkin 4
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 8
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 10
- [ ] ET MALWARE Win32.Morix.B checkin
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 11
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 12
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 13
- [ ] ET MALWARE Zbot Variant SSL cert for dewart.ru
- [ ] ET MALWARE Zbot Variant SSL cert for erjentronem.ru
- [x] ET MALWARE Agent.BAAB Checkin
- [x] ET MALWARE W32/Mevade.Variant CnC POST
- [x] ET MALWARE Kishop.A checkin
- [x] ET MALWARE PWS.Win32/Daceluw.A Checkin
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 15
- [x] ET MALWARE Java/Jacksbot Check-in
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 16
- [x] ET MALWARE W32.Nemim Checkin
- [x] ET MALWARE Kuluoz Activity
- [ ] ET MALWARE Possible Sakura Jar Download Oct 22 2013
- [ ] ET MALWARE Linux/Ssemgrvd sshd Backdoor HTTP CNC 1
- [x] ET MALWARE Possible TRAT proxy component user agent detected
- [x] ET MALWARE W32/Badur.Spy User Agent lawl
- [x] ET MALWARE Known Sinkhole Response Header
- [x] ET MALWARE Possible Backdoor.Adwind Download
- [x] ET MALWARE W32/Citadel.Arx Variant CnC Beacon 1
- [x] ET MALWARE FaceBook IM & Web Driven Facebook Trojan Posting Data
- [x] ET MALWARE Possible Trojan.APT.9002 POST
- [x] ET MALWARE Bamital checkin
- [ ] ET MALWARE Taidoor Checkin
- [x] ET MALWARE Athena Bot Nick in IRC
- [ ] ET MALWARE Trojan.BlackRev Botnet Login Request CnC Beacon
- [x] ET MALWARE Trojan.BlackRev Botnet Command Request CnC Beacon
- [x] ET MALWARE Sisproc update
- [x] ET MALWARE Possible SSH Linux.Fokirtor backchannel command
- [x] ET MALWARE Kryptik Check-in
- [x] ET MALWARE Trojan-Downloader Win32.Genome.AV
- [x] ET MALWARE Darkness DDoS HTTP Target/EXE
- [x] ET MALWARE WORM_VOBFUS Checkin Generic 2
- [x] ET MALWARE Common Zbot EXE filename Dec 09 2013
- [ ] ET MALWARE HTTP Connection To Known Sinkhole Domain sinkdns.org
- [x] ET MALWARE W32/Ke3chang.MovieStar.APT Campaign CnC Beacon
- [x] ET MALWARE W32/Ke3chang.MyWeb.APT Campaign CnC Beacon
- [x] ET MALWARE W32/Ke3chang.Dream.APT Campaign CnC Beacon 2
- [x] ET MALWARE W32/Liftoh.Downloader Feed404 CnC Beacon
- [ ] ET MALWARE W32/Liftoh.Downloader Final.html Payload Request
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 5
- [x] ET MALWARE W32/GMUnpacker.Downloader Download Instructions Response From CnC
- [x] ET MALWARE Possible PDF Dictionary Entry with Hex/Ascii replacement
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 7
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 9
- [x] ET MALWARE W32/Ferret DDOS Bot CnC Beacon 2
- [x] ET MALWARE Trojan Generic - POST To gate.php with no referer
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 12 SET
- [x] ET MALWARE Fake/Short Google Search Appliance UA Win32/Ranbyus and Others
- [ ] ET MALWARE Zbot Variant SSL cert for whoismama.ru
- [ ] ET MALWARE Zbot Variant SSL cert for anlogtewron.ru
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 14
- [x] ET MALWARE LDPinch Checkin Post
- [x] ET MALWARE PE EXE or DLL Windows file download disguised as ASCII
- [x] ET MALWARE StartPage jsp checkin
- [x] ET MALWARE ICEFOG JAVAFOG JAR checkin
- [ ] ET MALWARE Possible Updatre SSL Certificate cardiffpower
- [ ] ET MALWARE Upatre SSL Compromised site appsredeeem
- [x] ET MALWARE Cybergate/Rebhip/Spyrat Backdoor Keepalive

- [x] ET MALWARE Cybergate/Rebhip/Spyrat Backdoor Keepalive Response
- [x] ET MALWARE Worm.VBS Dunihi/Houdini/H-Worm Checkin UA
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 17
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 18
- [x] ET MALWARE Limitless Logger Sending Data over SMTP 2
- [ ] ET MALWARE Win32/Antilam.2_0 Sending Data over SMTP
- [x] ET MALWARE Possible Win32/Dimegup.A Downloading Image Common URI Struct
- [x] ET MALWARE Win32/Xtrat C2 Response
- [ ] ET MALWARE ehow/livestrong Malicious Flash 10/11
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 19
- [ ] ET MALWARE W32/Banker.AALV checkin
- [x] ET MALWARE SolarBot Plugin Download MessageBox
- [x] ET MALWARE SolarBot Plugin Download WalletSteal
- [x] ET MALWARE W32/Neverquest.InfoStealer Configuration Request CnC Beacon
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 20
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 21
- [ ] ET MALWARE Possible KAPTOXA Encoded Data Transferred Over SMB 1
- [ ] ET MALWARE Possible KAPTOXA Encoded Data Transferred Over SMB 3
- [ ] ET MALWARE Possible KAPTOXA Encoded Data Transferred Over SMB 5
- [ ] ET MALWARE Possible KAPTOXA Encoded Data Transferred Over SMB 7
- [ ] ET MALWARE Possible KAPTOXA Encoded Data Transferred Over SMB 9
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 22
- [ ] ET MALWARE W32/FakeAlert.FT.gen.Eldorado Downloading VBS
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 23
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 25
- [x] ET MALWARE W32.Blackshades/Shadesrat Backdoor CnC Beacon
- [x] ET MALWARE W32/Zeus.InfoStealer Infection Campaign Wav.exe Request
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 26
- [x] ET MALWARE DirtJumper Activity
- [x] ET MALWARE W32/Asprox.ClickFraudBot CnC Beacon Acknowledgement
- [x] ET MALWARE W32/Rshot.Backdoor File Upload CnC Beacon
- [ ] ET MALWARE W32/Woai.Dropper Config Request
- [x] ET MALWARE Possible Mask C2 Traffic
- [x] ET MALWARE vSkimmer.PoS Checkin
- [x] ET MALWARE Trojan/Win32.FraudPack User-Agent (Downloader MLR 1.0.0)
- [ ] ET MALWARE FTP File Upload - BlackPOS Naming Scheme
- [ ] ET MALWARE Possible Sinkhole banner
- [x] ET MALWARE Blackbeard Check-in
- [x] ET MALWARE Linkup Ransomware check-in
- [x] ET MALWARE MS Remote Desktop micros User Login Request
- [x] ET MALWARE W32/Trojan-Gypikon Sending Data
- [x] ET MALWARE Win32/Tapazom.A
- [x] ET MALWARE Android/FakeKakao checkin
- [x] ET MALWARE MSIL.Zapchast Checkin
- [ ] ET MALWARE GoonEK Jan 21 2013
- [ ] ET MALWARE Possible Upatre Downloader SSL certificate (fake org)
- [x] ET MALWARE DNS Query Possible Zbot Infection Query for networksecurityx.hopto.org
- [ ] ET MALWARE Limitless Logger Sending Data over SMTP
- [ ] ET MALWARE Predator Logger Sending Data over SMTP
- [ ] ET MALWARE Win32.WinSpy.pob Sending Data over SMTP
- [x] ET MALWARE W32/LockscreenBEI.Scareware Cnc Beacon
- [x] ET MALWARE W32/Madness Checkin
- [x] ET MALWARE Limitless Logger RAT HTTP Activity
- [ ] ET MALWARE Win32.Genome.boescz Checkin
- [x] ET MALWARE SolarBot Plugin Download Server Response
- [x] ET MALWARE SolarBot Plugin Download ComputerInfo
- [x] ET MALWARE Jadtree Downloader rar
- [x] ET MALWARE Zbot Generic URI/Header Struct .bin
- [x] ET MALWARE Upatre Binary Download Jan 02 2014
- [ ] ET MALWARE Possible KAPTOXA SMB Naming Format
- [ ] ET MALWARE Possible KAPTOXA Encoded Data Transferred Over SMB 2
- [ ] ET MALWARE Possible KAPTOXA Encoded Data Transferred Over SMB 4
- [ ] ET MALWARE Possible KAPTOXA Encoded Data Transferred Over SMB 6
- [ ] ET MALWARE Possible KAPTOXA Encoded Data Transferred Over SMB 8
- [ ] ET MALWARE Possible KAPTOXA Encoded Data Transferred Over SMB 10
- [ ] ET MALWARE W32/FakeAlert.FT.gen.Eldorado Downloading DLL
- [x] ET MALWARE Win32/StoredBt.A Activity
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 24
- [x] ET MALWARE W32/Kbot.Backdoor Variant CnC Beacon
- [ ] ET MALWARE W32/Zeus.InfoStealer Infection Campaign Kia.exe Request
- [x] ET MALWARE W32/Zeus.InfoStealer Infection Campaign Heap.exe Request
- [ ] ET MALWARE Possible malicious zipped-executable
- [x] ET MALWARE W32/Asprox.ClickFraudBot CnC Beacon
- [x] ET MALWARE W32/Asprox.ClickFraudBot POST CnC Beacon
- [x] ET MALWARE W32/Dinwod.Dropper Win32/Xtrat.B CnC Beacon
- [ ] ET MALWARE TecSystems (Possible Mask) Signed PE EXE Download
- [x] ET MALWARE Infostealer.Jackpos Checkin
- [x] ET MALWARE Win32.Blackbeard Downloader
- [x] ET MALWARE DNS Query for Known Chewbacca CnC Server
- [x] ET MALWARE MS Remote Desktop edc User Login Request
- [x] ET MALWARE Banking Trojan HTTP Cookie
- [x] ET MALWARE Onkods.A Downloader Checkin
- [ ] ET MALWARE Win32/Almanahe.B Checkin
- [x] ET MALWARE Infostealer.Jackpos Checkin 2
- [x] ET MALWARE W32/Trojan-Gypikon Server Check-in Response
- [x] ET MALWARE Win32/Tapazom.A 2
- [x] ET MALWARE Possible Compromised Host AnubisNetworks Sinkhole Cookie Value Snkz
- [ ] ET MALWARE Backdoor.Win32.Popwin Checkin

- [x] ET MALWARE W32/Dadobra.Downloader/DNSChanger Dnsmake CnC Beacon
- [x] ET MALWARE Win32.Hack.PcClient.g CnC (OUTBOUND) XOR b5
- [x] ET MALWARE Gh0st Trojan CnC 3
- [ ] ET MALWARE Generic CnC
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 29
- [x] ET MALWARE Zeus.Downloader Campaign Unknown Initial CnC Beacon
- [ ] ET MALWARE W32/FakeFlash.Dropper Initial CnC Beacon
- [ ] ET MALWARE W32/FakeFlash.Dropper PutInformation CnC Beacon
- [ ] ET MALWARE Backdoor.joggver backdoor initialization packet
- [x] ET MALWARE Win32/Kryptik.BSYO Checkin 2
- [x] ET MALWARE Downloader.Win32.Geral Checkin
- [x] ET MALWARE Win32/Kryptik.BSYO Checkin
- [ ] ET MALWARE Possible PlugX Common Header Struct
- [x] ET MALWARE SMSHoax Riskware checkin
- [x] ET MALWARE Possible Zeus GameOver Connectivity Check
- [x] ET MALWARE Havex RAT CnC Server Response HTML Tag
- [x] ET MALWARE Gamut Spambot Checkin Response
- [x] ET MALWARE Snake rootkit usermode-centric encrypted command from server
- [x] ET MALWARE W32/PointOfSales.Misc CnC Activity
- [x] ET MALWARE Possible Graftor EXE Download Common Header Order
- [ ] ET MALWARE TDLv4 SSL Cert
- [ ] ET MALWARE Linux/Kimodin SSH backdoor activity
- [ ] ET MALWARE Perl/Calfbot C&C DNS request
- [ ] ET MALWARE Perl/Calfbot C&C DNS request
- [ ] ET MALWARE Perl/Calfbot C&C DNS request
- [ ] ET MALWARE Perl/Calfbot C&C DNS request
- [ ] ET MALWARE Perl/Calfbot C&C DNS request
- [ ] ET MALWARE Linux/Onimiki DNS trojan activity long format (Inbound)
- [ ] ET MALWARE Possible Netwire RAT Client HeartBeat S1 (no alert)
- [x] ET MALWARE BKDR_SLOTH.A Checkin
- [ ] ET MALWARE MultiThreat/Winspy.RAT Keep-Alive (flowbit set)
- [ ] ET MALWARE MultiThreat/Winspy.RAT SMTP Data Exfiltration
- [x] ET MALWARE Mal/Ransom-CE Connectivity Check
- [ ] ET MALWARE Win32/Stoberox.B
- [ ] ET MALWARE Upatre SSL Compromised site trudeausociety
- [ ] ET MALWARE Saker UA
- [x] ET MALWARE W32/SpeedingUpMyPC.Rootkit Install CnC Beacon
- [ ] ET MALWARE Asprox Fake Ximian Evolution X-Mailer Header (XimianEvolution1.4.6)
- [x] ET MALWARE Kazy Checkin
- [ ] ET MALWARE Upatre SSL Compromised site potpourriflowers
- [ ] ET MALWARE Possible FakeAV binary download (setup)
- [x] ET MALWARE Ixeshe/Mecklow Checkin 2
- [x] ET MALWARE Zeus.Downloader Campaign Second Stage Executable Request 10/4/2014
- [x] ET MALWARE Backdoor Win32/Zegost.Q CnC traffic (OUTBOUND)
- [ ] ET MALWARE Common Upatre Header Structure
- [x] ET MALWARE CryptoDefense DNS Domain Lookup
- [ ] ET MALWARE BitCrypt Ransomware Domain
- [x] ET MALWARE GreenDou Downloader User-Agent (hello crazyk)
- [x] ET MALWARE Probable OneLouder downloader (Zeus P2P)
- [ ] ET MALWARE ftpchk3.php possible upload success
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 27
- [ ] ET MALWARE Ebury SSH Rootkit data exfiltration
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 28
- [x] ET MALWARE Gulpix/PlugX Client Request
- [ ] ET MALWARE Zeus Spam Campaign pdf.exe In ZIP - 26th Feb 2014
- [ ] ET MALWARE Zeus.Downloader Campaign Second Stage Executable Request
- [ ] ET MALWARE W32/FakeFlash.Dropper Initial CnC Beacon Acknowledgement
- [ ] ET MALWARE W32/FakeFlash.Dropper GetInformation CnC Beacon Acknowledgement
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 30
- [ ] ET MALWARE Win32/Matsnu.L Checkin
- [x] ET MALWARE W32/Qakbot.Bot Version 8 CnC Beacon
- [x] ET MALWARE Likely Geodo/Emotet Downloading PE
- [x] ET MALWARE Darkshell.A Checkin XOR C0 Win XP
- [x] ET MALWARE Possible Kelihos Infection Executable Download With Malformed Header
- [x] ET MALWARE Havex RAT CnC Server Response
- [x] ET MALWARE Gamut Spambot Checkin
- [ ] ET MALWARE Snake rootkit usermode-centric client request
- [x] ET MALWARE W32/PointOfSales.Misc CnC Beacon
- [x] ET MALWARE RDP Brute Force Bot Checkin
- [x] ET MALWARE Win32/Expiro.CD Check-in
- [x] ET MALWARE Gamut Spambot Checkin 2
- [ ] ET MALWARE Perl/Calfbot C&C DNS request
- [x] ET MALWARE Perl/Calfbot C&C DNS request
- [ ] ET MALWARE Perl/Calfbot C&C DNS request
- [ ] ET MALWARE Perl/Calfbot C&C DNS request
- [ ] ET MALWARE Perl/Calfbot C&C DNS request
- [x] ET MALWARE Linux/Onimiki DNS trojan activity long format (Outbound)
- [x] ET MALWARE Possible Netwire RAT Client HeartBeat C1 (no alert)
- [ ] ET MALWARE Possible Netwire RAT Client HeartBeat C2
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 31
- [ ] ET MALWARE MultiThreat/Winspy.RAT Keep-Alive Server Response
- [ ] ET MALWARE MultiThreat/Winspy.RAT FTP File Download Command
- [x] ET MALWARE Zeus GameOver Checkin
- [x] ET MALWARE Possible Zeus GameOver/FluBot Related DGA NXDOMAIN Responses
- [x] ET MALWARE Win32/Sisproc
- [x] ET MALWARE Bozok.RAT checkin
- [x] ET MALWARE W32/SpeedingUpMyPC.Rootkit CnC Beacon
- [x] ET MALWARE Win32.Sality-GR Checkin
- [x] ET MALWARE W32/SpeedingUpMyPC.Rootkit Successful Install GET Type CnC Beacon
- [ ] ET MALWARE Upatre SSL Compromised site kionic
- [x] ET MALWARE Ixeshe/Mecklow Checkin
- [ ] ET MALWARE Zeus.Downloader Campaign Unknown Initial CnC Beacon 10/4/2014
- [ ] ET MALWARE cryptodefense Checkin
- [x] ET MALWARE Plasmabot CnC Host Checkin
- [x] ET MALWARE Possible Kelihos.F EXE Download Common Structure 2
- [ ] ET MALWARE BitCrypt site accessed via .onion SSL Proxy
- [x] ET MALWARE Win32.Kazy Checkin
- [x] ET MALWARE Trojan-Spy.Win32.Zbot.qgxi Checkin
- [x] ET MALWARE ftpchk3.php upload attempted
- [x] ET MALWARE W32/Zbot.InfoStealer WindowsUpdate Connectivity Check With Opera UA

- [x] ET MALWARE hacker87 checkin
- [ ] ET MALWARE Upatre Binary Download April 28 2014
- [x] ET MALWARE Vawtrak/NeverQuest - Post Data Form 01
- [x] ET MALWARE Netwire RAT Check-in
- [x] ET MALWARE W32/Karagany.Downloader CnC Beacon
- [x] ET MALWARE Potential Sefnit C2 traffic (from server)
- [x] ET MALWARE Upatre Downloader 2p (Zeus) May 07 2014
- [x] ET MALWARE ELF/Mayhem Checkin
- [ ] ET MALWARE Possible Upatre SSL Compromised site iclasshd.net
- [x] ET MALWARE W32/Fsysna.Downloader CnC Beacon
- [ ] ET MALWARE OneLouder EXE download possibly installing Zeus P2P
- [ ] ET MALWARE Possible Backdoor.Unrecom Download
- [x] ET MALWARE PandoraRat/Refroso.bsp Directory Listing Sent To Server
- [x] ET MALWARE W32/HelloBridge.Backdoor Login CnC Beacon
- [ ] ET MALWARE Downloader.Win32.Tesch.A Bot Command Checkin 1
- [ ] ET MALWARE Possible Upatre SSL Compromised site dfsdirect.ca
- [x] ET MALWARE Possible Zendran ELF IRCBot Joining Channel
- [ ] ET MALWARE Possible Zendran ELF IRCBot Server Banner
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 33
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 35
- [x] ET MALWARE Miniduke Checkin
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL certificate detected (KINS C2)
- [x] ET MALWARE Win32/Urausy.C response
- [ ] ET MALWARE Upatre Compromised Site hot-buys
- [x] ET MALWARE Win32/Enosch.A gtalk connectivity check
- [x] ET MALWARE Win32/Spy.Banker.AAQD Checkin
- [x] ET MALWARE Soraya C2 User-Agent
- [x] ET MALWARE Soraya C2 User-Agent (rhyno321)
- [x] ET MALWARE Soraya C2 User-Agent (slayer)
- [x] ET MALWARE Soraya C2 User-Agent (VHIbot/1.0)
- [x] ET MALWARE Soraya C2 User-Agent (x09)
- [ ] ET MALWARE TorExplorer Certificate - Potentially Linked To W32/Cryptowall.Ransomware
- [ ] ET MALWARE Possible Upatre SSL Cert
- [x] ET MALWARE EtumBot Registration Request
- [ ] ET MALWARE EtumBot Command Status Message
- [ ] ET MALWARE EtumBot GET File Initial Response
- [x] ET MALWARE Backdoor.Win32/Etumbot.B Requesting RC4 Key
- [x] ET MALWARE Putter Panda HTTPClient CnC HTTP Request
- [x] ET MALWARE Win32/Ramnit Checkin
- [x] ET MALWARE Hangover related campaign Response
- [x] ET MALWARE HTTP Request to a *.pw domain with direct request/ fake browser (multiple families flowbit set)
- [ ] ET MALWARE Possible Andromeda download with fake Zip header (1)
- [x] ET MALWARE Dyreza RAT Ex-filtrating Data
- [x] ET MALWARE Win32/Neutrino Checkin
- [ ] ET MALWARE Possible Upatre SSL Cert webhostingpad.com
- [x] ET MALWARE Citadel Checkin
- [x] ET MALWARE Andromeda Downloading Module
- [x] ET MALWARE Likely CryptoWall .onion Proxy domain in SNI
- [x] ET MALWARE Win32/Sharik C2 Incoming Traffic
- [x] ET MALWARE Possible W32/VBKlip BAN Download
- [ ] ET MALWARE Downloader.Win32.Tesch.A Bot Command (OK acknowledgement)
- [ ] ET MALWARE Downloader.Win32.Tesch.A Server Command (Confirm C2 IP and port)
- [ ] ET MALWARE Downloader.Win32.Tesch.A Server Command (bot is ready to start receiving commands)
- [x] ET MALWARE Zbot downloader Installing Zeus
- [x] ET MALWARE W32/Eclipse.DDOSBot CnC Beacon Response
- [x] ET MALWARE Netwire RAT Check-in (set)
- [x] ET MALWARE W32/Hicrazyk.A Downloader Install CnC Beacon
- [x] ET MALWARE Sefnit Checkin
- [x] ET MALWARE CryptoWall Check-in
- [x] ET MALWARE DNS Reply Sinkhole - Anubis - 195.22.26.192/26
- [x] ET MALWARE Possible Upatre Downloader SSL certificate (fake loc)
- [ ] ET MALWARE Possible Upatre SSL Compromised site sabzevarsez.com
- [ ] ET MALWARE possible OneLouder header structure
- [ ] ET MALWARE Possible Backdoor.Adwind Download 2
- [x] ET MALWARE PandoraRat/Refroso.bsp Activity
- [x] ET MALWARE W32/HelloBridge.Backdoor Register CnC Beacon
- [x] ET MALWARE Downloader.Win32.Tesch.A Server CnC Checkin Reply
- [x] ET MALWARE Downloader.Win32.Tesch.A Server CnC Sending Executable
- [ ] ET MALWARE Trojan.Win32.Webprefix checkin
- [ ] ET MALWARE Possible Zendran ELF IRCBot Joining Channel 2
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 32
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 34
- [ ] ET MALWARE .gadget Email Attachment - Possible Upatre
- [ ] ET MALWARE Upatre SSL Cert May 20 2014
- [x] ET MALWARE Win32/Geodo Checkin
- [x] ET MALWARE W32/Zeus.BitcoinMiner Variant CnC Beacon
- [x] ET MALWARE Trojan-Dropper.Win32.Agent.ksja
- [ ] ET MALWARE SSL Cert Observed with Unkown Trojan (statswas)
- [x] ET MALWARE Trojan.Win32.VBKrypt.cugq/Umbra Checkin
- [x] ET MALWARE Soraya C2 User-Agent (default)
- [x] ET MALWARE Soraya C2 User-Agent (SBTCM)
- [x] ET MALWARE Soraya C2 User-Agent (Vulture)
- [x] ET MALWARE Soraya C2 User-Agent (xehanort321)
- [x] ET MALWARE Win32.Trojan.Agent.U3D7V0 Checkin
- [x] ET MALWARE PlugX/Destory HTTP traffic
- [x] ET MALWARE Neverquest/Vawtrak Posting Data
- [x] ET MALWARE EtumBot Ping
- [ ] ET MALWARE EtumBot PUT File Response
- [ ] ET MALWARE EtumBot GET File Data Upload
- [x] ET MALWARE Pandemiya User-Agent
- [x] ET MALWARE Putter Panda 3PARA RAT initial beacon
- [x] ET MALWARE Hangover related campaign Checkin
- [x] ET MALWARE HTTP Request to a *.su domain with direct request/ fakebrowser (multiple families flowbit set)
- [x] ET MALWARE W32/Asprox.Bot Knock Variant CnC Beacon
- [ ] ET MALWARE Possible Andromeda download with fake Zip header (2)
- [ ] ET MALWARE Dyreza RAT Checkin
- [x] ET MALWARE Single char EXE direct download likely trojan (multiple families)
- [ ] ET MALWARE Dyreza RAT Checkin Response
- [x] ET MALWARE W32/Citadel Download From CnC Server /files/ attachment
- [x] ET MALWARE Likely CryptoWall .onion Proxy DNS lookup
- [x] ET MALWARE Win32/Sharik Checkin
- [ ] ET MALWARE Win32/Sharik C2 Incoming Crafted Request
- [x] ET MALWARE Downloader.Win32.Tesch.A Bot Command Checkin 2
- [ ] ET MALWARE Downloader.Win32.Tesch.A Bot Command (Proxy command)
- [ ] ET MALWARE Downloader.Win32.Tesch.A Server Command (Confirm C2 IP and port) 2
- [x] ET MALWARE Trojan.Karagany C&C Response

- [x] ET MALWARE W32/Antifulai.APT CnC Beacon 1
- [x] ET MALWARE W32/Antifulai.APT CnC Beacon 2
- [x] ET MALWARE W32/Antifulai.APT CnC Beacon 3
- [x] ET MALWARE W32/Antifulai.APT CnC Beacon 4
- [x] ET MALWARE Common Upatre Header Structure 2
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 36
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 37
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 38
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 39
- [x] ET MALWARE Unknown Trojan with Fake Java User-Agent
- [ ] ET MALWARE BANKER.WIN32.BANBRA.BEEC Checkin
- [x] ET MALWARE DNS Reply Sinkhole Microsoft NO-IP Domain
- [x] ET MALWARE Win32/Zemot Checkin
- [x] ET MALWARE Win32/Zemot Checkin
- [ ] ET MALWARE TrojanSpy.Win32/Banker.AMB SQL Checkin
- [x] ET MALWARE Infostealer.Bancos Checkin via SMTP
- [ ] ET MALWARE Possible Upatre SSL Cert 999servers.com
- [x] ET MALWARE Win32.Banload.BTQP Checkin 1
- [x] ET MALWARE Win32.Banload.BTQP Checkin 2
- [ ] ET MALWARE Upatre SSL Cert July 7 2014
- [x] ET MALWARE Downloader.Banload2.KZU Checkin 1
- [x] ET MALWARE Downloader.Banload2.KZU Checkin 2
- [x] ET MALWARE CyberGate RAT Checkin
- [x] ET MALWARE CyberGate RAT User-Agent (USER_CHECK)
- [x] ET MALWARE Win32/Zemot Config Download
- [x] ET MALWARE Minirem
- [x] ET MALWARE Possible Zeus P2P Variant DGA NXDOMAIN Responses July 11 2014
- [x] ET MALWARE Possible Zeus P2P Variant Check-in
- [x] ET MALWARE Uroburos/Turla CnC (OUTBOUND) 1
- [x] ET MALWARE Uroburos/Turla CnC (OUTBOUND) 2
- [ ] ET MALWARE Possible Upatre SSL Cert acesecureshop.com
- [ ] ET MALWARE Possible Upatre SSL Cert new-install.privatedns.com
- [ ] ET MALWARE Possible Upatre SSL Cert July 14 2014
- [ ] ET MALWARE Possible Upatre SSL Cert faithmentoringandmore.com
- [ ] ET MALWARE Linux DDoS bot Antiq IRC
- [x] ET MALWARE Sharik/Smoke Loader Adobe Connectivity check
- [x] ET MALWARE Sharik/Smoke Loader Microsoft Connectivity check
- [x] ET MALWARE Upatre Common URI Struct July 15 2014
- [x] ET MALWARE DNS Possible User trying to visit POSHCODER.A .onion link outside of torbrowser
- [x] ET MALWARE Soraya Credit Card Exfiltration
- [x] ET MALWARE W32/Kazy.325252 Variant CnC Beacon 1
- [x] ET MALWARE W32/Kazy.325252 Variant CnC Beacon 2
- [x] ET MALWARE Dyreza RAT Checkin 2
- [ ] ET MALWARE Win32/Aibatook checkin
- [ ] ET MALWARE Win32/Aibatook checkin 2
- [x] ET MALWARE Predator Pain Sending Data over SMTP
- [ ] ET MALWARE Possible Upatre SSL Cert karinejoncas.com
- [ ] ET MALWARE Possible Upatre SSL Cert deslematin.ca
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL certificate detected (KINS C2)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL certificate detected (Vawtrak MITM)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL certificate detected (KINS C2)
- [ ] ET MALWARE Pain File Stealer sending wallet.dat via SMTP
- [ ] ET MALWARE Kuluoz / Asprox checkin
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL certificate detected (KINS C2)
- [ ] ET MALWARE PE downloaded malicious SSL certificate (CZ Solutions)
- [x] ET MALWARE Dyreza RAT Checkin 3
- [x] ET MALWARE Asterope Checkin
- [ ] ET MALWARE Possible Upatre SSL Cert twitterbacklinks.com
- [ ] ET MALWARE Possible Upatre Serial Number in SSL Cert
- [x] ET MALWARE XPSecurityCenter FakeAV Checkin
- [x] ET MALWARE Hupigon.DF Checkin
- [ ] ET MALWARE Win.Trojan.Agent-29225 Checkin
- [x] ET MALWARE W32/Zbot.Variant CnC Response
- [x] ET MALWARE Win32/Swizzor User-Agent (Swizz03r)
- [ ] ET MALWARE DNS Query to Pseudo Random Domain for Web Malware (.mynumber.org)
- [ ] ET MALWARE Malicious SSL Cert (KINS C2)
- [x] ET MALWARE Likely Malicious SSL Cert With Script Tags
- [x] ET MALWARE Dridex/Bugat/Feodo Cookie
- [x] ET MALWARE Dridex/Bugat/Feodo POST Checkin
- [x] ET MALWARE Dridex/Bugat/Feodo GET Checkin
- [x] ET MALWARE Win32/Pykspa.C Public IP Check
- [x] ET MALWARE Dyreza RAT Fake Server Header
- [ ] ET MALWARE Possible Upatre SSL Cert thelabelnashville.com
- [ ] ET MALWARE Possible Upatre SSL Cert cactussports.com
- [ ] ET MALWARE Possible Upatre SSL Cert yellowdevilgear.com
- [ ] ET MALWARE Possible Upatre SSL Cert michaelswinecellar.com
- [ ] ET MALWARE Possible Upatre SSL Cert migsparkle.com
- [x] ET MALWARE Win32/Neurevt.A/Betabot Check-in 4
- [x] ET MALWARE Win32/TrojanDownloader.Waski.F Locker DL URI Struct Jul 25 2014
- [ ] ET MALWARE Possible Upatre SSL Cert server.abaphome.net
- [ ] ET MALWARE Possible Upatre SSL Cert 1stopmall.us
- [x] ET MALWARE EUPUDS.A Requests for Boleto replacement
- [ ] ET MALWARE Infostealer.KLPROXY Checkin via SMTP
- [x] ET MALWARE Win32/Gatak Activity
- [ ] ET MALWARE Possible Upatre SSL Cert disenart.info
- [ ] ET MALWARE Possible Upatre SSL Cert host-galaxy.com
- [ ] ET MALWARE Possible Upatre SSL Cert fxbingpanel.fareexchange.co.uk
- [ ] ET MALWARE Possible Upatre SSL Cert 66h.66hosting.net
- [ ] ET MALWARE Possible Upatre SSL Cert businesswebstudios.com
- [ ] ET MALWARE Possible Upatre SSL Cert udderperfection.com
- [x] ET MALWARE DoS.Linux/Elknot.G Checkin
- [ ] ET MALWARE Possible Upatre SSL Cert www.senorwooly.com
- [ ] ET MALWARE Possible Upatre SSL Cert ns2.sicher.in
- [ ] ET MALWARE Malicious SSL Cert (KINS C2)
- [ ] ET MALWARE Possible ClickFraud Trojan Socks5 Connection
- [x] ET MALWARE Windows executable base64 encoded
- [x] ET MALWARE Backoff POS Checkin
- [ ] ET MALWARE Possible Upatre SSL Cert chinasemservice.com
- [x] ET MALWARE W32/Pgift.Backdoor APT CnC Beacon
- [ ] ET MALWARE Possible Upatre SSL Cert ns7-777.777servers.com
- [ ] ET MALWARE Possible Upatre SSL Cert adodis.com
- [ ] ET MALWARE Tor based locker .onion Proxy domain in SNI July 31 2014
- [ ] ET MALWARE Tor based locker Ransom Page
- [ ] ET MALWARE Tor based locker .onion Proxy DNS lookup July 31 2014
- [ ] ET MALWARE Tor based locker knowledgewiki.info in SNI July 31 2014
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 40
- [ ] ET MALWARE Possible Upatre SSL Cert power2.mschosting.com
- [x] ET MALWARE Troj/ReRol.A Checkin 1

- [x] ET MALWARE Troj/ReRol.A Checkin 2
- [ ] ET MALWARE Troj/ReRol.A Checkin 4
- [x] ET MALWARE Windows Command Prompt OUTBOUND
- [x] ET MALWARE Windows TaskList Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Infostealer.Mysayad Checkin 1
- [x] ET MALWARE Infostealer.Mysayad Checkin 2
- [x] ET MALWARE Kronos Checkin
- [x] ET MALWARE Zbot .onion Proxy domain in SNI Aug 04 2014
- [x] ET MALWARE Zbot .onion Proxy DNS lookup July 31 2014
- [x] ET MALWARE Probable OneLouder downloader (Zeus P2P)
- [x] ET MALWARE Ddex Loader Check-in
- [ ] ET MALWARE BitcoinMiner C2 SSL Cert
- [x] ET MALWARE Pushdo.S CnC response
- [ ] ET MALWARE Possible Upatre SSL Cert tradeledstore.co.uk
- [x] ET MALWARE BITTERBUG Checkin
- [ ] ET MALWARE BITTERBUG Checkin 2
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL certificate detected (KINS C2)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [x] ET MALWARE Lurk Downloader Check-in
- [x] ET MALWARE Lurk Click fraud Template Request
- [ ] ET MALWARE Unknown Trojan Dropped By Archie.EK
- [x] ET MALWARE OneLouder Common URI Struct
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [x] ET MALWARE Suspicious X-mailer Synapse
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (CryptoWall C2)
- [ ] ET MALWARE ClickFraud Trojan Socks5 Init Response
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Vawtrak MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Vawtrak MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [ ] ET MALWARE Likely Synolocker .onion DNS lookup
- [ ] ET MALWARE Win32/PSW.Steam.NBP Checkin
- [ ] ET MALWARE Tor Based Locker Page (Torrentlocker)
- [x] ET MALWARE ShellBot.C retrieval
- [x] ET MALWARE Worm.Win32.Vobfus Checkin 3
- [x] ET MALWARE ZeroLocker Downloading Config
- [x] ET MALWARE ZeroLocker Activity
- [ ] ET MALWARE ZeroLocker Activity
- [ ] ET MALWARE ZeroLocker EXE Download
- [x] ET MALWARE Variant.Strictor Dropper
- [x] ET MALWARE Python.Ragua Checkin
- [x] ET MALWARE Probable OneLouder downloader (Zeus P2P)
- [ ] ET MALWARE Possible Dyre SSL Cert Aug 20 2014 D1
- [ ] ET MALWARE Possible Dyre SSL Cert Aug 20 2014 D2
- [x] ET MALWARE Hoic.zip retrieval
- [x] ET MALWARE Miras C2 Activity
- [x] ET MALWARE Machete FTP activity
- [x] ET MALWARE Probable OneLouder downloader (Zeus P2P)
- [x] ET MALWARE Probable OneLouder downloader (Zeus P2P) exe download
- [x] ET MALWARE Probable OneLouder downloader (Zeus P2P)
- [x] ET MALWARE PlugX variant
- [x] ET MALWARE Suspicious User-Agent (Asteria md5)
- [ ] ET MALWARE Win32/Xema dropping file
- [x] ET MALWARE Win32/Spy.Tuscas
- [x] ET MALWARE Windows ipconfig Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Windows net start Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Windows systeminfo Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Windows netstat Microsoft Windows DOS prompt command exit OUTBOUND
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [ ] ET MALWARE Possible Upatre SSL Cert freeb4u.com
- [ ] ET MALWARE Possible Upatre SSL Cert developmentinn.com
- [ ] ET MALWARE Possible Upatre SSL Cert directory92.com
- [ ] ET MALWARE Possible Upatre SSL Cert epr-co.ch
- [ ] ET MALWARE Possible Upatre SSL Cert pouyasazan.org
- [ ] ET MALWARE Possible Upatre SSL Cert ara-photos.net
- [ ] ET MALWARE Possible Upatre SSL Cert tecktalk.com
- [ ] ET MALWARE Possible Upatre SSL Cert cyclivate.com
- [ ] ET MALWARE Possible Upatre SSL Cert mentoringgroup.com
- [ ] ET MALWARE Possible Upatre SSL Cert dineshuthayakumar.in
- [ ] ET MALWARE Possible Upatre SSL Cert ssshosting.net
- [ ] ET MALWARE Possible Upatre SSL Cert erotikturk.com
- [ ] ET MALWARE Possible Upatre SSL Cert mtnoutfitters.com
- [ ] ET MALWARE Possible Upatre SSL Cert jojik-international.com
- [ ] ET MALWARE Possible Upatre SSL Cert abarsolutions.com
- [ ] ET MALWARE Possible Upatre SSL Cert eastwoodvalley.com
- [ ] ET MALWARE Possible Upatre SSL Cert pejlain.se
- [ ] ET MALWARE Possible Upatre SSL Cert dominionthe.com
- [ ] ET MALWARE Possible Upatre SSL Cert delanecanada.ca
- [ ] ET MALWARE Possible Upatre SSL Cert hebergement-solutions.com
- [ ] ET MALWARE Possible Upatre SSL Cert sportoftenіq.com
- [ ] ET MALWARE Possible Upatre SSL Cert adoraacc.com
- [ ] ET MALWARE Possible Upatre SSL Cert tristacey.com
- [ ] ET MALWARE Possible Upatre SSL Cert nbc-mail.com
- [ ] ET MALWARE Possible Upatre SSL Cert tridayacipta.com
- [ ] ET MALWARE Possible Upatre SSL Cert trainthetrainerinternational.com
- [ ] ET MALWARE Possible Upatre SSL Cert lingayasuniversity.edu.in
- [ ] ET MALWARE Possible Upatre SSL Cert uleideargan.com
- [ ] ET MALWARE Possible Upatre SSL Cert picklingtank.com
- [ ] ET MALWARE Possible Upatre SSL Cert vcomdesign.com
- [ ] ET MALWARE Possible Upatre SSL Cert technosysuk.com
- [ ] ET MALWARE Possible Upatre SSL Cert slmp-550-105.slc.westdc.net
- [ ] ET MALWARE Possible Upatre SSL Cert itiltrainingcertworkshop.com
- [ ] ET MALWARE Possible Upatre SSL Cert udderperfection.com
- [ ] ET MALWARE Possible Upatre SSL Cert efind.co.il
- [ ] ET MALWARE Possible Upatre SSL Cert bloodsoft.com
- [ ] ET MALWARE Possible Upatre SSL Cert walletmix.com
- [ ] ET MALWARE Possible Upatre SSL Cert turnaliinsaat.com
- [ ] ET MALWARE Possible Upatre SSL Cert mdus-pp-wb12.webhostbox.net
- [ ] ET MALWARE Possible Upatre SSL Cert plastics-technology.com
- [ ] ET MALWARE Possible Upatre SSL Cert deserve.org.uk
- [ ] ET MALWARE Possible Upatre SSL Cert worldbuy.biz
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [x] ET MALWARE Vawtrak/NeverQuest Posting Data
- [ ] ET MALWARE Possible Upatre SSL Cert paydaypedro.co.uk
- [ ] ET MALWARE Possible Upatre SSL Cert chatso.com

- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [x] ET MALWARE Windows set Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 41
- [ ] ET MALWARE Unknown Trojan Dropped by Angler Aug 29 2014
- [ ] ET MALWARE Possible Dyre SSL Cert Sept 3 2014
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [x] ET MALWARE HighTide trojan Checkin
- [x] ET MALWARE W32/Waterspout.APT Backdoor CnC Beacon
- [ ] ET MALWARE Possible Double Flated Encoded Inbound Malicious PDF
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [ ] ET MALWARE Cryptolocker .onion Proxy Domain in SNI
- [x] ET MALWARE W32/Bravix.Dropper CnC Beacon
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [x] ET MALWARE Win32/Poweliks GET Request
- [x] ET MALWARE Win32/Frosparf.B Downloading Hosts File
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [x] ET MALWARE Possible Zeus GameOver Connectivity Check 2
- [ ] ET MALWARE TSPY_POCARDL.U Possible FTP Login
- [x] ET MALWARE DecebalPOS User-Agent
- [x] ET MALWARE W32/Alina.POS-Trojan Checkin
- [x] ET MALWARE Possible Banload Downloading Executable
- [x] ET MALWARE Tinba Checkin
- [x] ET MALWARE DoS.Linux/Elknot.E Checkin
- [ ] ET MALWARE Possible Dyre SSL Cert Sept 15 2014
- [ ] ET MALWARE Possible Dyre SSL Cert Sept 16 2014
- [ ] ET MALWARE Possible Dyre SSL Cert Sept 16 2014
- [ ] ET MALWARE Infostealer.Banprox Proxy.pac Download 2
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [x] ET MALWARE NewPosThings Data Exfiltration
- [ ] ET MALWARE Possible Dyre SSL Cert Sept 19 2014
- [x] ET MALWARE Backdoor.Win32.PcClient.bal CnC (OUTBOUND) 2
- [x] ET MALWARE Backdoor.Win32.PcClient.bal CnC (OUTBOUND)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL certificate detected (KINS CnC)
- [x] ET MALWARE Linux/BillGates Checkin Response
- [x] ET MALWARE Bossabot DDoS tool RFI attempt
- [x] ET MALWARE njrat ver 0.7d Malware CnC Callback (Capture)
- [x] ET MALWARE njrat ver 0.7d Malware CnC Callback (Message)
- [x] ET MALWARE njrat ver 0.7d Malware CnC Callback (Services Listing)
- [x] ET MALWARE njrat ver 0.7d Malware CnC Callback (Process Listing)
- [x] ET MALWARE njrat ver 0.7d Malware CnC Callback (Keylogging)
- [x] ET MALWARE Linux/Yangji.A Checkin
- [ ] ET MALWARE Pushdo v3 Checkin
- [ ] ET MALWARE Infostealer.Boleteiro checking stolen boleto payment information
- [ ] ET MALWARE Possible Dyre SSL Cert Sept 26 2014
- [x] ET MALWARE Windows arp -a Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Windows route Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Syrian Malware Checkin
- [x] ET MALWARE OneLouder EXE download possibly installing Zeus P2P
- [ ] ET MALWARE Possible Upatre SSL Cert bluehost.com Aug 27 2014
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [x] ET MALWARE W32/Threebyte.APT Checkin
- [ ] ET MALWARE Possible Double Flated Encoded Inbound Malicious PDF
- [ ] ET MALWARE Possible Double Flated Encoded Inbound Malicious PDF
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Upatre C2)
- [ ] ET MALWARE Cryptolocker .onion Proxy Domain (erhitnwfvpgajfbu)
- [x] ET MALWARE W32/Bapy.Downloader PE Download Request
- [x] ET MALWARE Backdoor.Win32/Dervec.gen Connectivity Check to Google
- [x] ET MALWARE APT OSX.XSLCmd CnC Beacon
- [x] ET MALWARE Zbot POST Request to C2
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [x] ET MALWARE Possible Malicious Invoice EXE
- [ ] ET MALWARE DecebalPOS Checkin
- [x] ET MALWARE Win.Trojan.Chewbacca connectivity check
- [x] ET MALWARE JackPOS XOR Encoded HTTP Client Body (key AA)
- [x] ET MALWARE Stobox Connectivity Check
- [x] ET MALWARE Tinba Server Response
- [x] ET MALWARE Linux.DDoS Checkin
- [x] ET MALWARE Linux/AES.DDoS Sending Real/Fake CPU&BW Info
- [ ] ET MALWARE MSIL/Spy.RapidStealer.B Checkin
- [x] ET MALWARE Kuluoz/Asprox CnC Response
- [x] ET MALWARE Infostealer.Banprox Proxy.pac Download 3
- [x] ET MALWARE NewPosThings Checkin
- [x] ET MALWARE NewPosThings POST with Fake UA and Accept Header
- [ ] ET MALWARE Backdoor.Win32/PcClient.AA Checkin
- [ ] ET MALWARE Backdoor.Win32.PcClient.bal CnC (OUTBOUND) 3
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [x] ET MALWARE Linux/BillGates Checkin
- [x] ET MALWARE Win32/Neutrino ping
- [ ] ET MALWARE Possible Dyre SSL Cert Sept 22 2014
- [x] ET MALWARE njrat ver 0.7d Malware CnC Callback (Microphone)
- [x] ET MALWARE njrat ver 0.7d Malware CnC Callback (Remote Shell)
- [x] ET MALWARE njrat ver 0.7d Malware CnC Callback (Registry Listing)
- [x] ET MALWARE njrat ver 0.7d Malware CnC Callback (File Manager Actions)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (UPATRE CnC)
- [x] ET MALWARE Possible Tinba DGA NXDOMAIN Responses
- [ ] ET MALWARE Linux/DDoS.M distributed via CVE-2014-6271 Checkin
- [ ] ET MALWARE Possible Dyre SSL Cert Sept 26 2014
- [ ] ET MALWARE Possible Upatre SSL Cert santa.my

- [ ] ET MALWARE Possible Upatre SSL Cert glynwedasia.com
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [x] ET MALWARE BlackEnergy POST Request
- [x] ET MALWARE Linux/ShellshockCampaign.DDOSBot Reporting IP
- [ ] ET MALWARE Linux/ShellshockCampaign.DDOSBot Ping CnC Server Message
- [x] ET MALWARE Linux/ShellshockCampaign.DDOSBot Execute Shell Command CnC Server Message
- [x] ET MALWARE Linux/ShellshockCampaign.DDOSBot UDP Flood CnC Server Message
- [ ] ET MALWARE Linux/ShellshockCampaign.DDOSBot HOLD TCP Flood CnC Server Message
- [x] ET MALWARE Linux/ShellshockCampaign.DDOSBot Terminate Process CnC Server Message
- [ ] ET MALWARE Dyre SSL Cert 2
- [x] ET MALWARE Sourtoff Download Simda Request
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL certificate detected (KINS CnC)
- [ ] ET MALWARE Possible Dyre SSL Cert Sept 30 2014
- [x] ET MALWARE Likely Bot Nick in IRC (Country Code ISO 3166-1 alpha-2)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (UPATRE CnC)
- [x] ET MALWARE Cryptowall 2.0 DL URI Struct Oct 2 2014
- [x] ET MALWARE FAKEIE Minimal Headers (flowbit set)
- [x] ET MALWARE Cryptolocker Checkin
- [ ] ET MALWARE W32/SpyClicker.ClickFraud CnC Beacon
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TeslaCrypt)
- [x] ET MALWARE Gozi/BlackNet Checkin
- [x] ET MALWARE Gozi/Ursnif/Papras Connectivity Check
- [x] ET MALWARE Neverquest Request URI Struct
- [ ] ET MALWARE Possible SandWorm INF Download
- [ ] ET MALWARE Possible SandWorm INF Download (UNICODE)
- [ ] ET MALWARE Possible SandWorm INF Download (SMB UNICODE)
- [x] ET MALWARE W32/BlackEnergy Dirconf CnC Beacon
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [x] ET MALWARE FrameworkPOS Covert DNS CnC Beacon 1
- [x] ET MALWARE Vawtrak/NeverQuest Posting Data
- [x] ET MALWARE Win32/Zemot Requesting PE
- [x] ET MALWARE Win32/Spy.KeyLogger.ODN Checkin
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dyre CnC)
- [x] ET MALWARE Orca RAT URI Struct 1
- [x] ET MALWARE Orca RAT URI Struct 3
- [x] ET MALWARE Possible IRC Bot Common PRIVMSG Commands
- [ ] ET MALWARE Possible Dyre SSL Cert Oct 22 2014
- [x] ET MALWARE W32/24x7Help.ScareWare CnC Beacon
- [x] ET MALWARE Vawtrak/NeverQuest Posting Data
- [x] ET MALWARE Wonton-JH Checkin
- [ ] ET MALWARE BlackEnergy SSL Cert
- [ ] ET MALWARE Possible Upatre SSL Cert www.tradeledstore.co.uk
- [x] ET MALWARE JST Perl IrcBot download
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Backoff CnC)
- [ ] ET MALWARE Win32/Chanitor.A Domain in SNI
- [ ] ET MALWARE Possible Dyre SSL Cert Oct 27 2014
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [x] ET MALWARE BlackEnergy v2 POST Request
- [ ] ET MALWARE Job314 EK Payload Checkin
- [ ] ET MALWARE Linux/ShellshockCampaign.DDOSBot Get Bot IP CnC Server Message
- [ ] ET MALWARE Linux/ShellshockCampaign.DDOSBot Scanner CnC Server Message
- [ ] ET MALWARE Linux/ShellshockCampaign.DDOSBot Random Byte Flood CnC Server Message
- [ ] ET MALWARE Linux/ShellshockCampaign.DDOSBot TCP Flood CnC Server Message
- [ ] ET MALWARE Linux/ShellshockCampaign.DDOSBot Kill Attack CnC Server Message
- [ ] ET MALWARE Dyre SSL Cert 1
- [ ] ET MALWARE Dyre SSL Cert 3
- [x] ET MALWARE Sourtoff Receiving Simda Payload
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (UPATRE CnC)
- [ ] ET MALWARE Possible Dyre SSL Cert Sept 30 2014
- [x] ET MALWARE Likely Bot Nick in IRC (Country Code ISO 3166-1 alpha-3)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [ ] ET MALWARE Possible Upatre SSL Cert mypreschool.sg
- [ ] ET MALWARE Possible Dyre SSL Cert Oct 3 2014
- [x] ET MALWARE Possible CryptoLocker TorComponent DL
- [x] ET MALWARE Reply Sinkhole - irc-sinkhole.cert.pl
- [ ] ET MALWARE SpyClicker.ClickFraud Query Instructions CnC Response
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [x] ET MALWARE Win32/Ursnif Checkin
- [x] ET MALWARE Win32/PSW.Papras.CK file upload
- [x] ET MALWARE Win32/Ursnif Connectivity Check
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL certificate detected (KINS CnC)
- [x] ET MALWARE TorrentLocker DNS Lookup
- [ ] ET MALWARE Possible SandWorm INF Download (SMB)
- [x] ET MALWARE Possible Bedep Connectivity Check
- [ ] ET MALWARE Possible Dyre SSL Cert Oct 15 2014
- [ ] ET MALWARE Possible Dyre SSL Cert Oct 15 2014
- [x] ET MALWARE FrameworkPOS Covert DNS CnC Beacon 2
- [x] ET MALWARE Win32/Zemot URI Struct
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [x] ET MALWARE Possible IRCBot.DDOS Common Commands
- [x] ET MALWARE Dridex POST Checkin
- [x] ET MALWARE Orca RAT URI Struct 2
- [x] ET MALWARE Orca RAT URI Struct 4
- [ ] ET MALWARE Possible Dyre SSL Cert Oct 22 2014
- [ ] ET MALWARE Possible Dyre SSL Cert Oct 22 2014
- [x] ET MALWARE Vawtrak/NeverQuest Server Response
- [x] ET MALWARE Vawtrak/NeverQuest Posting Data
- [ ] ET MALWARE BlackEnergy SSL Cert
- [ ] ET MALWARE Possible Upatre SSL Cert Oct 24 2014
- [x] ET MALWARE DNS Reply Sinkhole - IP - 161.69.13.44
- [x] ET MALWARE W32/Siggen.Dropper CnC Beacon
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [ ] ET MALWARE Win32/Chanitor.A DNS Lookup
- [ ] ET MALWARE Possible Dyre SSL Cert Oct 27 2014

- [ ] ET MALWARE Possible Dyre SSL Cert Oct 27 2014
- [x] ET MALWARE Sednit/AZZY Checkin
- [x] ET MALWARE OLDBAIT Checkin 2 brvc
- [ ] ET MALWARE Ransom.Win32.Blocker.fwlm Checkin
- [x] ET MALWARE Sofacy Request Outbound
- [ ] ET MALWARE Sofacy HTTP Request adobeincorp.com
- [ ] ET MALWARE Sofacy HTTP Request checkmalware.info
- [ ] ET MALWARE Sofacy HTTP Request check-fix.com
- [ ] ET MALWARE Sofacy HTTP Request microsofi.org
- [ ] ET MALWARE Sofacy HTTP Request scanmalware.info
- [ ] ET MALWARE Sofacy HTTP Request securitypractic.com
- [ ] ET MALWARE Sofacy HTTP Request testsnetcontrol.com
- [ ] ET MALWARE Sofacy HTTP Request updatesoftware24.com
- [ ] ET MALWARE Sofacy HTTP Request checkmalware.org
- [x] ET MALWARE Sofacy DNS Lookup adobeincorp.com
- [x] ET MALWARE Sofacy DNS Lookup checkmalware.info
- [x] ET MALWARE Sofacy DNS Lookup check-fix.com
- [x] ET MALWARE Sofacy DNS Lookup microsofi.org
- [x] ET MALWARE Sofacy DNS Lookup scanmalware.info
- [x] ET MALWARE Sofacy DNS Lookup securitypractic.com
- [x] ET MALWARE Sofacy DNS Lookup testservice24.net
- [x] ET MALWARE Sofacy DNS Lookup updatepc.org
- [x] ET MALWARE Sofacy DNS Lookup windows-updater.com
- [ ] ET MALWARE Sofacy HTTP Request symanttec.org
- [ ] ET MALWARE Sofacy HTTP Request msonlinelive.com
- [x] ET MALWARE W32/ZxShell Server Checkin Response
- [ ] ET MALWARE PoisonIvy Keepalive to CnC (Operation SMN Variant)
- [ ] ET MALWARE PoisonIvy Keepalive to CnC (Operation SMN Variant)
- [ ] ET MALWARE FlashPack Payload Download Oct 29
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 43
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [ ] ET MALWARE CryptoBot Downloading Files
- [x] ET MALWARE Possible Tinba DGA NXDOMAIN Responses (2)
- [x] ET MALWARE Win32/Hikit Server Authentication Response
- [ ] ET MALWARE Cohhoc RAT CnC Response
- [ ] ET MALWARE AnubisNetworks Sinkhole TCP Connection
- [x] ET MALWARE Win32.TrojanProxy Configuration file Download
- [x] ET MALWARE DirectsX Checkin Response
- [ ] ET MALWARE Backoff Variant Checkin
- [x] ET MALWARE Sofacy DNS Lookup malwarecheck.info
- [ ] ET MALWARE Shellshock Backdoor.Perl.Shellbot.F retrieval
- [ ] ET MALWARE Bedep SSL Cert
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dyre CnC)
- [x] ET MALWARE Win32/Spy.Banker.ABCG Checkin
- [x] ET MALWARE OSX/WireLurker User-agent (globalupdate)
- [x] ET MALWARE OSX/WireLurker CnC Beacon
- [ ] ET MALWARE iOS/WireLurker CnC Beacon
- [x] ET MALWARE OSX/WireLurker HTTP Request for www.comeinbaby.com
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dyre CnC)
- [x] ET MALWARE Ursnif Checkin
- [x] ET MALWARE Miuref/Boaxxe Checkin
- [ ] ET MALWARE Win32/Roficor.A (Darkhotel) Checkin 2
- [x] ET MALWARE Possible Emotet DGA NXDOMAIN Responses
- [x] ET MALWARE Ponmocup Post Infection DNS Lookup intohave
- [x] ET MALWARE Possible MalDoc Payload Download Nov 11 2014
- [ ] ET MALWARE Possible Dyre SSL Cert Nov 11 2014
- [ ] ET MALWARE Possible Dyre SSL Cert Nov 11 2014
- [ ] ET MALWARE Possible Dyre SSL Cert Nov 11 2014

- [ ] ET MALWARE Possible Dyre SSL Cert Oct 27 2014
- [x] ET MALWARE OLDBAIT Checkin sptr
- [x] ET MALWARE Win32/Chopstick Checkin (APT28 Related)
- [x] ET MALWARE Win32/Coreshell Checkin (APT28 Related)
- [ ] ET MALWARE Sofacy HTTP Request adawareblock.com
- [ ] ET MALWARE Sofacy HTTP Request azureon-line.com
- [ ] ET MALWARE Sofacy HTTP Request checkwinframe.com
- [ ] ET MALWARE Sofacy HTTP Request hotfix-update.com
- [x] ET MALWARE Sofacy HTTP Request microsof-update.com
- [ ] ET MALWARE Sofacy HTTP Request secnetcontrol.com
- [ ] ET MALWARE Sofacy HTTP Request testservice24.net
- [ ] ET MALWARE Sofacy HTTP Request updatepc.org
- [ ] ET MALWARE Sofacy HTTP Request windows-updater.com
- [x] ET MALWARE Sofacy DNS Lookup adawareblock.com
- [x] ET MALWARE Sofacy DNS Lookup azureon-line.com
- [x] ET MALWARE Sofacy DNS Lookup checkwinframe.com
- [ ] ET MALWARE Sofacy DNS Lookup hotfix-update.com
- [x] ET MALWARE Sofacy DNS Lookup microsof-update.com
- [x] ET MALWARE Sofacy DNS Lookup secnetcontrol.com
- [x] ET MALWARE Sofacy DNS Lookup symanttec.org
- [x] ET MALWARE Sofacy DNS Lookup testsnetcontrol.com
- [x] ET MALWARE Sofacy DNS Lookup updatesoftware24.com
- [x] ET MALWARE Sofacy DNS Lookup checkmalware.org
- [x] ET MALWARE CORESHELL Malware Response from server
- [x] ET MALWARE Sofacy DNS Lookup msonlinelive.com
- [ ] ET MALWARE W32/ZxShell Checkin
- [ ] ET MALWARE PoisonIvy Keepalive to CnC (Operation SMN Variant)
- [ ] ET MALWARE PoisonIvy Keepalive to CnC (Operation SMN Variant)
- [x] ET MALWARE Backdoor.Win32.PcClient.bal CnC (OUTBOUND) 4
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS C2)
- [x] ET MALWARE Poweliks Abnormal HTTP Headers high likelihood of Poweliks infection
- [x] ET MALWARE HB_Banker16 Get
- [ ] ET MALWARE Possible EITest Flash Redirect
- [x] ET MALWARE Cohhoc RAT CnC Request
- [ ] ET MALWARE AnubisNetworks Sinkhole SSL Cert lolcat - specific IPs
- [ ] ET MALWARE AnubisNetworks Sinkhole HTTP Response - 195.22.26.192/26
- [ ] ET MALWARE AnubisNetworks Sinkhole UDP Connection
- [ ] ET MALWARE ROM/BackOff C2 SSL Cert
- [ ] ET MALWARE Shellshock Backdoor.Perl.Shellbot.F C2
- [ ] ET MALWARE Sofacy HTTP Request malwarecheck.info
- [ ] ET MALWARE Bedep SSL Cert
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dyre CnC)
- [ ] ET MALWARE Possible Dyre SSL Cert Nov 05 2014
- [x] ET MALWARE Trojan.FakeMS Checkin
- [ ] ET MALWARE OSX/WireLurker Checkin
- [x] ET MALWARE OSX/WireLurker CnC Beacon
- [x] ET MALWARE OSX/WireLurker checkin
- [x] ET MALWARE OSX/WireLurker DNS Query Domain www.comeinbaby.com
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dyre CnC)
- [ ] ET MALWARE Archie EK Payload Checkin POST
- [x] ET MALWARE Win32/Roficor.A (Darkhotel) Checkin 1
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dyre CnC)
- [x] ET MALWARE Emotet Checkin
- [x] ET MALWARE Ponmocup Post Infection DNS Lookup fasternation
- [ ] ET MALWARE Possible Dridex Campaign Download Nov 11 2014
- [ ] ET MALWARE Possible Dyre SSL Cert Nov 11 2014
- [ ] ET MALWARE Possible Dyre SSL Cert Nov 11 2014
- [ ] ET MALWARE Possible Dyre SSL Cert Nov 11 2014
- [x] ET MALWARE Emotet CnC Beacon

- [ ] ET MALWARE Possible Dyre SSL Cert Nov 12 2014
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [ ] ET MALWARE W32Autorun.worm.aaeh Checkin
- [x] ET MALWARE Possible Asprox Pizza
- [x] ET MALWARE Windows executable base64 encoded in XML
- [x] ET MALWARE OSX/WireLurker DNS Query Domain manhuaba.com.cn
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dyre CnC)
- [x] ET MALWARE Malware Connectivity Check to Google
- [x] ET MALWARE Likely CryptoWall 2.0 .onion Proxy domain lookup
- [ ] ET MALWARE W32/AlienSpy RAT Checkin
- [ ] ET MALWARE W32/Matsnu.Backdoor CnC Beacon
- [x] ET MALWARE Bamital Connectivity Check
- [x] ET MALWARE Bamital Checkin
- [x] ET MALWARE Bamital Checkin Response 2
- [x] ET MALWARE Rerdom/Asprox CnC Beacon
- [x] ET MALWARE W32/AntiBreach Possible Activation Attempt
- [x] ET MALWARE CoinVault POST M2
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dyre CnC)
- [ ] ET MALWARE HTTP Request to a *.cvredirect.no-ip.net domain - CoinLocker Domain
- [ ] ET MALWARE HTTP Request to a *.cvredirect.ddns.net domain - CoinLocker Domain
- [x] ET MALWARE W32/DoubleTap.APT Downloader Socks5 Setup Request
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Hesperbot CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dyre CnC)
- [x] ET MALWARE W32/Coinminer.Backdoor CnC Beacon
- [ ] ET MALWARE Trojan/W32.KRBanker.60928.C Checkin
- [x] ET MALWARE Dridex v2 POST Checkin
- [ ] ET MALWARE Possible Dyre SSL Cert (fake org name)
- [x] ET MALWARE HompesA Activity
- [x] ET MALWARE Trojan/MSIL.bfsx Checkin
- [ ] ET MALWARE Vawtrak/NeverQuest Posting Data
- [ ] ET MALWARE Sony Breach Wiper Callout
- [x] ET MALWARE DNS Query for Operation Cleaver Domain
- [x] ET MALWARE DNS Query for Operation Cleaver Domain
- [x] ET MALWARE DNS Query for Operation Cleaver Domain
- [x] ET MALWARE DNS Query for Operation Cleaver Domain
- [x] ET MALWARE DNS Query for Operation Cleaver Domain
- [x] ET MALWARE DNS Query for Operation Cleaver Domain
- [x] ET MALWARE DNS Query for Operation Cleaver Domain
- [x] ET MALWARE DNS Query for Operation Cleaver Domain
- [x] ET MALWARE DNS Query for Operation Cleaver Domain
- [x] ET MALWARE DNS Query for Operation Cleaver Domain
- [x] ET MALWARE DNS Query for Operation Cleaver Domain
- [ ] ET MALWARE MS Office Macro Dridex Download URI Dec 5 2014
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [x] ET MALWARE Possible Dyre DGA NXDOMAIN Responses (.cc)
- [x] ET MALWARE Possible Dyre DGA NXDOMAIN Responses (.to)
- [x] ET MALWARE Possible Dyre DGA NXDOMAIN Responses (.hk)
- [x] ET MALWARE Possible Dyre DGA NXDOMAIN Responses (.tk)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [ ] ET MALWARE VBS/Autorun.J Checkin
- [ ] ET MALWARE W32/Keylogger.CI Checkin
- [x] ET MALWARE Terse alphanumeric executable downloader high likelihood of being hostile
- [x] ET MALWARE Alureon Checkin
- [ ] ET MALWARE Possible Dyre SSL Cert Nov 17 2014
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [x] ET MALWARE OSX/WireLurker HTTP Request for manhuaba.com.cn
- [x] ET MALWARE AlienSpy RAT Checkin Set
- [x] ET MALWARE OSX/AlienSpy RAT Checkin
- [x] ET MALWARE ELF_BASHLITE.SMB Dropping Files
- [x] ET MALWARE Bamital Headers - Likely CnC Beacon
- [ ] ET MALWARE Bamital Checkin Response 1
- [x] ET MALWARE Win32/Zemot Requesting PE
- [x] ET MALWARE Rogue.Win32/FakePAV Checkin
- [ ] ET MALWARE CoinVault POST M1
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dyre CnC)
- [x] ET MALWARE DNS Query for Suspicious cvredirect.no-ip.net Domain - CoinLocker Domain
- [x] ET MALWARE DNS Query for Suspicious cvredirect.ddns.net Domain - CoinLocker Domain
- [x] ET MALWARE W32/DoubleTap.APT Downloader CnC Beacon
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dyre CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dyre CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dyre CnC)
- [x] ET MALWARE W32/Hyteod.Downloader CnC Beacon
- [x] ET MALWARE W32/Wadolin.Downloader CnC Beacon
- [x] ET MALWARE W32/Fin4.InfoStealer Uploading User Credentials CnC Beacon
- [x] ET MALWARE W32/Syndicasec.Backdoor CnC Beacon
- [x] ET MALWARE Possible Dyre SSL Cert (fake state)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [x] ET MALWARE Win32/Swrort.A Checkin 2
- [x] ET MALWARE Upatre Common URI Struct Dec 01 2014
- [ ] ET MALWARE Possible Sony Breach Wiper Malware Download
- [x] ET MALWARE DNS Query for Operation Cleaver Domain
- [x] ET MALWARE DNS Query for Operation Cleaver Domain
- [x] ET MALWARE DNS Query for Operation Cleaver Domain
- [x] ET MALWARE DNS Query for Operation Cleaver Domain
- [x] ET MALWARE DNS Query for Operation Cleaver Domain
- [x] ET MALWARE DNS Query for Operation Cleaver Domain
- [x] ET MALWARE DNS Query for Operation Cleaver Domain
- [x] ET MALWARE DNS Query for Operation Cleaver Domain
- [x] ET MALWARE DNS Query for Operation Cleaver Domain
- [x] ET MALWARE DNS Query for Operation Cleaver Domain
- [x] ET MALWARE DNS Query for Operation Cleaver Domain
- [ ] ET MALWARE Possible Dyre SSL Cert Dec 4 2014
- [ ] ET MALWARE Destover RAT Check-in
- [x] ET MALWARE Chthonic Check-in
- [ ] ET MALWARE Possible Dyre DGA NXDOMAIN Responses (.ws)
- [x] ET MALWARE Possible Dyre DGA NXDOMAIN Responses (.in)
- [ ] ET MALWARE Possible Dyre DGA NXDOMAIN Responses (.cn)
- [x] ET MALWARE Possible Dyre DGA NXDOMAIN Responses (.so)

- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [x] ET MALWARE Backdoor.Linux.Turla Download
- [x] ET MALWARE VirRansom/VirLock Checkin Response
- [ ] ET MALWARE Win32/Critroni Tor DNS Proxy lookup
- [ ] ET MALWARE DNS Query for Cloud Atlas sanygroup.co.uk
- [x] ET MALWARE DNS Query for Cloud Atlas blackberry-support.herokuapp.com
- [x] ET MALWARE Cloud Atlas CnC Beacon
- [ ] ET MALWARE Win32/Dalexis.A Possible SSL Cert (smartoptionsinc.com)
- [ ] ET MALWARE Win32/Dalexis.A Possible SSL Cert (cargol.cat)
- [ ] ET MALWARE Beastdoor Keylogger Report via SMTP
- [x] ET MALWARE Possible Net Crawler SMB Share Access unicode (Operation Cleaver)
- [x] ET MALWARE Trojan.SpamBanker Report via SMTP
- [x] ET MALWARE Trojan/Downloader.Fosniw.sap Reporting via SMTP
- [x] ET MALWARE SpamBanker message
- [ ] ET MALWARE Win32.Bumrat.B Checkin
- [x] ET MALWARE ZhCAT.HackTool Operation Cleaver HTTP CnC Beacon
- [x] ET MALWARE W32/Farfli.BHQ!tr Dropper CnC Beacon
- [x] ET MALWARE W32/Symmi.46846 CnC Beacon
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [x] ET MALWARE Mera Keylogger POSTing keystrokes
- [ ] ET MALWARE Syrian.Slideshow Sending Information via SMTP
- [ ] ET MALWARE Cryptolocker Ransom Page
- [x] ET MALWARE Cryptolocker .onion Proxy Domain
- [x] ET MALWARE Tendrit CnC Beacon 2
- [x] ET MALWARE US-CERT TA14-353A Wiper 2
- [ ] ET MALWARE US-CERT TA14-353A Listening Implant 2
- [ ] ET MALWARE US-CERT TA14-353A Listening Implant 4
- [x] ET MALWARE US-CERT TA14-353A Listening Implant 6
- [ ] ET MALWARE US-CERT TA14-353A Listening Implant 8
- [ ] ET MALWARE US-CERT TA14-353A Listening Implant 10
- [ ] ET MALWARE US-CERT TA14-353A Listening Implant 12
- [x] ET MALWARE US-CERT TA14-353A Lightweight Backdoor 2
- [x] ET MALWARE US-CERT TA14-353A Lightweight Backdoor 4
- [x] ET MALWARE US-CERT TA14-353A Lightweight Backdoor 6
- [x] ET MALWARE US-CERT TA14-353A Lightweight Backdoor 8
- [x] ET MALWARE US-CERT TA14-353A Lightweight Backdoor 10
- [x] ET MALWARE US-CERT TA14-353A Proxy Tool 2
- [ ] ET MALWARE US-CERT TA14-353A WIPER4
- [ ] ET MALWARE Possible VirLock Connectivity Check
- [x] ET MALWARE Win32/Spy.Agent.OHT - AnunakAPT TCP Checkin 1
- [x] ET MALWARE Win32/Spy.Agent.OHT - AnunakAPT TCP Keep-Alive
- [ ] ET MALWARE Win32/Spy.Agent.OHT - AnunakAPT HTTP Checkin Response 1
- [ ] ET MALWARE Win32/Spy.Agent.OHT - AnunakAPT HTTP Checkin Response 2
- [x] ET MALWARE Trojan.Nurjax Downloading PE
- [x] ET MALWARE Trojan.Nurjax Checkin
- [x] ET MALWARE DNS query for known Anunak APT Domain (adguard.name)
- [x] ET MALWARE DNS query for known Anunak APT Domain (ddnservice10.ru)
- [x] ET MALWARE DNS query for known Anunak APT Domain (worldnewsonline.pw)
- [x] ET MALWARE TorrentLocker DNS Lookup (allwayshappy.ru)
- [ ] ET MALWARE TorrentLocker DNS Lookup (cryptdomain.dp.ua)
- [x] ET MALWARE TorrentLocker DNS Lookup (doubleclickads.net)
- [ ] ET MALWARE TorrentLocker DNS Lookup (js-static.ru)
- [ ] ET MALWARE TorrentLocker DNS Lookup (lebanonwarrior.ru)
- [x] ET MALWARE TorrentLocker DNS Lookup (octoberpics.ru)
- [x] ET MALWARE W32/Dridex POST CnC Beacon
- [x] ET MALWARE VirRansom/VirLock Checkin
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Cridex CnC)
- [ ] ET MALWARE DNS Query for Cloud Atlas haarmannsi.cz
- [x] ET MALWARE DNS Query for Cloud Atlas ecolines.es
- [ ] ET MALWARE Cloud Atlas Request to WebDAV CloudMe
- [x] ET MALWARE LinuxNet.perlbot Checkin Via IRC
- [ ] ET MALWARE Win32/Dalexis.A Possible SSL Cert (ppc.cba.pl)
- [x] ET MALWARE HawkEye Keylogger Report SMTP
- [x] ET MALWARE Probable Keylogger Report SMTP
- [x] ET MALWARE Possible Net Crawler SMB Share Access ascii (Operation Cleaver)
- [x] ET MALWARE Trojan/Win32.Espy Report via SMTP
- [x] ET MALWARE DNS query for Known OphionLocker Domain
- [x] ET MALWARE Infostealer.Bancos Sending Stolen info SMTP
- [ ] ET MALWARE W32/TinyZBot Checkin (Operation Cleaver)
- [x] ET MALWARE Trojan.Agent.AIXD Checkin
- [x] ET MALWARE W32/TRCrypt.ULPM Downloader CnC Beacon
- [x] ET MALWARE Win32/Spy.Banker.AAXV Retrieving key from Pinterest
- [ ] ET MALWARE W32/AGENT.NXNX checkin
- [x] ET MALWARE Win32/Poweliks.A Checkin 2
- [ ] ET MALWARE W32/Dridex Distribution Campaign Dec 19 2014
- [ ] ET MALWARE Cryptolocker .onion Proxy Domain
- [x] ET MALWARE Tendrit CnC Beacon 1
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [ ] ET MALWARE US-CERT TA14-353A Listening Implant 1
- [ ] ET MALWARE US-CERT TA14-353A Listening Implant 3
- [ ] ET MALWARE US-CERT TA14-353A Listening Implant 5
- [x] ET MALWARE US-CERT TA14-353A Listening Implant 7
- [ ] ET MALWARE US-CERT TA14-353A Listening Implant 9
- [ ] ET MALWARE US-CERT TA14-353A Listening Implant 11
- [x] ET MALWARE US-CERT TA14-353A Lightweight Backdoor 1
- [ ] ET MALWARE US-CERT TA14-353A Lightweight Backdoor 3
- [x] ET MALWARE US-CERT TA14-353A Lightweight Backdoor 5
- [ ] ET MALWARE US-CERT TA14-353A Lightweight Backdoor 7
- [x] ET MALWARE US-CERT TA14-353A Lightweight Backdoor 9
- [x] ET MALWARE US-CERT TA14-353A Proxy Tool 1
- [x] ET MALWARE US-CERT TA14-353A Proxy Tool 3
- [ ] ET MALWARE Possible Operation Poisoned Helmand jar download
- [ ] ET MALWARE US-CERT TA14-353A Network Propagation Wiper
- [ ] ET MALWARE Win32/Spy.Agent.OHT - AnunakAPT TCP Checkin 2
- [x] ET MALWARE Win32/Spy.Agent.OHT - AnunakAPT HTTP Checkin 1
- [x] ET MALWARE Win32/Spy.Agent.OHT - AnunakAPT HTTP Checkin 2
- [x] ET MALWARE Trojan.Nurjax Retrieving Domains via JS
- [ ] ET MALWARE Possible Trojan.Nurjax SSL Cert
- [x] ET MALWARE DNS query for known Anunak APT Domain (great-codes.com)
- [x] ET MALWARE DNS query for known Anunak APT Domain (coral-trevel.com)
- [x] ET MALWARE DNS query for known Anunak APT Domain (paradise-plaza.com)
- [x] ET MALWARE DNS query for known Anunak APT Domain (update-java.net)
- [ ] ET MALWARE TorrentLocker DNS Lookup (casinoroyal7.ru)
- [x] ET MALWARE TorrentLocker DNS Lookup (deadwalk32.ru)
- [ ] ET MALWARE TorrentLocker DNS Lookup (it-newsblog.ru)
- [ ] ET MALWARE TorrentLocker DNS Lookup (lagosadventures.com)
- [ ] ET MALWARE TorrentLocker DNS Lookup (nigerianbrothers.net)
- [ ] ET MALWARE TorrentLocker DNS Lookup (princeofnigeria.net)

- [ ] ET MALWARE TorrentLocker DNS Lookup (royalgourp.org)
- [x] ET MALWARE TorrentLocker DNS Lookup (ssl-server24.ru)
- [ ] ET MALWARE TorrentLocker DNS Lookup (tweeter-stat.ru)
- [x] ET MALWARE TorrentLocker DNS Lookup (walkingdead32.ru)
- [x] ET MALWARE Dridex Post Check-in Activity
- [x] ET MALWARE DNS query for known Anunak APT Domain (financialnewsonline.pw)
- [ ] ET MALWARE Unknown Dropped by RIG EK
- [x] ET MALWARE Andromeda Checkin Dec 29 2014
- [x] ET MALWARE RocketKitten APT Checkin
- [x] ET MALWARE Kronos Checkin
- [x] ET MALWARE Win64/Havex Checkin
- [x] ET MALWARE Trojan.Generic.5325921 Checkin
- [x] ET MALWARE Win32/Neutrino CC dump
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Malware CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [x] ET MALWARE TinyLoader.A Checkin x64
- [ ] ET MALWARE TinyLoader.A Sending UUID and Processes x64
- [x] ET MALWARE Win32/Recslurp.D C2 Response
- [ ] ET MALWARE Win32/Emotet.C Variant Checkin
- [ ] ET MALWARE Linux/DDoS.M JUNK command
- [ ] ET MALWARE Linux/DDoS.M SCANNER command
- [ ] ET MALWARE Linux/DDoS.M LOLNOGTFO command
- [x] ET MALWARE Win32/Spy.Obator .onion Proxy Domain
- [x] ET MALWARE Possible Office Doc with Embedded VBA containing Reverse Meterpreter Shell
- [x] ET MALWARE Known Sinkhole Response Header CERT.PL
- [x] ET MALWARE Skeleton Key Filename in SMB Traffic (ASCII)
- [x] ET MALWARE Skeleton Key Filename in SMB Traffic (Unicode)
- [x] ET MALWARE Skeleton Key Filename in SMB Traffic (Unicode)
- [x] ET MALWARE Cryptowall 3.0 .onion Proxy Domain
- [x] ET MALWARE Linux/ChinaZ DDoS Bot Checkin
- [x] ET MALWARE Filename svchost.exe Download - Common Hostile Filename
- [x] ET MALWARE Filename hkcmd.exe Download - Common Hostile Filename
- [x] ET MALWARE Win32/Zeprox.B Checkin
- [ ] ET MALWARE Critroni Variant .onion Proxy Domain
- [ ] ET MALWARE Critroni Variant .onion Proxy Domain
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 44
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (URLzone CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dyre CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [x] ET MALWARE Known Sinkhole Response abuse.ch
- [ ] ET MALWARE DNS Query for Suspicious proxy1-1-1.i2p Domain - Possible CryptoWall Activity
- [ ] ET MALWARE DNS Query for Suspicious proxy3-3-3.i2p Domain - Possible CryptoWall Activity
- [ ] ET MALWARE DNS Query for Suspicious proxy5-5-5.i2p Domain - Possible CryptoWall Activity
- [x] ET MALWARE Mazilla Suspicious User-Agent Jan 15 2015
- [x] ET MALWARE Backdoor.TurlaCarbon.A C2 HTTP Request
- [ ] ET MALWARE Scieron Possible SSL Cert
- [x] ET MALWARE Scieron DNS Lookup (autocar.ServeUser.com)
- [ ] ET MALWARE Scieron DNS Lookup (bulldog.toh.info)
- [x] ET MALWARE TorrentLocker DNS Lookup (server38.info)
- [x] ET MALWARE TorrentLocker DNS Lookup (tweeterplanet.ru)
- [x] ET MALWARE TorrentLocker DNS Lookup (updatemyhost.ru)
- [x] ET MALWARE TorrentLocker DNS Lookup (worldnews247.net)
- [x] ET MALWARE DNS query for known Anunak APT Domain (ddnservice11.ru)
- [ ] ET MALWARE TROJ_WHAIM.A message
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [x] ET MALWARE Kronos Checkin M2
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [ ] ET MALWARE Win32.Akdoor Reporting MAC Address
- [x] ET MALWARE Win32/Htbot.B Checkin
- [x] ET MALWARE Win32/Neutrino Cookie
- [x] ET MALWARE Steam Stealer
- [x] ET MALWARE MS Office Macro Dridex Download URI Jan 7 2015
- [x] ET MALWARE TinyLoader.A Checkin x86
- [ ] ET MALWARE TinyLoader.A Sending UUID and Processes x86
- [x] ET MALWARE Win32/Recslurp.D C2 Request (no alert)
- [x] ET MALWARE Win32/Emotet.C Checkin
- [x] ET MALWARE Mini/Cosmic Duke variant FTP upload
- [ ] ET MALWARE Linux/DDoS.M GETLOCALIP command
- [ ] ET MALWARE Linux/DDoS.M KILLATTK command
- [x] ET MALWARE Linux/DDoS.M Admin console status
- [x] ET MALWARE Hong Kong SWC Attack PcClient CnC Beacon
- [x] ET MALWARE Hong Kong SWC Attack DNS Lookup (aoemvp.com)
- [x] ET MALWARE Skeleton Key Filename in SMB Traffic (ASCII)
- [x] ET MALWARE Skeleton Key Filename in SMB Traffic (ASCII)
- [x] ET MALWARE Skeleton Key Filename in SMB Traffic (Unicode)
- [x] ET MALWARE Brontok User-Agent Detected (Rivest)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [x] ET MALWARE Filename explorer.exe Download - Common Hostile Filename
- [x] ET MALWARE Filename server.exe Download - Common Hostile Filename
- [ ] ET MALWARE Possible Mailer Dropped by Dyre SSL Cert
- [x] ET MALWARE Win32.ChinaZ.DDoSClient Checkin
- [ ] ET MALWARE Critroni Variant .onion Proxy Domain
- [x] ET MALWARE Backdoor.Win32.PcClient.bal CnC (OUTBOUND) 5
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dyre CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [ ] ET MALWARE Win32/Nitol.A Checkin M2
- [ ] ET MALWARE Critroni Variant .onion Proxy Domain
- [ ] ET MALWARE DNS Query for Suspicious proxy2-2-2.i2p Domain - Possible CryptoWall Activity
- [ ] ET MALWARE DNS Query for Suspicious proxy4-4-4.i2p Domain - Possible CryptoWall Activity
- [x] ET MALWARE CryptoWall CryptoWall 3.0 Check-in
- [x] ET MALWARE Inception APT malware
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dyre CnC)
- [x] ET MALWARE Scieron DNS Lookup (apple.dynamic-dns.net)
- [ ] ET MALWARE Scieron DNS Lookup (blackblog.chatnook.com)
- [ ] ET MALWARE Scieron DNS Lookup (cew58e.xxxy.info)

- [x] ET MALWARE Scieron DNS Lookup (coastnews.darktech.org)
- [x] ET MALWARE Scieron DNS Lookup (demon.4irc.com)
- [ ] ET MALWARE Scieron DNS Lookup (dynamic.ddns.mobi)
- [ ] ET MALWARE Scieron DNS Lookup (expert.4irc.com)
- [ ] ET MALWARE Scieron DNS Lookup (football.mrbasic.com)
- [ ] ET MALWARE Scieron DNS Lookup (gjjb.flnet.org)
- [ ] ET MALWARE Scieron DNS Lookup (imirnov.ddns.info)
- [ ] ET MALWARE Scieron DNS Lookup (jingnan88.chatnook.com)
- [ ] ET MALWARE Scieron DNS Lookup (lehnjb.epac.to)
- [ ] ET MALWARE Scieron DNS Lookup (logoff.25u.com)
- [x] ET MALWARE Scieron DNS Lookup (logoff.ddns.info)
- [ ] ET MALWARE Scieron DNS Lookup (ls910329.my03.com)
- [ ] ET MALWARE Scieron DNS Lookup (mailru.25u.com)
- [ ] ET MALWARE Scieron DNS Lookup (Markshell.etowns.net)
- [ ] ET MALWARE Scieron DNS Lookup (mydear.ddns.info)
- [ ] ET MALWARE Scieron DNS Lookup (nazgul.zyns.com)
- [ ] ET MALWARE Scieron DNS Lookup (newdyndns.scieron.com)
- [ ] ET MALWARE Scieron DNS Lookup (newoutlook.darktech.org)
- [ ] ET MALWARE Scieron DNS Lookup (photocard.4irc.com)
- [ ] ET MALWARE Scieron DNS Lookup (pricetag.deaftone.com)
- [ ] ET MALWARE Scieron DNS Lookup (rubberduck.gotgeeks.com)
- [ ] ET MALWARE Scieron DNS Lookup (shutdown.25u.com)
- [ ] ET MALWARE Scieron DNS Lookup (sorry.ns2.name)
- [ ] ET MALWARE Scieron DNS Lookup (sskill.b0ne.com)
- [ ] ET MALWARE Scieron DNS Lookup (text-First.flnet.org)
- [ ] ET MALWARE Scieron DNS Lookup (uudog.4pu.com)
- [ ] ET MALWARE Scieron DNS Lookup (will-smith.dtdns.net)
- [ ] ET MALWARE Scieron DNS Lookup (ndcinformation.acmetoy.com)
- [ ] ET MALWARE Scieron DNS Lookup (service.authorizeddns.net)
- [ ] ET MALWARE Scieron DNS Lookup (text-first.trickip.org)
- [x] ET MALWARE Scieron DNS Lookup (yellowblog.flnet.org)
- [ ] ET MALWARE DNS Query for Suspicious crptarv4hcu24ijv Domain - CryptoWall Domains
- [ ] ET MALWARE DNS Query for Suspicious crptbfoi5i54ubez Domain - CryptoWall Domains
- [ ] ET MALWARE DNS Query for Suspicious crptcj7wd4oaafdl Domain - CryptoWall Domains
- [x] ET MALWARE DNS Query for Suspicious tolotor.com Domain - Possible CryptoWall Activity
- [ ] ET MALWARE DNS Query for Suspicious boltotor.com Domain - Possible CryptoWall Activity
- [ ] ET MALWARE DNS Query for Suspicious bonytor2.com Domain - Possible CryptoWall Activity
- [ ] ET MALWARE DNS Query for Suspicious speecostor.com Domain - Possible CryptoWall Activity
- [ ] ET MALWARE Possible Dyre SSL Cert Jan 22 2015
- [x] ET MALWARE Possible Dyre SSL Cert Jan 22 2015
- [x] ET MALWARE Possible Upatre or Dyre SSL Cert Jan 22 2015
- [x] ET MALWARE Generic DNS Query for Suspicious CryptoWall (crpt) Domains
- [x] ET MALWARE W32/Adrom.Backdoor CnC Beacon
- [x] ET MALWARE W32/Upatre.Downloader Encoded Binary Download Request
- [x] ET MALWARE Common Upatre Header Structure 3
- [ ] ET MALWARE Scieron Retrieving Information
- [ ] ET MALWARE Scieron Retrieving Information Response
- [x] ET MALWARE Win32/Scieron-A UA (HTClient)
- [x] ET MALWARE Win32/Scieron-A Checkin via HTTP POST
- [x] ET MALWARE Dridex POST CnC Beacon 2
- [ ] ET MALWARE Dridex Post Checkin Activity 2
- [x] ET MALWARE W32/AGENT.NXNX Checkin 2
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [x] ET MALWARE Regin Hopscotch Module Accessing SMB2 Named Pipe (Unicode) 1
- [x] ET MALWARE Regin Hopscotch Module Accessing SMB Named Pipe (Unicode) 2
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [x] ET MALWARE KL-Remote / Cryp_Banker14 RAT connection
- [x] ET MALWARE KL-Remote / Cryp_Banker14 RAT response
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [ ] ET MALWARE Possible Dridex Campaign Download Jan 28 2015
- [x] ET MALWARE Unknown Mailer CnC Beacon 2
- [ ] ET MALWARE Unknown Mailer CnC Beacon
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [ ] ET MALWARE MSIL/Agent.PYO Retrieving Update
- [ ] ET MALWARE MSIL/Agent.PYO Retrieving Config
- [ ] ET MALWARE MSIL/Agent.PYO Receiving Config
- [x] ET MALWARE MSIL/Agent.PYO Possible net.tcp CnC Beacon (stat)
- [x] ET MALWARE MSIL/Agent.PYO Possible net.tcp CnC Beacon (control)
- [x] ET MALWARE f0xy Checkin
- [ ] ET MALWARE f0xy Checkin
- [ ] ET MALWARE f0xy Download
- [x] ET MALWARE ArcDoor User-Agent (ALIZER)
- [x] ET MALWARE ArcDoor Intial Checkin
- [ ] ET MALWARE BePush/Kilim Checkin
- [ ] ET MALWARE BePush/Kilim Checkin response
- [x] ET MALWARE BePush/Kilim payload retrieval
- [ ] ET MALWARE Possible Dridex e-mail inbound
- [ ] ET MALWARE Critroni Variant .onion Proxy Domain
- [x] ET MALWARE Critroni Variant .onion Proxy Domain
- [x] ET MALWARE Critroni Variant .onion Proxy Domain
- [x] ET MALWARE Critroni Variant .onion Proxy Domain
- [x] ET MALWARE Common Upatre URI/Headers Struct
- [x] ET MALWARE Upatre External IP Check
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 45
- [x] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dyre CnC)
- [x] ET MALWARE Possible DEEP PANDA C2 Activity
- [x] ET MALWARE Sakula/Mivast C2 Activity
- [x] ET MALWARE Possible Deep Panda User-Agent
- [x] ET MALWARE DDoS.XOR Checkin
- [x] ET MALWARE Skeleton Key Filename in SMB2 Traffic
- [x] ET MALWARE Skeleton Key Filename in SMB2 Traffic
- [x] ET MALWARE Skeleton Key Filename in SMB2 Traffic
- [x] ET MALWARE Linux/Xnote Keep-Alive
- [x] ET MALWARE Win32/Rovnix.J Checkin 2
- [x] ET MALWARE HawkEye Keylogger FTP
- [x] ET MALWARE MSIL/Golroted.B Keylogger FTP
- [x] ET MALWARE Predator Pain Keylogger FTP
- [x] ET MALWARE Tinba Checkin 2
- [x] ET MALWARE Upatre Common URI Struct Feb 12 2015
- [ ] ET MALWARE Win32/Gulcrypt.B Downloading components - set
- [ ] ET MALWARE Win32/Gulcrypt.B Downloading components
- [x] ET MALWARE Arid Viper APT Advtravel Campaign GET Request
- [x] ET MALWARE Likely Arid Viper APT Advtravel Campaign GET Keepalive
- [x] ET MALWARE Likely Arid Viper APT Advtravel Campaign POST

- [x] ET MALWARE Arid Viper APT Checkin 1
- [x] ET MALWARE Arid Viper APT Checkin 2
- [x] ET MALWARE Arid Viper APT File information
- [x] ET MALWARE Arid Viper APT Transmitting Date
- [x] ET MALWARE Arid Viper APT Possible User-Agent (Skype)
- [x] ET MALWARE Arid Viper APT DNS Lookup (pstcmedia.com)
- [x] ET MALWARE Arid Viper APT DNS Lookup (ahmedfaiez.info)
- [x] ET MALWARE Arid Viper APT DNS Lookup (flushupate.com)
- [x] ET MALWARE Arid Viper APT DNS Lookup (mediahitech.info)
- [x] ET MALWARE Arid Viper APT Advtravel Campaign DNS Lookup (advtravel.info)
- [x] ET MALWARE Arid Viper APT Advtravel Campaign DNS Lookup (linksis.info)
- [x] ET MALWARE Carbanak APT CnC Beacon 2
- [x] ET MALWARE Desert Falcon APT DNS Lookup (linkedim.in)
- [x] ET MALWARE Desert Falcon APT DNS Lookup (liptona.net)
- [x] ET MALWARE Desert Falcon Related APT DNS Lookup (nice-mobiles.com)
- [x] ET MALWARE Desert Falcon Related APT DNS Lookup (abuhmaid.net)
- [x] ET MALWARE Desert Falcon Related APT DNS Lookup (tvgate.rocks)
- [x] ET MALWARE Babar POST Request
- [x] ET MALWARE Possible Babar POST Request
- [x] ET MALWARE Trojan.NSIS.Comame.A Checkin
- [x] ET MALWARE SuperFish CnC Beacon 2
- [ ] ET MALWARE SuperFish Possible SSL Cert CnC Traffic
- [x] ET MALWARE Win32/HydraCrypt CnC Beacon 3
- [ ] ET MALWARE Win32.Sality.3 Checkin
- [ ] ET MALWARE Netwire RAT Client HeartBeat
- [x] ET MALWARE Tinba Checkin 3
- [ ] ET MALWARE Chanitor .onion Proxy Domain
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 46
- [x] ET MALWARE LogPOS Sending Data
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 48
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 50
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 52
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 54
- [x] ET MALWARE Teerac/CryptoFortress .onion Proxy Domain (3v6e2oe5y5ruimpe)
- [x] ET MALWARE Trojan.Bayrob Keepalive
- [ ] ET MALWARE Possible Upatre SSL Cert www.eshaalfoundation.org
- [x] ET MALWARE Win32/Trapwot FakeAV Post Infection CnC Beacon
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [ ] ET MALWARE Banker Boleto Fraud JS_BROBAN.SM Known Domain (bagacavoltou.ru)
- [ ] ET MALWARE Banker Boleto Fraud JS_BROBAN.SM Firefox Plug-In Download
- [ ] ET MALWARE Banker Boleto Fraud JS_BROBAN.SM Checkin 2
- [x] ET MALWARE Possible malicious Office doc hidden in XML file
- [ ] ET MALWARE Win32/Rofin.A CnC traffic (OUTBOUND)
- [x] ET MALWARE Zbot .onion Proxy Domain
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [x] ET MALWARE Arid Viper APT Exfiltrating files
- [x] ET MALWARE Arid Viper APT Checking filename
- [x] ET MALWARE Arid Viper APT Transmitting Serial
- [x] ET MALWARE Arid Viper APT Possible User-Agent (SK)
- [x] ET MALWARE Arid Viper APT Possible User-Agent (Skypee)
- [x] ET MALWARE Arid Viper APT DNS Lookup (mixedwork.com)
- [x] ET MALWARE Arid Viper APT DNS Lookup (flushupdate.com)
- [x] ET MALWARE Arid Viper APT DNS Lookup (ineltdriver.com)
- [x] ET MALWARE Arid Viper APT DNS Lookup (plmedgroup.com)
- [x] ET MALWARE Arid Viper APT Advtravel Campaign DNS Lookup (fpupdate.info)
- [x] ET MALWARE Carbanak APT CnC Beacon 1
- [x] ET MALWARE Chanitor Variant .onion Proxy Domain
- [x] ET MALWARE Desert Falcon APT DNS Lookup (androcity.com)
- [x] ET MALWARE Desert Falcon Related APT DNS Lookup (nauss-lab.com)
- [x] ET MALWARE Desert Falcon Related APT DNS Lookup (facebook-emoticons.bitblogoo.com)
- [x] ET MALWARE Desert Falcon Related APT DNS Lookup (blogging-host.info)
- [ ] ET MALWARE Dridex POST Retrieving Second Stage
- [x] ET MALWARE Desert Falcon APT DNS Lookup (iwork-sys.com)
- [x] ET MALWARE Win32.Beaugrit.gen.AAAA
- [x] ET MALWARE SuperFish CnC Beacon 1
- [x] ET MALWARE Possible Bedep Connectivity Check (2)
- [x] ET MALWARE SuperFish Possible SSL Cert Signed By Compromised Root CA
- [x] ET MALWARE Win32/LockScreen CnC Beacon 2
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [x] ET MALWARE Unknown Trojan Downloading PE via MSSQL Connection to Non-Standard Port
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (CryptoLocker CnC)
- [ ] ET MALWARE Xunpf.A Retrieving DLL
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 47
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 49
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 51
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 53
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 55
- [ ] ET MALWARE Teerac/CryptoFortress .onion Proxy Domain (h63rbx7gkd3gygag)
- [x] ET MALWARE rechnung zip file download
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [x] ET MALWARE Win32/Trapwot FakeAV Checkin
- [ ] ET MALWARE Banker Boleto Fraud JS_BROBAN.SM Known Domain (bagacaoutra.ru)
- [ ] ET MALWARE Banker Boleto Fraud JS_BROBAN.SM Known Domain (bagacaveia.ru)
- [ ] ET MALWARE Banker Boleto Fraud JS_BROBAN.SM Checkin 1
- [x] ET MALWARE Banker Boleto Fraud JS_BROBAN.SM Checkin 3
- [ ] ET MALWARE Cryptolocker .onion Proxy Domain (juf5pjk4sl7uojh4)
- [x] ET MALWARE Gamarue/Andromeda Downloading Payload
- [ ] ET MALWARE Cryptolocker .onion Proxy Domain (4elcqmis624seeo7)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)

- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Ransomware CnC)
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 56
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 58
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 60
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [ ] ET MALWARE VaultCrypt Uploading Files
- [x] ET MALWARE 9002 RAT C&C DNS request
- [x] ET MALWARE Win32/Teslacrypt Ransomware HTTP CnC Beacon M1
- [x] ET MALWARE FindPOS Checkin
- [ ] ET MALWARE Zbot .onion Proxy Domain (3bjpwsf3fjcwtnwx)
- [x] ET MALWARE Fileless infection dropped by EK CnC Beacon
- [x] ET MALWARE Win32/TrojanProxy.JpiProx.B CnC Beacon 1
- [x] ET MALWARE Chanitor .onion Proxy Domain (l7gbml27czk3kvr5)
- [x] ET MALWARE Win32.Hyteod.acox Domain Generation Algorithm (DGA) Lookup NXDOMAIN Response
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [x] ET MALWARE Win32.Chroject.B Requesting ClickFraud Commands from CnC
- [x] ET MALWARE Win32.Chroject.B Receiving ClickFraud Commands from CnC 2
- [ ] ET MALWARE VBA Office Document Dridex Binary Download User-Agent
- [ ] ET MALWARE Vawtrak/NeverQuest .onion Proxy Domain (4bpthx5z4e7n6gnb)
- [x] ET MALWARE Vawtrak/NeverQuest .onion Proxy Domain (llgerw4plyyff446)
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 63
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 65
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 67
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 69
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 71
- [ ] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 73
- [ ] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 75
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 77
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 79
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 81
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 83
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 85
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 87
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 89
- [ ] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 91
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 93
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 95
- [ ] ET MALWARE Vicepass CnC Beacon
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 57
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 59
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 61
- [x] ET MALWARE FakeAV Variant CnC Beacon
- [x] ET MALWARE Win32/Agent.WMN CnC Beacon
- [ ] ET MALWARE HOMEUNIX/9002 CnC Beacon
- [x] ET MALWARE Win32/Teslacrypt Ransomware HTTP CnC Beacon M2
- [x] ET MALWARE KeyLogger related to FindPOS CnC Beacon
- [x] ET MALWARE Possible Adwind/jSocket SSL Cert (assylias.Inc)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Ransomware CnC)
- [x] ET MALWARE Win32/TrojanProxy.JpiProx.B CnC Beacon 2
- [x] ET MALWARE CryptoLocker .onion Proxy Domain (iezqmd4s2fflmh7n)
- [x] ET MALWARE Win32.Hyteod.acox Domain Generation Algorithm (DGA) Lookup NXDOMAIN Response
- [x] ET MALWARE Win32.Chroject.B Retrieving encoded payload
- [ ] ET MALWARE Win32.Chroject.B Receiving ClickFraud Commands from CnC 1
- [x] ET MALWARE Win32.Chroject.B ClickFraud Request
- [ ] ET MALWARE Vawtrak/NeverQuest .onion Proxy Domain (otsaa35gxbcwvrqs)
- [ ] ET MALWARE Vawtrak/NeverQuest .onion Proxy Domain (bc3ywvif4m3lnw4o)
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 62
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 64
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 66
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 68
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 70
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 72
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 74
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 76
- [ ] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 78
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 80
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 82
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 84
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 86
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 88
- [ ] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 90
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 92
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 94
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 96

- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 97
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 98
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 99
- [x] ET MALWARE Skyfall fake Skype install link
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Ransomware CnC)
- [ ] ET MALWARE VBA Office Document Dridex Binary Download User-Agent 2
- [ ] ET MALWARE Volatile Cedar Win32.Explosive CnC Beacon 1
- [ ] ET MALWARE Volatile Cedar Win32.Explosive CnC Beacon 2
- [x] ET MALWARE Volatile Cedar Win32.Explosive CnC Beacon 3
- [x] ET MALWARE Volatile Cedar Win32.Explosive Fake User-Agent
- [ ] ET MALWARE Volatile Cedar Win32.Explosive External IP Leak
- [x] ET MALWARE Volatile Cedar Win32.Explosive HTTP CnC Beacon 1
- [x] ET MALWARE Volatile Cedar Win32.Explosive HTTP CnC Beacon 1
- [x] ET MALWARE Volatile Cedar DNS Lookup (saveweb.wink.ws)
- [x] ET MALWARE Volatile Cedar DNS Lookup (carima2012.site90.com)
- [x] ET MALWARE Volatile Cedar DNS Lookup (explorerdotnt.info)
- [x] ET MALWARE Volatile Cedar DNS Lookup (dotnetexplorer.info)
- [x] ET MALWARE Volatile Cedar DNS Lookup (dotntexplorere.info)
- [x] ET MALWARE Volatile Cedar DNS Lookup (xploreredotnet.info)
- [x] ET MALWARE Volatile Cedar DNS Lookup (erdotntexplore.info)
- [x] ET MALWARE Win32/Hyteod CnC Beacon
- [x] ET MALWARE Dridex POST Retrieving Second Stage M2
- [x] ET MALWARE Potential Dridex.Maldoc Minimal Executable Request
- [x] ET MALWARE Win32/LockScreen.BW Payment Info
- [x] ET MALWARE Win32/LockScreen.BW Payment Info 2
- [ ] ET MALWARE Win32/LockScreen.BW Checkin
- [x] ET MALWARE Win32/Injector.BXEW Variant HTTP CnC Beacon 1
- [x] ET MALWARE Win32/Injector.BXEW Variant HTTP CnC Beacon 2
- [x] ET MALWARE Win32/Injector.BXEW Variant HTTP CnC Beacon 3
- [ ] ET MALWARE IRC Bot dropped by Mikey Variant CnC Beacon
- [ ] ET MALWARE Malicious Doc Download EXE Primer (flowbits set)
- [ ] ET MALWARE Malicious Doc Downloading EXE
- [x] ET MALWARE Win32/Teslacrypt Ransomware .onion domain (63ghdye17.com)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [x] ET MALWARE Win32/Teslacrypt Ransomware .onion domain (7hwr34n18.com)
- [x] ET MALWARE Possible Win32/SillyFDC WordPress Traffic
- [ ] ET MALWARE Possible Upatre DNS Query (jamco .com .pk)
- [x] ET MALWARE TinyLoader.B1 Checkin x86
- [x] ET MALWARE TinyLoader.B1 Checkin x64
- [x] ET MALWARE TinyLoader.B2 Checkin no architecture
- [x] ET MALWARE TinyLoader.B1 Sending Processes
- [x] ET MALWARE CryptoWall Check-in M2
- [ ] ET MALWARE Malicious Office Doc CnC Beacon
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [ ] ET MALWARE Possible Dridex downloader SSL Certificate srv1.mainsftdomain.com
- [x] ET MALWARE Win32/Teslacrypt Ransomware .onion domain (wh47f2as19.com)
- [x] ET MALWARE Win32/Teslacrypt Ransomware .onion domain (epmhyca5ol6plmx3)
- [x] ET MALWARE Kriptovor Checkin
- [x] ET MALWARE Kriptovor SMTP Traffic
- [x] ET MALWARE Kriptovor Retrieving RAR Payload
- [x] ET MALWARE Kriptovor External IP Lookup checkip.dyndns.org
- [ ] ET MALWARE Shellshock Worm Checkin
- [x] ET MALWARE Vobus/Beebone Sinkhole DNS Reply
- [ ] ET MALWARE Operation Buhtrap CnC Beacon 1
- [x] ET MALWARE Operation Buhtrap CnC Beacon 2
- [x] ET MALWARE Possible Maldoc Retrieving Dridex from pastebin
- [x] ET MALWARE Possible APT30 or Win32/Nuclear HTTP Framework
- [x] ET MALWARE Possible APT30 or Win32/Nuclear HTTP Framework POST
- [x] ET MALWARE Emotet v2 Exfiltrating Outlook information
- [ ] ET MALWARE Possible APT30 Fake Mozilla UA
- [x] ET MALWARE LankerBoy HTTP CnC Beacon
- [ ] ET MALWARE CoinVault Mailer CnC Beacon
- [x] ET MALWARE CoinVault CnC Beacon M1
- [x] ET MALWARE CoinVault CnC Beacon M2
- [ ] ET MALWARE CoinVault CnC Beacon Response
- [x] ET MALWARE Win32/Ruckguv.A Requesting Payload
- [x] ET MALWARE Likely Trojan Multi-part Macro Download M1
- [x] ET MALWARE W32/Farfli.BHQ!tr Dropper CnC Beacon 2
- [ ] ET MALWARE CryptoLocker .onion Proxy Domain (33p5mqkaj22irv4z)
- [x] ET MALWARE FighterPOS CnC Beacon 1
- [x] ET MALWARE FighterPOS CnC Beacon 2
- [ ] ET MALWARE FighterPOS CnC Beacon 3
- [x] ET MALWARE Sysget/HelloBridge HTTP GET CnC Beacon
- [ ] ET MALWARE Sysget/HelloBridge HTTP POST CnC Beacon
- [ ] ET MALWARE Unit42 PoisonIvy Keepalive to CnC
- [x] ET MALWARE Zacom/NFlog HTTP POST Connectivity Check
- [x] ET MALWARE Zacom/NFlog HTTP POST Fake UA CnC Beacon
- [ ] ET MALWARE FormerFirstRAT HTTP POST CnC Beacon
- [ ] ET MALWARE Bioazih RAT Checkin
- [x] ET MALWARE Zacom/NFlog Checkin
- [ ] ET MALWARE Possible Dalexis downloader encrypted binary (1)
- [ ] ET MALWARE Possible Dalexis downloader encrypted binary (2)
- [ ] ET MALWARE Possible Dalexis downloader encrypted binary (3)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [x] ET MALWARE Dalexis CnC Beacon
- [x] ET MALWARE PunkeyPOS HTTP CnC Beacon Fake UA
- [x] ET MALWARE PunkeyPOS HTTP CnC Beacon 1
- [x] ET MALWARE PunkeyPOS HTTP CnC Beacon 2
- [x] ET MALWARE PunkeyPOS HTTP CnC Beacon 3
- [x] ET MALWARE PunkeyPOS HTTP CnC Beacon 4
- [ ] ET MALWARE PunkeyPOS HTTP CnC Beacon 5
- [ ] ET MALWARE PunkeyPOS HTTP CnC Beacon 6
- [x] ET MALWARE Potential Dridex.Maldoc Minimal Executable Request
- [x] ET MALWARE Win32/Filecoder Ransomware Variant .onion Proxy Domain (tkj3higtqlvohs7z)
- [ ] ET MALWARE Possible Dridex downloader SSL Certificate
- [x] ET MALWARE Chthonic CnC Beacon 5
- [x] ET MALWARE Win32/Tesch.B CnC Beacon
- [x] ET MALWARE Chthonic CnC Beacon 6
- [x] ET MALWARE Win32/StreamFlaw.A Checkin
- [x] ET MALWARE Win32/Neutrino Bot Fake 404 Checkin Response
- [ ] ET MALWARE CryptoLocker .onion Proxy Domain (pf3tlgkpks7pu7yr)
- [ ] ET MALWARE CryptoLocker .onion Proxy Domain (v7lfogalalzc2c4d)
- [x] ET MALWARE Windows nbtstat -a Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Windows nbtstat -n Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Windows nbtstat -s Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE CryptoLocker .onion Proxy Domain (zoqowm4kzz4cvvvl)
- [x] ET MALWARE CryptoWall .onion Proxy Domain (7oqnsnzwwnm6zb7y)
- [ ] ET MALWARE Possible Graftor Downloading Dridex

- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [x] ET MALWARE CozyDuke APT HTTP GET CnC Beacon
- [x] ET MALWARE CozyDuke APT HTTP POST CnC Beacon
- [x] ET MALWARE CozyDuke APT HTTP CnC Beacon Response
- [x] ET MALWARE CozyDuke APT Possible SSL Cert 1
- [x] ET MALWARE CozyDuke APT Possible SSL Cert 2
- [x] ET MALWARE CozyDuke APT Possible SSL Cert 3
- [x] ET MALWARE CozyDuke APT Possible SSL Cert 4
- [x] ET MALWARE CozyDuke APT Possible SSL Cert 5
- [x] ET MALWARE CozyDuke APT Possible SSL Cert 6
- [x] ET MALWARE CozyDuke APT Possible SSL Cert 7
- [x] ET MALWARE CozyDuke APT Possible SSL Cert 8
- [x] ET MALWARE DDoS.Win32.Agent.bay Variant Covert Channel (VERSONEX)
- [ ] ET MALWARE Possible Dridex Downloader SSL Certificate
- [x] ET MALWARE Email Contains InternetOpen WinInet API Call - Potentially Dridex MalDoc 1
- [x] ET MALWARE Email Contains InternetOpen WinInet API Call - Potentially Dridex MalDoc 2
- [x] ET MALWARE Email Contains InternetOpen WinInet API Call - Potentially Dridex MalDoc 3
- [x] ET MALWARE Email Contains wininet.dll Call - Potentially Dridex MalDoc 1
- [x] ET MALWARE Email Contains wininet.dll Call - Potentially Dridex MalDoc 2
- [x] ET MALWARE Email Contains wininet.dll Call - Potentially Dridex MalDoc 3
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 100
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)
- [ ] ET MALWARE TorrentLocker SSL Cert
- [ ] ET MALWARE Win32/Ruckguv.A SSL Cert
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Ransomware CnC)
- [x] ET MALWARE Dalexis Downloading EXE
- [x] ET MALWARE MewsSpy/NionSpy .onion Proxy Domain (z3mm6cupmtw5b2xx)
- [x] ET MALWARE Kaspersky Sinkhole DNS Reply
- [x] ET MALWARE Wapack Labs Sinkhole DNS Reply
- [x] ET MALWARE Downeks Checkin
- [ ] ET MALWARE Downeks Checkin 2
- [x] ET MALWARE BePush/Kilim CnC Beacon
- [ ] ET MALWARE Malicious SSL Cert (KINS C2)
- [ ] ET MALWARE Malicious SSL Cert (KINS C2)
- [ ] ET MALWARE Teerac/CryptoFortress .onion Proxy Domain (cld7vqwcvn2bii67)
- [x] ET MALWARE Linux/DDoS.Sotdas/IptabLex Checkin
- [x] ET MALWARE Linux.Trojan.IptabLex Variant Checkin
- [x] ET MALWARE Linux.Mumblehard Initial Checkin
- [x] ET MALWARE Linux.Mumblehard Command Status CnC
- [x] ET MALWARE Linux.Mumblehard Spam Command CnC
- [ ] ET MALWARE Carbon FormGrabber/Retgate.A/Rombertik Checkin
- [ ] ET MALWARE Dyre Downloading Mailer 2
- [x] ET MALWARE njRAT Variant Outbound CnC Beacon
- [ ] ET MALWARE Ursnif SSL Cert
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Ransomware CnC)
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 101
- [ ] ET MALWARE TeslaCrypt/AlphaCrypt Variant .onion Proxy Domain (is6xsotjdy4qtgur)
- [x] ET MALWARE Enfal CnC POST
- [x] ET MALWARE Enfal CnC GET
- [x] ET MALWARE Possible CryptoPHP Leaking Credentials May 8 2015 M1
- [x] ET MALWARE Possible CryptoPHP Leaking Credentials May 8 2015 M2
- [x] ET MALWARE Possible CryptoPHP Leaking Credentials May 8 2015 M3
- [x] ET MALWARE TeslaCrypt/AlphaCrypt Variant .onion Proxy Domain (iq3ahijcfeont3xx)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Ransomware CnC)
- [x] ET MALWARE Win32/Agent.WVW CnC Beacon 2
- [ ] ET MALWARE VaultCrypt Checkin
- [ ] ET MALWARE Possible Dridex Remote Macro Download
- [ ] ET MALWARE Putty SSH Credential Stealer
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Malware CnC)
- [ ] ET MALWARE Win32/Ruckguv.A SSL Cert
- [x] ET MALWARE Generic Dropper Installing PUP 2
- [x] ET MALWARE Generic Dropper Installing PUP 1
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex CnC)
- [x] ET MALWARE FrauDrop Checkin
- [x] ET MALWARE FrauDrop UA LETITGO
- [x] ET MALWARE FrauDrop UA single
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex CnC)
- [x] ET MALWARE Win32/Zemot Fake Search Page
- [x] ET MALWARE APT Hellsing Proxy Checker Checkin
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Ransomware CnC)
- [x] ET MALWARE DDoS.Win32/Nitol.B Checkin
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dyre CnC)
- [x] ET MALWARE Yahoyah CnC Beacon
- [ ] ET MALWARE CTB-Locker .onion Proxy Domain (tlunjscxn5n76iyz)
- [x] ET MALWARE Possible APT17 CnC Content in Public Website
- [x] ET MALWARE SPEAR CnC Beacon
- [x] ET MALWARE SPEAR CnC Beacon 2
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [ ] ET MALWARE Worm.VBS.Jenxcus.H URL Structure
- [x] ET MALWARE Worm.VBS.Jenxcus.H User Agent
- [x] ET MALWARE Blue Bot DDoS Proxy Request
- [x] ET MALWARE Blue Bot DDoS Blog Request
- [x] ET MALWARE Blue Bot DDoS Target Request
- [x] ET MALWARE Blue Bot DDoS Logger Request
- [x] ET MALWARE JavaScriptBackdoor HTTP GET CnC Beacon
- [ ] ET MALWARE JavaScriptBackdoor HTTP POST CnC Beacon
- [ ] ET MALWARE JavaScriptBackdoor SSL Cert
- [x] ET MALWARE H1N1 Loader CnC Beacon M1
- [x] ET MALWARE H1N1 Loader CnC Beacon M2
- [x] ET MALWARE Win32/Bancos URL Structure
- [x] ET MALWARE MSIL/Autorun.AD Checkin
- [x] ET MALWARE Nitlove POS CnC
- [ ] ET MALWARE Likely Dridex SSL Cert
- [x] ET MALWARE Linux/Moose HTTP CnC Beacon

- [x] ET MALWARE Linux/Moose HTTP CnC Beacon Response
- [x] ET MALWARE Linux/Moose NAT Traversal CnC Beacon set
- [x] ET MALWARE Linux/Moose NAT Traversal CnC Beacon - Multiple Tunnel
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dyre CnC)
- [x] ET MALWARE Win32/Gatak.DR Payload Instructions
- [ ] ET MALWARE DNS Query to TOX Ransomware onion (xwxwninkssujglja)
- [ ] ET MALWARE PunkeyPOS HTTP CnC Beacon 7
- [x] ET MALWARE PunkeyPOS HTTP CnC Beacon 9
- [ ] ET MALWARE Bladabindi/njRAT CnC Command (ll)
- [x] ET MALWARE Possible BlackEnergy Accessing SMB/SMB2 Named Pipe (Unicode)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex CnC)
- [x] ET MALWARE KeyBase Keylogger Checkin
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Geodo MITM)
- [ ] ET MALWARE Qadars WebInject SSL Cert
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Geodo MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Geodo MITM)
- [x] ET MALWARE Sakula/Mivast RAT CnC Beacon 3
- [x] ET MALWARE DNS Query to TOX Ransomware onion (toxicola7qwv37qj)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Geodo MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Geodo MITM)
- [x] ET MALWARE Win32/Zacom.A CnC Beacon 1
- [x] ET MALWARE IsSpace/Zacom Connectivity Check
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Geodo MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Geodo MITM)
- [x] ET MALWARE Poweliks Clickfraud CnC M1
- [x] ET MALWARE Poweliks Clickfraud CnC M3
- [x] ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (ASCII) 1
- [x] ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (ASCII) 3
- [x] ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (ASCII) 5
- [x] ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (Unicode) 1
- [x] ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (Unicode) 3
- [x] ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (Unicode) 5
- [x] ET MALWARE Possible Duqu 2.0 Accessing backdoor over 443
- [x] ET MALWARE Possible Dridex Download URI Struct with no referer
- [x] ET MALWARE Possible Duqu 2.0 Request
- [ ] ET MALWARE TorrentLocker .onion Proxy Domain (zbqxpjfvltb6d62m)
- [x] ET MALWARE Win32/Agent.WVW CnC Beacon 1
- [ ] ET MALWARE Torrentlocker C2 SSL cert
- [x] ET MALWARE Win32/Chinad Checkin
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TeslaCrypt MITM)
- [x] ET MALWARE Backdoor.Elise CnC Beacon 1 M2
- [x] ET MALWARE Backdoor.Elise CnC Beacon 3 M1
- [x] ET MALWARE Possible Linux/Moose Telnet CnC Beacon
- [x] ET MALWARE Linux/Moose NAT Traversal CnC Beacon - Sleep
- [ ] ET MALWARE Wordpress Errorcontent CnC Beacon
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Yakes CnC)
- [ ] ET MALWARE DNS Query to TOX Ransomware onion (wdthvb6jut2rupu4)
- [ ] ET MALWARE DNS Query to TOX Ransomware onion (7fa6gldxg64t5wnt)
- [ ] ET MALWARE PunkeyPOS HTTP CnC Beacon 8
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Downloader CnC)
- [x] ET MALWARE Possible BlackEnergy Accessing SMB/SMB2 Named Pipe (ASCII)
- [x] ET MALWARE APT Backspace CnC Beacon
- [x] ET MALWARE IOS.Oneclickfraud HTTP Host
- [x] ET MALWARE Databack CnC
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gootkit CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Spy.Shiz CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Geodo MITM)
- [x] ET MALWARE Sakula/Mivast RAT CnC Beacon 2
- [x] ET MALWARE Possible Deep Panda - Sakula/Mivast RAT CnC Beacon 5
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Geodo MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Geodo MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Geodo MITM)
- [ ] ET MALWARE Win32/Zacom.A CnC Beacon 2
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Geodo MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Geodo MITM)
- [x] ET MALWARE Poweliks Clickfraud CnC M2
- [x] ET MALWARE Scanbox Sending Host Data
- [x] ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (ASCII) 2
- [x] ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (ASCII) 4
- [x] ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (ASCII) 6
- [x] ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (Unicode) 2
- [x] ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (Unicode) 4
- [x] ET MALWARE Possible Duqu 2.0 Accessing SMB/SMB2 Named Pipe (Unicode) 6
- [ ] ET MALWARE Dridex Download June 10 2015
- [x] ET MALWARE Win32/Gatak.DR Activity
- [x] ET MALWARE Poweliks Clickfraud CnC M4
- [ ] ET MALWARE Torrentlocker C2 Domain in SNI
- [x] ET MALWARE Win32/Agent.WVW CnC Beacon 3
- [x] ET MALWARE Win32/Chinad Retrieving Config
- [x] ET MALWARE Gatak CnC
- [x] ET MALWARE Backdoor.Elise CnC Beacon 1 M1
- [x] ET MALWARE Backdoor.Elise CnC Beacon 2
- [x] ET MALWARE Backdoor.Elise CnC Beacon 3 M2

☐ ET MALWARE Backdoor.Elise SSL Cert
☑ ET MALWARE Malicious SSL certificate detected (FindPOS)
☑ ET MALWARE Downloader.Win32.Adload (KaiXin Payload) Config Download
☑ ET MALWARE Downloader.Win32.Adload (KaiXin Payload) Checkin Response
☐ ET MALWARE TeslaCrypt/AlphaCrypt Variant .onion Proxy Domain (gzc7lj4rvmkg25dm)
☑ ET MALWARE Likely Malicious wininet UA Downloading EXE
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Possible Sinkhole)
☑ ET MALWARE Win32/Ascrirac .onion proxy Domain (5sse6j4kdaeh3yus)
☐ ET MALWARE AlphaCrypt .onion proxy Domain (tkjthigtqlvohs7z)
☐ ET MALWARE CryptoLocker .onion Proxy Domain (xvha2ctkacx2ug3b)
☑ ET MALWARE Likely Linux/Xorddos.F DDoS Attack Participation (ns1.hostasa.org)
☑ ET MALWARE Likely Linux/Xorddos.F DDoS Attack Participation (ns3.hostasa.org)
☑ ET MALWARE Likely Linux/Xorddos.F DDoS Attack Participation (gh.dsaj2a1.org)
☑ ET MALWARE Likely Linux/Xorddos.F DDoS Attack Participation (wangzongfacai.com)
☑ ET MALWARE DDoS.XOR Checkin 3
☑ ET MALWARE Win32/Vflooder.C Connectivity Check
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex CnC)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
☐ ET MALWARE Dridex SSL Cert 30 June 2015
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi CnC)
☐ ET MALWARE UpDocX Download
☑ ET MALWARE Zberp receiving config via image file - SET
☑ ET MALWARE Zberp/ZeusVM receiving config via image file (steganography) 2
☐ ET MALWARE Likely Dridex SSL Cert
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dyre CnC)
☐ ET MALWARE Wekby PCRat/Gh0st CnC Beacon (Outbound)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (CryptoLocker CnC)
☑ ET MALWARE W32/Banload.VZS Banker POST CnC Beacon 1
☑ ET MALWARE Likely Linux/Xorddos DDoS Attack Participation (gggatat456.com)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Spy.Shiz CnC)
☑ ET MALWARE BernhardPOS Possible Data Exfiltration via DNS Lookup (29a.de)
☑ ET MALWARE Bedep HTTP POST CnC Beacon
☑ ET MALWARE APT CozyCar SSL Cert 3
☑ ET MALWARE APT CozyCar SSL Cert 6

☐ ET MALWARE W2KM_BARTALEX Downloading Payload
☐ ET MALWARE Netwire RAT Client Check-in 2
☐ ET MALWARE Downloader.Win32.Adload (KaiXin Payload) Checkin
☐ ET MALWARE TeslaCrypt/AlphaCrypt Variant .onion Proxy Domain (bpq4dub4rlivvswu)
☑ ET MALWARE W2KM_BARTALEX Downloading Payload 2
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Spy.Shiz CnC)
☑ ET MALWARE Linux/ChinaZ DDoS Bot Checkin 2
☐ ET MALWARE Ransomware Variant .onion proxy Domain (kurrmpfx6kgmsopm)
☑ ET MALWARE Gozi/Ursnif/Papras Grabftp Module Download
☑ ET MALWARE Likely Linux/Xorddos.F DDoS Attack Participation (aa.hostasa.org)
☑ ET MALWARE Likely Linux/Xorddos.F DDoS Attack Participation (ns2.hostasa.org)
☑ ET MALWARE Likely Linux/Xorddos.F DDoS Attack Participation (ns4.hostasa.org)
☑ ET MALWARE Likely Linux/Xorddos.F DDoS Attack Participation (navert0p.com)
☑ ET MALWARE DDoS.XOR Checkin 2
☑ ET MALWARE DDoS.XOR Checkin via HTTP
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
☐ ET MALWARE ELF.DES.Downloader Request
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Ransomware CnC)
☑ ET MALWARE AlphaCrypt .onion Proxy Domain (djdkduep62kz4nzx)
☐ ET MALWARE Dridex SSL Cert 1 July 2015
☐ ET MALWARE UpDocX Checkin
☑ ET MALWARE Mocelpa Client Hello CnC Beacon
☑ ET MALWARE Zberp/ZeusVM receiving config via image file (steganography)
☑ ET MALWARE Win32/Denisca.A CnC Beacon
☑ ET MALWARE Win32/Denisca.A CnC Beacon 2
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex CnC)
☐ ET MALWARE Wekby PCRat/Gh0st CnC Beacon (Inbound)
☑ ET MALWARE Matsnu Checkin
☑ ET MALWARE W32/Banload.VZS Banker POST CnC Beacon 2
☑ ET MALWARE Likely Linux/Xorddos DDoS Attack Participation (xxxatat456.com)
☑ ET MALWARE SeaDuke CnC Beacon
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Ransomware CnC)
☑ ET MALWARE APT CozyCar SSL Cert 2
☑ ET MALWARE APT CozyCar SSL Cert 5
☑ ET MALWARE APT CozyCar SSL Cert 7

- [x] ET MALWARE APT CozyCar SSL Cert 8
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dyre CnC)
- [ ] ET MALWARE Possible IE MSMXL Detection of Local SYS (Likely Malicious)
- [x] ET MALWARE Possible Dyre SSL Cert M1 (L O)
- [x] ET MALWARE Possible Dyre SSL Cert M3 (O CN)
- [x] ET MALWARE Tsyrval Panda CnC Beacon
- [x] ET MALWARE KeyBase Keylogger HTTP Pattern
- [x] ET MALWARE Win32.Rioselx.A Checkin
- [x] ET MALWARE Likely Linux/IptabLesX C2 Domain Lookup (GroUndHog.MapSnode.CoM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Ransomware CnC)
- [ ] ET MALWARE Jiripbot CnC 2
- [ ] ET MALWARE Java/QRat Receiving Command 1
- [x] ET MALWARE Sednit Connectivity Check 0 Byte POST
- [x] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex CnC)
- [x] ET MALWARE PoisonIvy HTTP CnC Beacon
- [x] ET MALWARE Linux/ChinaZ 2.0 DDoS Bot Checkin 3
- [x] ET MALWARE KINS/ZeusVM Variant Retrieving Config
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE W2KM_BARTALEX Downloading Payload M2
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Ransomware CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi CnC)
- [ ] ET MALWARE CryptoLocker .onion Proxy Domain (vacdgwaw5djp5hmu)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (VMZeuS MITM)
- [x] ET MALWARE Potao CnC POST Response
- [x] ET MALWARE Possible Java/Downloader Observed in Pawn Storm CVE-2015-2590 1
- [x] ET MALWARE URI Struct Observed in Pawn Storm CVE-2015-2950
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Ransomware CnC)
- [x] ET MALWARE Sakula/Mivast RAT CnC Beacon 7
- [x] ET MALWARE APT SuperhardCorp DNS Lookup (drometic.suroot.com)
- [x] ET MALWARE APT SuperhardCorp DNS Lookup (ohio.sysbloger.com)
- [x] ET MALWARE APT SuperhardCorp DNS Lookup (np3.Jkub.com)
- [x] ET MALWARE APT SuperhardCorp DNS Lookup (books.mrface.com)
- [x] ET MALWARE APT Lurker POST CnC Beacon
- [ ] ET MALWARE Possible Dyre SSL Cert (non-ASCII) Jul 21 2015
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex CnC)
- [ ] ET MALWARE Possible IE MSMXL Detection of Local DLL (Likely Malicious)
- [x] ET MALWARE Possible CVE-2015-2424 RTF Dropping Sofacy
- [x] ET MALWARE Possible Dyre SSL Cert M2 (L CN)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (VMZeuS MITM)
- [x] ET MALWARE Win32/Bancos.AMM CnC Beacon
- [x] ET MALWARE KeyBase Keylogger Uploading Screenshots
- [x] ET MALWARE Likely Linux/Xorddos.F DDoS Attack Participation (v8.f1122.org)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (VMZeuS MITM)
- [ ] ET MALWARE Jiripbot CnC 1
- [x] ET MALWARE Java/QRat Checkin
- [ ] ET MALWARE Java/QRat Receiving No Commands
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE Likely Dridex SSL Cert
- [x] ET MALWARE KINS/ZeusVM Variant CnC Beacon
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Ransomware CnC)
- [ ] ET MALWARE Zberp/ZeusVM receiving config via image file (steganography) 3
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex CnC)
- [x] ET MALWARE W2KM_BARTALEX Downloading Payload M2 (set)
- [ ] ET MALWARE Poshcoder .onion Proxy Domain (hlvumvvclxy2nw7j)
- [x] ET MALWARE EncryptorRaas .onion Proxy Domain
- [x] ET MALWARE EncryptorRaas .onion Proxy Domain
- [ ] ET MALWARE Critroni .onion Proxy Domain
- [x] ET MALWARE Potao CnC
- [x] ET MALWARE Dyre CnC Checkin
- [x] ET MALWARE Possible Java/Downloader Observed in Pawn Storm CVE-2015-2590 2
- [ ] ET MALWARE EncryptorRaas .onion Proxy Domain (613cb6owitcouepv)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Ransomware CnC)
- [x] ET MALWARE Sakula/Mivast RAT CnC Beacon 6
- [ ] ET MALWARE Sakula/Mivast RAT CnC Beacon 8
- [x] ET MALWARE APT SuperhardCorp DNS Lookup (docume.sysbloger.com)
- [x] ET MALWARE APT SuperhardCorp DNS Lookup (specs.dnsrd.com)
- [x] ET MALWARE APT SuperhardCorp DNS Lookup (ns8.ddns1.com)
- [x] ET MALWARE APT SuperhardCorp DNS Lookup (kieti.ipsecsl.net)
- [x] ET MALWARE APT Lurker GET CnC Beacon
- [x] ET MALWARE APT CozyCar SSL Cert 1
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)

- [x] ET MALWARE W32/Alina.POS-Trojan Checkin
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Ransomware CnC)
- [x] ET MALWARE Win32.VBKrypt.vquj Checkin
- [x] ET MALWARE Win32.Androm.gnlb Checkin
- [x] ET MALWARE DarkHotel Initial Beacon
- [x] ET MALWARE Possible DarkHotel Landing M3
- [x] ET MALWARE PSEmpire Checkin via POST
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (BlackEnergy CnC)
- [x] ET MALWARE Hacking Team Elite Windows Implant Exfiltration
- [x] ET MALWARE Hacking Team Android Implant Exfiltration
- [ ] ET MALWARE MS Terminal Server Single Character Login possible Morto inbound
- [x] ET MALWARE Sharik/Smoke CnC Beacon 3
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Redyms CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [x] ET MALWARE Ponmocup Post Infection DNS Lookup messagewild
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [x] ET MALWARE Likely Linux/Tsunami DDoS Attack Participation (s-p-o-o-f-e-d.h-o-s-t.name)
- [x] ET MALWARE EXE Download Request To Wordpress Folder Likely Malicious
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi CnC)
- [ ] ET MALWARE Careto Mask DNS Lookup (msupdate.ath.cx)
- [ ] ET MALWARE Careto Mask DNS Lookup (isaserver.minrex.gov.cu)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [x] ET MALWARE APT Cheshire Cat CnC Beacon
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
- [x] ET MALWARE AlphaCrypt CnC Beacon 3
- [x] ET MALWARE Cryptowall docs campaign Aug 2015 encrypted binary (1)
- [x] ET MALWARE PawnStorm Java Class Stage 2 M1 Aug 28 2015
- [x] ET MALWARE PawnStorm Sednit DL Aug 28 2015
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
- [ ] ET MALWARE Possible Dyre SSL Cert Aug 31 2015
- [x] ET MALWARE Corebot Checkin
- [x] ET MALWARE Corebot Module Download
- [x] ET MALWARE Win32/Reconyc.equo Checkin
- [x] ET MALWARE Win32.Spy/TVRat Checkin
- [ ] ET MALWARE Possible Upatre/Dyre/Kegotip SSL Cert Sept 8 2015
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [x] ET MALWARE Corebot Module Download 2
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
- [ ] ET MALWARE Potential W32/Dridex Alphanumeric Download Pattern
- [x] ET MALWARE Possible DarkHotel Landing M1
- [x] ET MALWARE Possible DarkHotel Landing M2
- [ ] ET MALWARE Dridex Downloader SSL Certificate
- [ ] ET MALWARE Possible Dridex SSL Cert Aug 12 2015
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Ransomware CnC)
- [x] ET MALWARE W2KM_BARTALEX August 11 2015
- [x] ET MALWARE Hacking Team Scout Windows Implant Exfiltration
- [x] ET MALWARE Hacking Team Implant Exfiltration
- [x] ET MALWARE Sharik/Smoke CnC Beacon 2
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi)
- [x] ET MALWARE LokiBot User-Agent (Charon/Inferno)
- [x] ET MALWARE BandarChor Ransomware Checkin
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE MWI Maldoc Stats Callout Aug 18 2015
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (KINS CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Ursnif CnC)
- [x] ET MALWARE TeslaCrypt/AlphaCrypt Variant .onion Proxy Domain (kb63vhjuk3wh4ex7)
- [ ] ET MALWARE Careto Mask DNS Lookup (karpeskmon.dyndns.org)
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 102
- [ ] ET MALWARE Bedep HTTP POST CnC Beacon 2
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [x] ET MALWARE Alphacrypt/TeslaCrypt Ransomware CnC Beacon Response
- [x] ET MALWARE PawnStorm Java Class Stage 1 M1 Aug 28 2015
- [x] ET MALWARE PawnStorm Java Class Stage 2 M2 Aug 28 2015
- [x] ET MALWARE Joanap CnC Checkin
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Tinba MITM)
- [ ] ET MALWARE Possible Dyre SSL Cert Aug 31 2015
- [x] ET MALWARE Corebot Requesting Module
- [ ] ET MALWARE Possible Dyre SSL Cert Sept 2 2015
- [ ] ET MALWARE PredatorPain Keylogger FTP Activity
- [x] ET MALWARE Win32/Boaxxe.BR CnC Beacon
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 103
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)

- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [ ] ET MALWARE Possible Upatre/Dyre/Kegotip SSL Cert Sept 14 2015
- [x] ET MALWARE AlphaCrypt Connectivity Check 1
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE SYNful Knock Cisco IOS Router Implant CnC Beacon (INBOUND)
- [ ] ET MALWARE Iron Tiger DNSTunnel Retrieving CnC
- [x] ET MALWARE PlugX UDP CnC Beacon
- [x] ET MALWARE Iron Tiger Likely PlugX DNS Lookup (chrome.servehttp.com)
- [x] ET MALWARE Iron Tiger HTTPBrowser DNS Lookup (trendmicro-update.org)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Rovnix CnC)
- [x] ET MALWARE XCodeGhost DNS Lookup
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE Ursnif Variant CnC Beacon 2
- [x] ET MALWARE Ursnif Variant CnC Beacon 3
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Spy.Shiz CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE XcodeGhost CnC Checkin
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE Ursnif Variant CnC Beacon 4
- [x] ET MALWARE Naikon DNS Lookup (greensky27.vicp.net)
- [x] ET MALWARE r0 CnC Check
- [x] ET MALWARE r0 CnC Architecture POST 2
- [x] ET MALWARE r0 CnC Architecture POST 4
- [x] ET MALWARE r0 CnC POST
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE TeslaCrypt/AlphaCrypt Variant .onion Proxy Domain
- [x] ET MALWARE Ransomware Win32/WinPlock.A CnC Beacon 2
- [x] ET MALWARE Ransomware Win32/WinPlock.A CnC Beacon 3
- [ ] ET MALWARE Ransomware Win32/WinPlock.A CnC Beacon 5
- [ ] ET MALWARE Ransomware Win32/WinPlock.A CnC Beacon 7
- [ ] ET MALWARE Ransomware Win32/WinPlock.A CnC Beacon 9
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE Malicious SSL certificate detected (FindPOS)
- [x] ET MALWARE PE EXE or DLL Windows file download Text
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE Cryptowall docs campaign Sept 2015 encrypted binary (1)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Shifu CnC)
- [x] ET MALWARE Iron Tiger DNSTunnel DNS Lookup (xssok.blogspot.com)
- [ ] ET MALWARE Iron Tiger Backdoor.GCloud CnC Beacon
- [x] ET MALWARE Iron Tiger Gh0ST/PlugX/Various Backdoors DNS Lookup (gameofthrones.ddns.net)
- [x] ET MALWARE Iron Tiger Backdoor.GTalkTrojan DNS Lookup (update.gtalklite.com)
- [x] ET MALWARE Possible Passthru/Kshell Port Redirection Initiation
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE Win32/Spy.Odlanor CnC Checkin
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [x] ET MALWARE XCodeGhost DNS Lookup
- [x] ET MALWARE XCodeGhost DNS Lookup
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE Ursnif Variant CnC Beacon
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Spy.Shiz CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi CnC)
- [x] ET MALWARE Ursnif Variant CnC Data Exfil
- [x] ET MALWARE XcodeGhost CnC M2
- [x] ET MALWARE r0 CnC Architecture POST 1
- [x] ET MALWARE r0 CnC Architecture POST 3
- [x] ET MALWARE r0 CnC Report POST
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Shifu CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [ ] ET MALWARE TeslaCrypt/AlphaCrypt Variant .onion Proxy Domain
- [ ] ET MALWARE Ransomware Win32/WinPlock.A CnC Beacon 1
- [x] ET MALWARE Ransomware Win32/WinPlock.A Successfully Installed CnC Beacon
- [ ] ET MALWARE Ransomware Win32/WinPlock.A CnC Beacon 4
- [ ] ET MALWARE Ransomware Win32/WinPlock.A CnC Beacon 6
- [ ] ET MALWARE Ransomware Win32/WinPlock.A CnC Beacon 8
- [ ] ET MALWARE Ransomware Win32/WinPlock.A CnC Beacon 10

- [ ] ET MALWARE Ransomware Win32/WinPlock.A CnC Beacon 11
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE Winlock/Torrentlocker SSL Cert
- [x] ET MALWARE Hawkeye Keylogger SMTP Beacon
- [x] ET MALWARE Linux/dtool IRC Command (TCPFLOOD)
- [x] ET MALWARE Linux/dtool IRC Command (AUTH)
- [x] ET MALWARE Linux/dtool IRC Command (EXEC)
- [x] ET MALWARE Linux/dtool IRC Command (STOP)
- [x] ET MALWARE Linux/dtool IRC Command Complete 1
- [x] ET MALWARE Linux/dtool IRC Command Complete 3
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [ ] ET MALWARE Winlock/Torrentlocker SSL Cert
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE ELF/muBoT IRC Activity 2
- [x] ET MALWARE ELF/muBoT IRC Activity 4
- [x] ET MALWARE ELF/muBoT User-Agent (I'm a mu mu mu ?)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [x] ET MALWARE StartPage Userclass HTTP Request
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE MSIL/Banker.M Downloading Binary from SQL
- [ ] ET MALWARE Possible PlugX DNS Lookup (operaa.net)
- [x] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE Win32/Kelihos.F Checkin
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [x] ET MALWARE JS/Nemucod.M.gen requesting PDF payload 2015-10-07
- [x] ET MALWARE JS/Nemucod.M.gen downloading PDF payload
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE PlugX or EvilGrab DNS Lookup (appeur.gnway.cc)
- [x] ET MALWARE NetWire Variant - Client Hello
- [x] ET MALWARE NetWire / Ozone / Darktrack Alien RAT - Client KeepAlive
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Retefe CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE Winlock/Torrentlocker SSL Cert
- [ ] ET MALWARE Winlock/Torrentlocker SSL Cert
- [x] ET MALWARE Linux/dtool IRC Command (HTTPFLOOD)
- [x] ET MALWARE Linux/dtool IRC Command (UDPFLOOD)
- [x] ET MALWARE Linux/dtool IRC Command (RAW)
- [x] ET MALWARE Linux/dtool IRC Command (CHSERVER)
- [x] ET MALWARE Linux/dtool IRC Command (RESTART)
- [x] ET MALWARE Linux/dtool IRC Command Complete 2
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [x] ET MALWARE Java/QRat Retrieving PE
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE ELF/muBoT IRC Activity 1
- [x] ET MALWARE ELF/muBoT IRC Activity 3
- [x] ET MALWARE ELF/muBoT IRC Activity 5
- [x] ET MALWARE DustySky CnC Beacon
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [x] ET MALWARE Win32/Neshta.A Posting Data
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE MSIL/Banker.M Requesting Binary from SQL
- [x] ET MALWARE Possible PlugX DNS Lookup (googlemanage.com)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE Possible Dridex SSL Cert Oct 12 2015
- [ ] ET MALWARE Possible Upatre/Dyre/Kegotip SSL Cert Oct 12 2015
- [x] ET MALWARE JS/Nemucod.M.gen requesting EXE payload 2015-10-07
- [x] ET MALWARE JS/Nemucod.M.gen downloading EXE payload
- [x] ET MALWARE Nemucod Downloading Payload 2
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [x] ET MALWARE PlugX or EvilGrab DNS Lookup (websecexp.com)
- [x] ET MALWARE PlugX DNS Lookup (mailsecurityservice.com)
- [x] ET MALWARE NetWire / Ozone / Darktrack Alien RAT - Server Hello
- [x] ET MALWARE NetWire Variant - Server Directory Listing Request
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Shifu CnC)
- [x] ET MALWARE Possible click2play bypass Oct 19 2015 as observed in PawnStorm
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)

- [x] ET MALWARE Win32/Necurs Common POST Header Structure
- [ ] ET MALWARE Duuzer Checkin
- [x] ET MALWARE LuminosityLink - Data Channel Server Response
- [ ] ET MALWARE LummoX Keylogger Report SMTP
- [x] ET MALWARE MWI Maldoc Load Payload
- [x] ET MALWARE Vawtrak/NeverQuest Posting Data 2
- [ ] ET MALWARE Malicious SSL certificate detected (Spy.Shiz CnC)
- [x] ET MALWARE Sharik/Smoke Loader Java Connectivity Check
- [x] ET MALWARE Silent Miner Changelog Checkin
- [x] ET MALWARE JS/Nemucod.M.gen requesting PDF payload 2015-11-02
- [x] ET MALWARE Cryptowall .onion Proxy Domain
- [x] ET MALWARE Likely Evil EXE download from dotted Quad by MSXMLHTTP M2
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Shifu)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL Certificate Detected (Shifu)
- [x] ET MALWARE njrat ver 0.7d Malware CnC Callback (Remote Desktop)
- [x] ET MALWARE njrat ver 0.7d Malware CnC Callback Response (File Manager)
- [ ] ET MALWARE Win32/HideWindows.C IRC Checkin
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (ProxyChanger)
- [x] ET MALWARE KilerRAT CnC - Remote Shell
- [x] ET MALWARE TinyLoader.B2 Checkin x64
- [x] ET MALWARE Bookworm CnC Beacon 2
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Shifu)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Qadars CnC)
- [x] ET MALWARE Trojan-Ransom.Win32.Blocker.dham Checkin
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (FindPOS CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gootkit)
- [x] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Downloader CnC)
- [x] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Downloader CnC)
- [x] ET MALWARE r0 CnC Architecture GET 1
- [x] ET MALWARE r0 CnC Architecture GET 3
- [x] ET MALWARE r0 CnC Report GET
- [x] ET MALWARE Nymaim.BA CnC M1
- [x] ET MALWARE Sofacy DNS Lookup
- [x] ET MALWARE Sharik/Smoke Loader Microsoft Connectivity Check
- [x] ET MALWARE MegalodonHTTP/LuciferHTTP Client Action
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Retefe CnC)
- [ ] ET MALWARE Rincux CnC (set)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Downloader CnC)
- [x] ET MALWARE Matryoshka CnC Beacon 1
- [x] ET MALWARE Possible CopyKittens DNS Lookup (alhadath.mobi)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (cacheupdate14.com)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (fbstatic-a.xyz)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (gmailtagmanager.com)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (haaretz-news.com)
- [x] ET MALWARE Backdoor.Win32.DarkComet Screenshot Upload Successful
- [x] ET MALWARE LuminosityLink - Data Channel Client Request
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)
- [x] ET MALWARE Agent Tesla Keylogger Report SMTP
- [x] ET MALWARE MWI Maldoc Stats Callout Oct 28
- [ ] ET MALWARE Likely Malvertising Malicious PE Download
- [x] ET MALWARE Sharik/Smoke Loader Adobe Connectivity Check 2
- [x] ET MALWARE Sharik/Smoke Loader Adobe Connectivity Check 3
- [x] ET MALWARE JS/Nemucod.M.gen requesting EXE payload 2015-11-02
- [x] ET MALWARE Wrapper/Gholee/Wedex Checkin
- [x] ET MALWARE Likely Evil EXE download from dotted Quad by MSXMLHTTP M1
- [x] ET MALWARE Likely Evil EXE download from MSXMLHTTP non-exe extension M2
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (ProxyChanger)
- [x] ET MALWARE njrat ver 0.7d Malware CnC Callback Response (Get Passwords)
- [x] ET MALWARE njrat ver 0.7d Malware CnC Callback Response (Remote Desktop)
- [x] ET MALWARE njrat ver 0.7d Malware CnC Callback (Get Passwords)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Shifu)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (ProxyChanger)
- [ ] ET MALWARE KilerRAT CnC - Info Checkin
- [x] ET MALWARE Bookworm CnC Beacon
- [x] ET MALWARE Possible Chimera Ransomware - Bitmessage Activity
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Shifu)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Shifu CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Qadars CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (FindPOS CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (FindPOS CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (FindPOS CnC)
- [x] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Downloader CnC)
- [x] ET MALWARE r0 CnC Check
- [x] ET MALWARE r0 CnC Architecture GET 2
- [x] ET MALWARE r0 CnC Architecture GET 4
- [x] ET MALWARE r0 CnC GET
- [x] ET MALWARE Nymaim.BA CnC M2
- [x] ET MALWARE Sofacy DNS Lookup
- [x] ET MALWARE MegalodonHTTP CnC Checkin
- [x] ET MALWARE MegalodonHTTP CoinMiner Activity
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Retefe CnC)
- [ ] ET MALWARE Rincux CnC
- [ ] ET MALWARE Critroni .onion Proxy Domain (tmclybfqzgkaeilm)
- [ ] ET MALWARE Matryoshka CnC Beacon 2
- [x] ET MALWARE Possible CopyKittens DNS Lookup (big-windowss.com)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (fbstatic-a.space)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (fbstatic-akamaihd.com)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (haaretz.link)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (heartax.info)

- [x] ET MALWARE Possible CopyKittens DNS Lookup (img.gmailtagmanager.com)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (kernel4windows.in)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (main.windowskernel14.com)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (micro-windows.in)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (mswordupdate15.com)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (mswordupdate16.com)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (mswordupdate17.com)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (mywindows24.in)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (patch7-windows.com)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (patch8-windows.com)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (patchthiswindows.com)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (u.mywindows24.in)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (walla.link)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (wethearservice.com)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (wheatherserviceapi.info)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (windowkernel.com)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (windows-10patch.in)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (windows24-kernel.in)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (windows-drive20.com)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (windows-india.in)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (windowskernel.in)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (windows-kernel.in)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (windowskernel14.com)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (windowslayer.in)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (windows-my50.com)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (windowssup.in)
- [x] ET MALWARE Possible CopyKittens DNS Lookup (windowsupup.com)
- [x] ET MALWARE Win32/Swrort.A Checkin 3
- [ ] ET MALWARE Win32/Scieron-A Checkin via HTTP POST 2
- [x] ET MALWARE ELF/muBoT IRC Activity 6 (SOCKS)
- [x] ET MALWARE ELF/muBoT IRC Activity 7 (bindshell)
- [ ] ET MALWARE Win32/Teslacrypt .onion Proxy Domain (tw7kaqthui5ojcez)
- [x] ET MALWARE VBKlip/ClipBanker.P Status Update
- [x] ET MALWARE Send-Safe Bulk Mailer SSL Cert - Observed in Spam Campaigns
- [x] ET MALWARE Ponmocup HTTP Request (generic) M1
- [x] ET MALWARE Ponmocup HTTP Request (generic) M2
- [x] ET MALWARE Ponmocup HTTP Request (generic) M3
- [x] ET MALWARE Ponmocup HTTP Request (generic) M4
- [x] ET MALWARE Ponmocup HTTP Request (generic) M5
- [x] ET MALWARE Ponmocup HTTP Request (generic) M6
- [x] ET MALWARE Ponmocup HTTP Request (generic) M7
- [x] ET MALWARE Ponmocup HTTP Request (generic) M8
- [x] ET MALWARE Ponmocup HTTP Request (generic) M9
- [ ] ET MALWARE Ponmocup plugin #2600 (SIP scanner)
- [x] ET MALWARE JS/Nemucod requesting EXE payload 2015-12-01
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Shifu CnC)
- [x] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Bancos/DarkTequila CnC)
- [x] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Bancos/DarkTequila CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Shifu CnC)
- [x] ET MALWARE ELF/lizkebab CnC Activity (Flooding 1)
- [x] ET MALWARE ELF/lizkebab CnC Activity (Server Banner)
- [x] ET MALWARE ELF/STDbot CnC Activity (STD attack)
- [x] ET MALWARE ELF/STDbot CnC Activity (UNK attack)
- [x] ET MALWARE Linux/KDefend Checkin
- [x] ET MALWARE Linux/MayhemBruter Checkin
- [x] ET MALWARE Linux/MayhemBruter Inbound Ping From CnC
- [x] ET MALWARE Vawtrak HTTP CnC Beacon
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (FindPOS CnC)
- [ ] ET MALWARE Malicious SSL certificate detected (FindPOS)
- [x] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gootkit MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gootkit MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gootkit CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (FindPOS CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Zeus CnC)
- [x] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gootkit CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gootkit CnC)
- [ ] ET MALWARE EncryptorRaas .onion Domain (75nzutdjjtnpgscz)
- [ ] ET MALWARE TeslaCrypt/AlphaCrypt Variant .onion Domain
- [ ] ET MALWARE TeslaCrypt/AlphaCrypt Variant .onion Domain
- [x] ET MALWARE NetBackdoor Checkin
- [x] ET MALWARE NetBackdoor User-Agent (.net backdoor)
- [x] ET MALWARE PPI User-Agent (InstallCapital)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gootkit CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gootkit CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gootkit CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gootkit CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE Possible Gootkit CnC SSL Cert M1
- [ ] ET MALWARE Possible Gootkit CnC SSL Cert M2
- [ ] ET MALWARE Possible Gootkit CnC SSL Cert M3
- [ ] ET MALWARE Possible Gootkit CnC SSL Cert M4
- [ ] ET MALWARE Possible Gootkit CnC SSL Cert M5
- [ ] ET MALWARE Possible Gootkit CnC SSL Cert M6
- [ ] ET MALWARE Possible Gootkit CnC SSL Cert M7

- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE Possible Evil Macro Downloading Trojan Dec 16 2015 Post to EXE
- [x] ET MALWARE Sakula DNS Lookup (inocnation.com)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE Win32/Nivdort Posting Data 1
- [ ] ET MALWARE Win32/ProPoS CnC Beacon
- [x] ET MALWARE AlphaCrypt CnC Beacon 5
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE Ironhalo CnC Beacon
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE ASCII Executable Inside of MSCOFF File DL Over HTTP
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (FindPOS CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE BBSRAT GET request CnC
- [ ] ET MALWARE TeslaCrypt/AlphaCrypt Variant .onion Payment Domain (czc57cr2pn3zfn4b)
- [ ] ET MALWARE TeslaCrypt/AlphaCrypt Variant .onion Payment Domain (vr6g2curb2kcidou)
- [x] ET MALWARE Zbot download config
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE BlackEnergy SSL Cert
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE NanoLocker Check-in (ICMP) M1
- [x] ET MALWARE Malicious VBS Downloader fake image zip
- [x] ET MALWARE ELF.MrBlack DOS.TF Variant
- [ ] ET MALWARE Dridex Download 6th Jan 2016 Flowbit
- [x] ET MALWARE DustySky Payload Link Request
- [ ] ET MALWARE Win32/Bulta DNS Lookup (kugo.f3322.net)
- [x] ET MALWARE EvilGrab or APT.9002 DNS Lookup (secvies.com)
- [x] ET MALWARE Linux/Torte Downloading Binary
- [x] ET MALWARE TrochilusRAT CnC Beacon 1
- [x] ET MALWARE Win32/Agent.XST Checkin
- [x] ET MALWARE ELF.STD.ddos Checkin
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Qadars CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Qadars CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Qadars CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE Cryptolocker Payment Page (4nauizsaaopuj3qj)
- [x] ET MALWARE Cryptolocker Payment Page (krfdnhfnsai3d)
- [x] ET MALWARE Win32/7ev3n Ransomware Initial Checkin
- [x] ET MALWARE Possible Derusbi/Winnti Receiving Configuration
- [ ] ET MALWARE Sakula DNS Lookup (mail.cbppnews.com)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Malware CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)
- [x] ET MALWARE Win32/Nivdort Posting Data 2
- [x] ET MALWARE FAKBEN Ransomware
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE Possible Gootkit CnC SSL Cert M8
- [ ] ET MALWARE Kelihos CnC Server Activity
- [x] ET MALWARE AlphaCrypt CnC Beacon 6
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)
- [x] ET MALWARE Powersploit Framework Script Downloaded
- [x] ET MALWARE BBSRAT POST request CnC
- [ ] ET MALWARE TeslaCrypt/AlphaCrypt Variant .onion Payment Domain (o7zeip6us33igmgw)
- [x] ET MALWARE Zbot download config - SET
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE Malicious SSL certificate detected (Possible Sinkhole)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE NanoLocker Check-in (ICMP) M2
- [x] ET MALWARE Cryptojoker Checkin
- [x] ET MALWARE ELF.MrBlack DOS.TF Malformed Lookup (/lib32/libc.so.6)
- [x] ET MALWARE Win32.Nitol.K Variant CnC
- [ ] ET MALWARE W32/Dridex Binary Download 6th Jan 2016
- [x] ET MALWARE Win32/Bulta CnC Beacon
- [ ] ET MALWARE Win32/Bulta DNS Lookup (yk.ftwxw.com)
- [x] ET MALWARE TrochilusRAT DNS Lookup (security-centers.com)
- [ ] ET MALWARE Linux/Torte Checkin
- [x] ET MALWARE TrochilusRAT CnC Beacon 2
- [ ] ET MALWARE Win32/Agent.XST Keepalive
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Qadars CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Qadars CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)
- [x] ET MALWARE Cryptolocker Payment Page (aynfksddnnfwkd)
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 104
- [x] ET MALWARE Win32/7ev3n Ransomware Process Checkin

- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Qadars CnC)
- [x] ET MALWARE LeChiffre Ransomware CnC
- [x] ET MALWARE Win32/Kaicone.A Checkin via HTTP POST
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)
- [x] ET MALWARE Scarlet Mimic DNS Lookup 1
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 2
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 3
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 4
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 5
- [x] ET MALWARE Scarlet Mimic DNS Lookup 6
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 7
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 8
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 9
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 10
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 11
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 12
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 13
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 14
- [x] ET MALWARE Scarlet Mimic DNS Lookup 15
- [x] ET MALWARE Scarlet Mimic DNS Lookup 16
- [x] ET MALWARE Scarlet Mimic DNS Lookup 17
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 18
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 19
- [x] ET MALWARE Scarlet Mimic DNS Lookup 20
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 21
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 22
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 23
- [x] ET MALWARE Scarlet Mimic DNS Lookup 24
- [x] ET MALWARE Scarlet Mimic DNS Lookup 25
- [x] ET MALWARE Scarlet Mimic DNS Lookup 26
- [x] ET MALWARE Scarlet Mimic DNS Lookup 27
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 28
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 29
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 30
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 31
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 32
- [x] ET MALWARE Scarlet Mimic DNS Lookup 33
- [x] ET MALWARE Scarlet Mimic DNS Lookup 34
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 35
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 36
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 37
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 38
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 39
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 40
- [x] ET MALWARE Scarlet Mimic DNS Lookup 41
- [x] ET MALWARE Scarlet Mimic DNS Lookup 42
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 43
- [x] ET MALWARE Scarlet Mimic DNS Lookup 45
- [x] ET MALWARE Scarlet Mimic DNS Lookup 46
- [x] ET MALWARE Scarlet Mimic DNS Lookup 47
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 48
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 49
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 50
- [x] ET MALWARE Scarlet Mimic DNS Lookup 44
- [x] ET MALWARE Win32/Neutrino Checkin 2
- [x] ET MALWARE Win32/Neutrino Checkin 3
- [x] ET MALWARE Bedep Connectivity Check M2
- [x] ET MALWARE CenterPOS User Agent Observed
- [x] ET MALWARE CenterPOS CnC
- [x] ET MALWARE CenterPOS Delete Plugins
- [x] ET MALWARE CenterPOS Load Plugins
- [x] ET MALWARE CenterPOS CnC 2
- [x] ET MALWARE CustomRAT DNS lookup
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Qadars CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Ursnif Injects)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gootkit CnC)
- [ ] ET MALWARE Mokes CnC Keep-Alive
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Zeus CnC)
- [x] ET MALWARE JS/Nemucod requesting EXE payload 2016-02-01
- [x] ET MALWARE JS/Nemucod requesting EXE payload 2016-01-28
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)
- [x] ET MALWARE TeslaCrypt/AlphaCrypt Variant .onion Payment Domain(yez2o5lwqkmlv5lc)
- [x] ET MALWARE Win32/Fluxer CnC Checkin
- [x] ET MALWARE Win32/LockScreen CnC HTTP Pattern
- [x] ET MALWARE Win32/HydraCrypt CnC Beacon 1
- [x] ET MALWARE Xbagger Macro Encrypted DL
- [x] ET MALWARE TeslaCrypt/AlphaCrypt Variant .onion Payment Domain(fwgrhsao3aoml7ej)
- [x] ET MALWARE Various Malicious AlphaNum DL Feb 10 2016
- [x] ET MALWARE Alphacrypt/TeslaCrypt Ransomware CnC Beacon
- [x] ET MALWARE W32/Gaudox Checkin
- [x] ET MALWARE TeslaCrypt/AlphaCrypt Payment DNS Lookup
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Qadars CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Qadars CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Qadars CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Qadars CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gootkit CnC)
- [x] ET MALWARE Bedep Connectivity Check M3
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)
- [x] ET MALWARE W32/GCman.Backdoor CnC Beacon
- [x] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Qadars CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)
- [x] ET MALWARE Ransomware Locky CnC Beacon
- [x] ET MALWARE Possible OceanLotus Time Check to Microsoft.com
- [x] ET MALWARE Possible OceanLotus CnC Heartbeat
- [x] ET MALWARE Possible OceanLotus C2 Checkin
- [ ] ET MALWARE Ransomware Locky .onion Payment Domain

- [x] ET MALWARE Dridex DL Pattern Feb 18 2016
- [x] ET MALWARE FrameworkPOS CnC Server Reporting IP Address To Agent
- [x] ET MALWARE Linux/Tsunami DNS Request (updates.absentvodka.com)
- [x] ET MALWARE Linux/Tsunami DNS Request (eggstrawdinarry.mylittlerepo.com)
- [x] ET MALWARE FrameworkPOS Covert DNS CnC Initial Check In
- [ ] ET MALWARE TeslaCrypt/AlphaCrypt Variant .onion Payment Domain(xlowfznrg4wf7dli)
- [x] ET MALWARE Possible Malicious Macro EXE DL AlphaNumL
- [ ] ET MALWARE PadCrypt .onion Payment Domain
- [ ] ET MALWARE Andromeda Download (set)
- [x] ET MALWARE jFect HTTP CnC Checkin
- [x] ET MALWARE Ransomware Locky .onion Payment Domain
- [x] ET MALWARE Dridex Base64 Executable
- [x] ET MALWARE OSX/KeRanger Ransomware CnC DNS Request 2
- [x] ET MALWARE OSX/KeRanger Ransomware CnC DNS Request 4
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 45
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 47
- [x] ET MALWARE TeslaCrypt/AlphaCrypt Variant .onion Payment Domain(k7tlx3ghr3m4n2tu)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)
- [x] ET MALWARE Suckfly/Nidiran Backdoor DNS Lookup
- [ ] ET MALWARE Maktub Locker Payment Domain
- [x] ET MALWARE Possible Locky Ransomware Writing Encrypted File over - SMB and SMB-DS v1 ASCII
- [x] ET MALWARE PE EXE or DLL Windows file download Text M2
- [x] ET MALWARE W32/Dridex Binary Download Mar 23 2016
- [x] ET MALWARE Genome User-Agent (Http Down)
- [ ] ET MALWARE IrcBot Downloading Files via FTP
- [x] ET MALWARE Possible Malicious Macro DL EXE Feb 2016 (WinHTTPRequest)
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected (TeslaCrypt Payment)
- [ ] ET MALWARE ABUSE.CH Ransomware Domain Detected (Locky Payment)
- [x] ET MALWARE Ransomware Locky CnC Beacon
- [ ] ET MALWARE Ransomware/Coverton Checkin
- [ ] ET MALWARE Ransomware/Coverton CnC 2
- [x] ET MALWARE Win32.TreasureHunter Checkin
- [x] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Zeus CnC)
- [x] ET MALWARE Likely Evil Macro EXE DL mar 28 2016
- [x] ET MALWARE Win32/Backdoor.Dripion HTTP CnC Checkin
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker C2)
- [ ] ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker C2)
- [x] ET MALWARE LuminosityLink - Data Channel Client Request 2
- [x] ET MALWARE LuminosityLink - CnC
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected
- [ ] ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker C2)
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker C2)
- [ ] ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker C2)
- [ ] ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker C2)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (FindPOS CnC)

- [x] ET MALWARE Possible Malicious Macro DL EXE Feb 2016
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Malware CnC)
- [x] ET MALWARE Linux/Tsunami DNS Request (updates.mintylinux.com)
- [x] ET MALWARE Linux/Tsunami DNS Request (linuxmint.kernel-org.org)
- [x] ET MALWARE Ransomware Locky .onion Payment Domain
- [x] ET MALWARE Operation Blockbuster User-Agent (Mozillar)
- [x] ET MALWARE Likely PadCrypt Locker PKG DL
- [ ] ET MALWARE Malicious SSL certificate detected (Geodo MITM)
- [ ] ET MALWARE Andromeda Download
- [x] ET MALWARE Ransomware Locky .onion Payment Domain
- [x] ET MALWARE Possible Godzilla Loader Base64 Filename
- [x] ET MALWARE OSX/KeRanger Ransomware CnC DNS Request 1
- [x] ET MALWARE OSX/KeRanger Ransomware CnC DNS Request 3
- [x] ET MALWARE Panda Banker CnC
- [ ] ET MALWARE Scarlet Mimic DNS Lookup 46
- [ ] ET MALWARE Malicious SSL certificate detected (Ursnif Injects)
- [x] ET MALWARE Likely Evil Macro EXE DL mar 15 2016
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Kasidet CnC)
- [x] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)
- [x] ET MALWARE Possible Locky Ransomware Writing Encrypted File over - SMB and SMB-DS v1 Unicode
- [x] ET MALWARE Possible Locky Ransomware Writing Encrypted File over - SMB and SMB-DS v2
- [x] ET MALWARE Cryptolocker Payment Domain (3qbyaoohkcqkzrz6)
- [x] ET MALWARE Likely Evil EXE download from WinHttpRequest non-exe extension
- [x] ET MALWARE IrcBot Fantasy Name Gen
- [x] ET MALWARE IrcBot Downloading .old
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected (Locky Payment)
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker Payment)
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker Payment)
- [ ] ET MALWARE Ransomware/Coverton Onion Domain Lookup
- [ ] ET MALWARE Ransomware/Coverton CnC 1
- [x] ET MALWARE Ransomware Locky Possible Payment Page
- [x] ET MALWARE Win32/CryptFile2 Ransomware Checkin
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)
- [x] ET MALWARE Win32/Backdoor.Dripion External IP Check
- [x] ET MALWARE JS/Nemucod requesting EXE payload 2016-03-31
- [ ] ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker C2)
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker C2)
- [x] ET MALWARE LuminosityLink - CnC Password Exfil
- [ ] ET MALWARE TeslaCrypt/AlphaCrypt Variant .onion Payment Domain(xzjvzkgjxebzreap)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker C2)
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker C2)
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker Payment)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gootkit CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (FindPOS CnC)

- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Qadars CnC)
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker C2)
- [ ] ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker C2)
- [ ] ET MALWARE Win32/Agent.XST/UP007 Keepalive 2
- [ ] ET MALWARE TrojanDownloader.Banload.XDL Checkin
- [x] ET MALWARE APT.Fwits CnC Beacon M1
- [x] ET MALWARE Blackmoon/Banbra Configuration Request
- [ ] ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker C2)
- [ ] ET MALWARE Retefe Banker .onion Domain
- [ ] ET MALWARE Retefe Banker .onion Domain
- [ ] ET MALWARE Retefe Banker .onion Domain
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 105
- [x] ET MALWARE ABUSE.CH Locky Domain
- [x] ET MALWARE Backdoor.Darpapox/Jaku CNAME CnC Beacon (WinVer 5.1)
- [x] ET MALWARE Backdoor.Darpapox/Jaku CNAME CnC Beacon (WinVer 6.0)
- [x] ET MALWARE Backdoor.Darpapox/Jaku CNAME CnC Beacon (WinVer 6.2)
- [x] ET MALWARE Backdoor.Darpapox/Jaku CNAME CnC Beacon (WinVer 10.0)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)
- [ ] ET MALWARE SHUJIN .onion Payment Page
- [x] ET MALWARE ABUSE.CH Cryptolocker Payment Page (de2nuvwegoo32oqv)
- [x] ET MALWARE Win32.Sality-GR Checkin 2
- [x] ET MALWARE MSIL/Spy.Banker.DH Checkin
- [x] ET MALWARE Generic gate .php GET with minimal headers
- [ ] ET MALWARE Hidden-Tear Ransomware Variant (.bloccato) DNS Request to CnC Domain
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (ZeuS CnC)
- [x] ET MALWARE PowerShell/Agent.A DNS Lookup (go0gle.com)
- [x] ET MALWARE PowerShell/Agent.A DNS File Transfer CnC Beacon
- [x] ET MALWARE Possible CryptXXX Ransomware Renaming Encrypted File SMB v1 ASCII
- [x] ET MALWARE Possible ReactorBot .bin Download
- [ ] ET MALWARE ABUSE.CH Ransomware Domain Detected (Locky C2)
- [x] ET MALWARE Criptobit/Mobef Ransomware Checkin
- [ ] ET MALWARE Luminosity RAT Possible Module Download M2
- [x] ET MALWARE FastPOS Version Checkin
- [x] ET MALWARE FastPOS Software Update Request
- [x] ET MALWARE FastPOS Successful Software Update Request
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected (Locky C2)
- [x] ET MALWARE FastPOS RAM Scraper Sending Details
- [x] ET MALWARE Windows Executable Sent When Remote Host Claims to Send a RAR Archive
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gootkit CnC)
- [x] ET MALWARE Qarallax RAT Downloading Modules
- [x] ET MALWARE Qarallax RAT Keepalive C2
- [x] ET MALWARE W32/Virus-Encoder Ransomware Checkin
- [ ] ET MALWARE Unknown PowerShell Loader DNS Lookup (spl.noip.me)
- [ ] ET MALWARE Win32/Agent.XST/UP007 Checkin 2
- [ ] ET MALWARE PoisonIvy SPIVY DNS Lookup (leeh0m.org)
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker C2)
- [x] ET MALWARE APT.Fwits CnC Beacon M2
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected (Locky C2)
- [ ] ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker C2)
- [ ] ET MALWARE Retefe Banker .onion Domain
- [ ] ET MALWARE Retefe Banker .onion Domain
- [x] ET MALWARE Ransomware Locky CnC Beacon 2
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected
- [x] ET MALWARE Backdoor.Darpapox/Jaku CNAME CnC Beacon (WinVer 5.0)
- [x] ET MALWARE Backdoor.Darpapox/Jaku CNAME CnC Beacon (WinVer 5.2)
- [x] ET MALWARE Backdoor.Darpapox/Jaku CNAME CnC Beacon (WinVer 6.1)
- [x] ET MALWARE Backdoor.Darpapox/Jaku CNAME CnC Beacon (WinVer 6.3)
- [x] ET MALWARE Backdoor.Darpapox/Jaku Initial C2 Checkin
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Shifu CnC)
- [ ] ET MALWARE Malicious SSL certificate detected (Ursnif Injects)
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker C2)
- [ ] ET MALWARE Ransomware Locky .onion Payment Domain (hw5qrh6fxv2tnaqn)
- [ ] ET MALWARE Ransomware Locky .onion Payment Domain (eqrvbczir5ua2emd)
- [x] ET MALWARE Possible Malicious Macro DL EXE May 2016 (Mozilla compatible)
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker C2)
- [x] ET MALWARE Possible Malicious Macro DL BIN May 2016 (No UA)
- [x] ET MALWARE PowerShell/Agent.A DNS Checkin
- [x] ET MALWARE Possible CryptXXX Ransomware Renaming Encrypted File SMB v1 Unicode
- [x] ET MALWARE Possible CryptXXX Ransomware Renaming Encrypted File SMB v2
- [x] ET MALWARE ProjectSauron Remsec/HTTPBrowser/Pisloader Covert DNS CnC Channel TXT Lookup
- [x] ET MALWARE Ransomware Locky CnC Beacon 4 21 May
- [ ] ET MALWARE Luminosity RAT Possible Module Download M1
- [x] ET MALWARE FastPOS Initial Checkin
- [x] ET MALWARE FastPOS Sending Status Logs
- [x] ET MALWARE FastPOS Reporting Error Code
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)
- [x] ET MALWARE FastPOS Sending Keystrokes
- [x] ET MALWARE Win32/DMA Locker CnC Checkin
- [x] ET MALWARE BandarChor/CryptON Ransomware Checkin
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Shifu CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gootkit CnC)
- [x] ET MALWARE Qarallax RAT Keepalive C2 (set)
- [ ] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 106

- [ ] ET MALWARE Malicious SSL Certificate Detected (Bancos C2)
- [ ] ET MALWARE Unknown Botnet Checkin
- [x] ET MALWARE Win32.Crypren/Zcrypt Ransomware Checkin
- [x] ET MALWARE FOX-SRT ShimRat check-in (Data)
- [x] ET MALWARE FOX-SRT ShimRat check-in (Yuok)
- [x] ET MALWARE Towerweb Ransomware Landing Page
- [x] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL Certificate Detected (Sinkhole)
- [x] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Malware C2)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Malware C2)
- [x] ET MALWARE Win32/Satana Ransomware Checkin
- [x] ET MALWARE Possible Malicous Macro DL EXE Jul 01 2016 (userdir dotted quad)
- [ ] ET MALWARE Possible Malicous Macro DL EXE Jul 01 2016 (exe generic custom headers)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Malware C2)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Zeus C2)
- [x] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Malware C2)
- [x] ET MALWARE OSX/Keydnap DNS Query to CnC
- [x] ET MALWARE Malicious SSL certificate detected (OSX/Keydnap CnC)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gootkit C2)
- [x] ET MALWARE Ranscam Ransomware Contact Form
- [x] ET MALWARE W32.Dreambot File Upload (No Data Sent)
- [x] ET MALWARE Cknife Shell Command Struct Inbound (aspx)
- [x] ET MALWARE Possible Maldoc Downloading EXE Jul 26 2016
- [x] ET MALWARE Generic Request to gate.php Dotted-Quad
- [ ] ET MALWARE ABUSE.CH Ransomware Domain Detected
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected
- [ ] ET MALWARE ABUSE.CH Ransomware Domain Detected
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (ZeuS CnC)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gootkit C2)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Downloader.Pony CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)
- [x] ET MALWARE ProjectSauron Remsec DNS Lookup (bikessport.com)
- [x] ET MALWARE ProjectSauron Remsec DNS Lookup (wildhorses.awardspace.info)
- [x] ET MALWARE ProjectSauron Remsec DNS Lookup (sx4-ws42 .yi.org)
- [x] ET MALWARE RAMNIT.A M1
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gootkit C2)
- [ ] ET MALWARE ProjectSauron Remsec CnC Beacon (hardcoded HTTP headers)
- [x] ET MALWARE Linux/Lady CnC Beacon 1
- [x] ET MALWARE Monsoon Tinytyphon CnC Beacon GET
- [x] ET MALWARE DarkHotel DNS Lookup (apply-wsu.ebizx.net)
- [x] ET MALWARE Aveo Checkin
- [x] ET MALWARE Aveo C2 Request
- [x] ET MALWARE Curso Banker Downloading Modules
- [x] ET MALWARE Ransomware Locky .onion Payment Domain (5n7y4yihirccftc5)
- [x] ET MALWARE PNScan.2 Inbound Status Check - set
- [x] ET MALWARE Bolek HTTP Checkin
- [x] ET MALWARE Xbagger Macro Encrypted DL Jun 13 2016
- [x] ET MALWARE JS/RAA Ransomware check-in
- [x] ET MALWARE FOX-SRT ShimRat check-in (php)
- [x] ET MALWARE FOX-SRT ShimRatReporter check-in
- [x] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL Certificate Detected (Sinkhole)
- [x] ET MALWARE Ransomware Locky .onion Payment Domain (mphtadhci5mrdlju)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gootkit C2)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (H1N1 C2 or Zeus Panda C2)
- [x] ET MALWARE Possible Pony DLL Download
- [x] ET MALWARE Possible Malicous Macro DL EXE Jul 01 2016 (dll generic custom headers)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gootkit C2)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Rockloader)
- [x] ET MALWARE BartCrypt Payment DNS Query to .onion proxy Domain (khh5cmzh5q7yp7th)
- [x] ET MALWARE OSX/Keydnap DNS Query to CnC
- [x] ET MALWARE Ransomware Locky CnC Beacon 21 May
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (H1N1 CnC)
- [x] ET MALWARE SFG Client Information POST
- [x] ET MALWARE Win32.Razy.azv Downloading Content
- [x] ET MALWARE Cknife Shell Command Struct Inbound (PHP)
- [x] ET MALWARE Evil Monero Cryptocurrency Miner Request Pools
- [x] ET MALWARE Trojan Generic - POST To gate.php with no accept headers
- [x] ET MALWARE Win32/Pottieq.A Check-in
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gootkit C2)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gootkit CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gootkit CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi CnC)
- [x] ET MALWARE ProjectSauron Remsec DNS Lookup (rapidcomments.com)
- [x] ET MALWARE ProjectSauron Remsec DNS Lookup (flowershop22.110mb.com)
- [x] ET MALWARE ProjectSauron Remsec DNS Lookup (asrgd-uz .weedns.com)
- [x] ET MALWARE ProjectSauron Remsec DNS Lookup (we .q.tcow.eu)
- [ ] ET MALWARE RAMNIT.A M2
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gootkit C2)
- [x] ET MALWARE Win32/Radonskra.B C2 Check-in
- [x] ET MALWARE Linux/Lady CnC Beacon 2
- [x] ET MALWARE Monsoon Tinytyphon CnC Beacon Exfiltrating Docs
- [x] ET MALWARE DarkHotel DNS Lookup (apply.ebizx.net)
- [x] ET MALWARE Aveo C2 Response
- [ ] ET MALWARE Curso Banker.BR Checkin
- [x] ET MALWARE Alfa/Alpha Ransomware Checkin
- [ ] ET MALWARE R980/CRYPBEE.A Ransomware Activity
- [x] ET MALWARE PNScan.2 Inbound Status Check Response

☐ ET MALWARE PNScan.2 CnC Beacon
☐ ET MALWARE PNScan.2 CnC Beacon 2
☑ ET MALWARE Backdoor.Win32.DarkComet Keepalive Outbound
☑ ET MALWARE Possible Pegasus Related DNS Lookup (aalaan .tv)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (accounts .mx)
☐ ET MALWARE Possible Pegasus Related DNS Lookup (adjust-local-settings .com)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (alawaeltech .com)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (alljazeera .co)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (asrararabiya .co)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (asrararablya .com)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (asrarrarabiya .com)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (bahrainsms .co)
☐ ET MALWARE Possible Pegasus Related DNS Lookup (bbc-africa .com)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (bulbazaur .com)
☐ ET MALWARE Possible Pegasus Related DNS Lookup (checkinonlinehere .com)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (cnn-africa .co)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (damanhealth .online)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (emiratesfoundation .net)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (fb-accounts .com)
☐ ET MALWARE Possible Pegasus Related DNS Lookup (googleplay-store .com)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (icloudcacher .com)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (icrcworld .com)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (manoraonline .net)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (mz-vodacom .info)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (newtarrifs .net)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (ooredoodeals .com)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (pickuchu .com)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (redcrossworld .com)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (sabafon .info)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (smser .net)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (sms .webadv.co)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (topcontactco .com)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (tpcontact .co.uk)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (track-your-fedex-package .org)
☐ ET MALWARE Possible Pegasus Related DNS Lookup (turkeynewsupdates .com)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (turkishairines .info)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (uaenews .online)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (univision .click)
☐ ET MALWARE Possible Pegasus Related DNS Lookup (unonoticias .net)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (whatsapp-app .com)
☑ ET MALWARE Possible Pegasus Related DNS Lookup (y0utube .com.mx)
☑ ET MALWARE Possible Pegasus/Trident Related HTTP Beacon 1
☑ ET MALWARE Possible Pegasus/Trident Related HTTP Beacon 2
☐ ET MALWARE Possible Pegasus/Trident Related HTTP Beacon 3
☑ ET MALWARE Possible Pegasus/Trident Related HTTP Beacon 4
☑ ET MALWARE Possible Pegasus/Trident Related HTTP Beacon 5
☑ ET MALWARE TorrentLocker DNS Lookup (bigcrashcar.net)
☑ ET MALWARE AgentTesla PWS HTTP CnC Checkin
☑ ET MALWARE Locky Ransomware Renaming File via SMB
☑ ET MALWARE Locky Ransomware Writing Instructions via SMB
☑ ET MALWARE Zlader Ransomware Worm Propagating Over SMB v1 ASCII
☐ ET MALWARE BartCrypt Payment DNS Query to .onion proxy Domain (s3clm4lufbmfhmeb)
☑ ET MALWARE Linux/LuaBot CnC Beacon
☑ ET MALWARE Linux/LuaBot CnC Beacon Response
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Vawtrak CnC)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
☑ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Vawtrak CnC)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Vawtrak CnC)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Vawtrak CnC)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi CnC)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Hancitor CnC)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (RockLoader CnC)
☐ ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
☑ ET MALWARE ABUSE.CH Ransomware Domain Detected (Locky C2)
☑ ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker C2)
☑ ET MALWARE OSX/Mokes.A CnC Heartbeat Request (set)

- [x] ET MALWARE OSX/Mokes.A CnC Heartbeat
- [x] ET MALWARE Quant Loader Download Request
- [x] ET MALWARE Quant Loader Download Response
- [x] ET MALWARE Windows dir Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Windows Microsoft Windows DOS prompt command Error Invalid Argument
- [x] ET MALWARE Windows Microsoft Windows DOS prompt command Error not recognized
- [x] ET MALWARE Windows Microsoft Windows DOS prompt command Error not found
- [x] ET MALWARE Windows net statistics workstation Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Windows net statistics server Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Windows driverquery -v Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Windows driverquery -si Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Windows qwinsta Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Windows quser Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Windows gpresult Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Windows netsh advfirewall show allprofiles Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Windows WMIC OS get Microsoft Windows DOS prompt command exit OUTBOUND
- [ ] ET MALWARE Windows WMIC COMPUTERSYSTEM get Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Windows WMIC NETLOGIN get Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Windows WMIC NIC get Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Windows WMIC PROCESS get Microsoft Windows DOS prompt command exit OUTBOUND
- [ ] ET MALWARE Windows WMIC SERVER get Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Windows WMIC SERVICE get Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Windows WMIC SHARE get Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Windows WMIC SYSACCOUNT get Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE Windows WMIC STARTUP get Microsoft Windows DOS prompt command exit OUTBOUND
- [x] ET MALWARE LuminosityLink - Inbound Data Channel CnC Delimiter
- [x] ET MALWARE LuminosityLink - Outbound Data Channel CnC Delimiter
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE Windows sc query Microsoft Windows DOS prompt command exit OUTBOUND
- [ ] ET MALWARE Ransomware Locky .onion Payment Domain (f5xraa2y2ybtrefz)
- [x] ET MALWARE Book of Eli CnC Checkin
- [ ] ET MALWARE Libyan Scorpions Adwind DNS Lookup (winmeif .myq-see.com)
- [x] ET MALWARE Libyan Scorpions Adwind DNS Lookup (collge .myq-see.com)
- [x] ET MALWARE Libyan Scorpions Adwind DNS Lookup (sara2011 .no-ip.biz)
- [ ] ET MALWARE Libyan Scorpions Netwire RAT DNS Lookup (samsung .ddns.me)
- [x] ET MALWARE Libyan Scorpions Netwire RAT DNS Lookup (wininit .myq-see.com)
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected (Locky C2)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Qadars MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE BleedingLife EK CVE-2014-6332 Exploit
- [ ] ET MALWARE BleedingLife EK CVE-2016-0189 Exploit
- [ ] ET MALWARE BleedingLife EK Payload Request
- [ ] ET MALWARE BleedingLife EK Payload Delivered
- [x] ET MALWARE Win32.Pony Variant FOX Checkin
- [ ] ET MALWARE Win32.Pony Variant FOX Reporting Adfraud Activity
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist DNS Lookup (Gozi MITM) (gtldsfs .com)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist DNS Lookup (Gozi MITM) (cdnfastnetwork .com)
- [x] ET MALWARE APT28 Komplex DNS Lookup (appleupdate .com)
- [x] ET MALWARE APT28 Komplex DNS Lookup (apple-iclouds .net)
- [x] ET MALWARE APT28 Komplex DNS Lookup (itunes-helper .net)
- [x] ET MALWARE Anuna PHP Backdoor Attempt
- [x] ET MALWARE Anuna PHP Backdoor Sucessful Exploit
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist DNS Lookup (Gozi MITM) (sdpvss .com)
- [ ] ET MALWARE Possible Locky AlphaNum Downloader Oct 3 2016
- [ ] ET MALWARE Possible Locky AlphaNum Downloader Oct 3 2016
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)

- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE ABUSE.CH TorrenLocker Payment Domain Detected
- [x] ET MALWARE ABUSE.CH Locky Payment Domain Detected
- [x] ET MALWARE CryptoWall/TeslaCrypt Payment Domain
- [x] ET MALWARE Linux.Mirai Login Attempt (xc3511)
- [x] ET MALWARE Nuke Ransomware Checkin
- [x] ET MALWARE Win32/Infostealer.Snifula File Upload
- [ ] ET MALWARE Malicious SSL certificate detected (Powershell Trojan)
- [x] ET MALWARE Win32/CryPy Ransomware CnC Checkin
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gootkit C2)
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 106
- [x] ET MALWARE Observed AgentTesla Domain Request
- [x] ET MALWARE APT28/Sednit DNS Lookup (aljazeera-news .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (bbc-press .org)
- [x] ET MALWARE APT28/Sednit DNS Lookup (dailyforeignnews .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (defenceiq .us)
- [x] ET MALWARE APT28/Sednit DNS Lookup (diplomatnews .org)
- [x] ET MALWARE APT28/Sednit DNS Lookup (euroreport24 .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (military-info .eu)
- [x] ET MALWARE APT28/Sednit DNS Lookup (militaryobserver .net)
- [x] ET MALWARE APT28/Sednit DNS Lookup (nato-news .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (natopress .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (osce-press .org)
- [x] ET MALWARE APT28/Sednit DNS Lookup (politicalreview .eu)
- [x] ET MALWARE APT28/Sednit DNS Lookup (reuters-press .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (stratforglobal .net)
- [x] ET MALWARE APT28/Sednit DNS Lookup (theguardiannews .org)
- [x] ET MALWARE APT28/Sednit DNS Lookup (unian-news .info)
- [x] ET MALWARE APT28/Sednit DNS Lookup (virusdefender .org)
- [x] ET MALWARE APT28/Sednit DNS Lookup (worldpoliticsnews .org)
- [x] ET MALWARE APT28/Sednit DNS Lookup (dataclen .org)
- [x] ET MALWARE APT28/Sednit DNS Lookup (windowscheckupdater .net)
- [x] ET MALWARE APT28/Sednit DNS Lookup (biocpl .org)
- [x] ET MALWARE Bitter RAT TCP CnC Beacon
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE APT28/Sednit DNS Lookup (timezoneutc .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (advpdxapi .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (driversupdate .info)
- [x] ET MALWARE APT28/Sednit DNS Lookup (microsoftdriver .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (nortonupdate .org)
- [x] ET MALWARE APT28/Sednit DNS Lookup (symantecsupport .org)
- [x] ET MALWARE APT28/Sednit DNS Lookup (updatesystems .net)
- [x] ET MALWARE APT28/Sednit DNS Lookup (windowsappstore .net)
- [x] ET MALWARE SA Banker Checkin
- [x] ET MALWARE Ransomware/Cerber Onion Domain Lookup
- [x] ET MALWARE Ransomware/Cerber Onion Domain Lookup
- [x] ET MALWARE Possible Linux.Mirai Login Attempt (1111111)
- [x] ET MALWARE Possible Linux.Mirai Login Attempt (666666)
- [x] ET MALWARE Possible Linux.Mirai Login Attempt (7ujMko0vizxv)
- [x] ET MALWARE Possible Linux.Mirai Login Attempt (anko)
- [x] ET MALWARE Possible Linux.Mirai Login Attempt (fucker)
- [x] ET MALWARE Possible Linux.Mirai Login Attempt (ikwb)
- [x] ET MALWARE Possible Linux.Mirai Login Attempt (jvbzd)
- [x] ET MALWARE Possible Linux.Mirai Login Attempt (klv1234)
- [x] ET MALWARE Possible Linux.Mirai Login Attempt (realtek)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH TorrenLocker Payment Domain Detected
- [ ] ET MALWARE CryptoWall/TeslaCrypt Payment Domain
- [x] ET MALWARE CryptoWall/TeslaCrypt Payment Domain
- [x] ET MALWARE Enigma Locker Checkin
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE TheTrick Banking Trojan User-Agent
- [x] ET MALWARE APT28 DealersChoice.B DNS Lookup (appexsrv .net)
- [x] ET MALWARE Win32/CryPy Ransomware Encrypting File
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Vawtrak CnC)
- [x] ET MALWARE APT28/Sednit DNS Lookup (microsoftsupp .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (ausameetings .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (cnnpolitics .eu)
- [x] ET MALWARE APT28/Sednit DNS Lookup (dailypoliticsnews .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (defencereview .eu)
- [x] ET MALWARE APT28/Sednit DNS Lookup (euronews24 .info)
- [x] ET MALWARE APT28/Sednit DNS Lookup (kg-news .org)
- [x] ET MALWARE APT28/Sednit DNS Lookup (militaryadviser .org)
- [x] ET MALWARE APT28/Sednit DNS Lookup (nato-hq .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (natoint .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (osce-info .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (pakistan-mofa .net)
- [x] ET MALWARE APT28/Sednit DNS Lookup (politicsinform .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (shurl .biz)
- [x] ET MALWARE APT28/Sednit DNS Lookup (thediplomat-press .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (trend-news .org)
- [x] ET MALWARE APT28/Sednit DNS Lookup (unitednationsnews .eu)
- [x] ET MALWARE APT28/Sednit DNS Lookup (worldmilitarynews .org)
- [x] ET MALWARE APT28/Sednit DNS Lookup (capisp .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (mscoresvw .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (acledit .com)
- [x] ET MALWARE Win32/CryptFile2 Ransomware Checkin M2
- [x] ET MALWARE Bitter RAT HTTP CnC Beacon
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Vawtrak CnC)
- [x] ET MALWARE APT28/Sednit DNS Lookup (ciscohelpcenter .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (inteldrv64 .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (cloudflarecdn .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (kenlynton .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (microsofthelpcenter .info)
- [x] ET MALWARE APT28/Sednit DNS Lookup (softwaresupportsv .com)
- [x] ET MALWARE APT28/Sednit DNS Lookup (updatecenter .name)
- [x] ET MALWARE APT28/Sednit DNS Lookup (updmanager .com)
- [x] ET MALWARE APT28/Sednit SSL Cert
- [x] ET MALWARE Ransomware/Cerber Onion Domain Lookup
- [x] ET MALWARE Ransomware/Cerber Onion Domain Lookup
- [x] ET MALWARE Houdini/Hworm CnC Checkin M1
- [x] ET MALWARE Possible Linux.Mirai Login Attempt (54321)
- [x] ET MALWARE Possible Linux.Mirai Login Attempt (7ujMko0admin)
- [x] ET MALWARE Possible Linux.Mirai Login Attempt (888888)
- [x] ET MALWARE Possible Linux.Mirai Login Attempt (dreambox)
- [x] ET MALWARE Possible Linux.Mirai Login Attempt (hi3518)
- [x] ET MALWARE Possible Linux.Mirai Login Attempt (juantech)
- [x] ET MALWARE Possible Linux.Mirai Login Attempt (klv123)
- [x] ET MALWARE Possible Linux.Mirai Login Attempt (meinsm)
- [x] ET MALWARE Possible Linux.Mirai Login Attempt (service)

- [x] ET MALWARE Possible Linux.Mirai Login Attempt (ubnt)
- [x] ET MALWARE Possible Linux.Mirai Login Attempt (xmhdipc)
- [x] ET MALWARE Possible Linux.Mirai Login Attempt (Zte521)
- [x] ET MALWARE Win32/Jackpot Ransomware CnC Checkin
- [x] ET MALWARE Possible Malicious Tor Module Download
- [x] ET MALWARE Moose CnC Request M1
- [x] ET MALWARE Moose CnC Request M2
- [x] ET MALWARE JS/HTA Downloader Behavior M3
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Vawtrak CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (FindPOS CnC)
- [ ] ET MALWARE XRatLocker/AiraCrop Ransomware Payment Domain
- [x] ET MALWARE CerberTear Ransomware CnC Checkin
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Vawtrak CnC)
- [x] ET MALWARE KeyBoy DNS Lookup (www .about.jkub.com)
- [x] ET MALWARE KeyBoy DNS Lookup (www .backus.myftp.name)
- [x] ET MALWARE KeyBoy CnC Beacon
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL Certificate Detected (Chthonic MITM)
- [x] ET MALWARE Win32/CHIP Ransomware CnC Checkin
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gootkit C2)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TrickBot CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gootkit CnC)
- [x] ET MALWARE Win32/TrojanDownloader.Delf.BVP Win32/BioData CnC Beacon
- [ ] ET MALWARE Malicious SSL Certificate Detected (Gootkit CnC)
- [x] ET MALWARE Locky CnC checkin Nov 21 M2
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE Sharik/Smoke Loader Receiving Payload
- [x] ET MALWARE DistTrack/Shamoon CnC Beacon M2
- [ ] ET MALWARE Unknown AutoIt Bot DNS Lookup (webmail .duia.in)
- [x] ET MALWARE Locky CnC Checkin Dec 5 M1
- [ ] ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker C2)
- [x] ET MALWARE ABUSE.CH Ransomware/Cerber Onion Domain Lookup
- [x] ET MALWARE ABUSE.CH Ransomware/Cerber Onion Domain Lookup
- [ ] ET MALWARE Ransomware Goldeneye .onion Payment Domain (goldenhjnqvc2lld)
- [x] ET MALWARE Trojan.Win32.Qadars Checkin
- [ ] ET MALWARE Zeus OPENSSL Banker Malicious SSL Certificate Detected
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
- [x] ET MALWARE Trojan.Kwampirs Outbound GET request
- [ ] ET MALWARE Mirai Botnet Domain Observed
- [x] ET MALWARE Mirai Botnet Domain Observed
- [x] ET MALWARE Mirai Botnet Domain Observed
- [x] ET MALWARE Possible Linux.Mirai Login Attempt (vizxv)
- [x] ET MALWARE Possible Linux.Mirai Login Attempt (zlxx)
- [x] ET MALWARE Ransomware/Cerber Checkin 2
- [x] ET MALWARE Possible Emissary External IP Lookup
- [x] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)
- [x] ET MALWARE Moose CnC Response
- [x] ET MALWARE MSIL/HadesLocker Ransomware Checkin
- [x] ET MALWARE Sednit/APT28/Sofacy Delphocy CnC Beacon
- [x] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gootkit C2)
- [ ] ET MALWARE XRatLocker/AiraCrop Ransomware Payment Domain
- [x] ET MALWARE MSIL/Alcatrez Locker Ransomware CnC Checkin
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Vawtrak CnC)
- [x] ET MALWARE KeyBoy DNS Lookup (www .eleven.mypop3.org)
- [x] ET MALWARE KeyBoy DNS Lookup (tibetvoices .com)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL Certificate Detected (Chthonic CnC)
- [x] ET MALWARE CryptoLuck / YafunnLocker Ransomware CnC Checkin
- [ ] ET MALWARE Observed Malicious SSL Cert (FlokiBot CnC)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Tuhkit C2)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Vawtrak CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Zeus CnC)
- [x] ET MALWARE Win32/VB.SDB CnC Beacon
- [x] ET MALWARE Win32/TrojanDownloader.Delf.BXC CnC Beacon
- [x] ET MALWARE Locky CnC checkin Nov 21
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Flokibot CnC)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gozi MITM)
- [x] ET MALWARE DistTrack/Shamoon CnC Beacon M1
- [x] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gootkit C2)
- [x] ET MALWARE User-Agent (Visbot)
- [x] ET MALWARE Locky CnC Checkin HTTP Pattern
- [x] ET MALWARE ABUSE.CH Ransomware/Cerber Onion Domain Lookup
- [x] ET MALWARE ABUSE.CH Ransomware/Cerber Onion Domain Lookup
- [x] ET MALWARE Known Malicious Doc Downloading Payload Dec 06 2016
- [ ] ET MALWARE Ransomware Goldeneye .onion Payment Domain (golden2uqpiqcs6j)
- [ ] ET MALWARE Ransomware Popcorn-Time .onion Payment Domain (3hnuhydu4pd247qb)
- [ ] ET MALWARE Zeus OPENSSL Banker Malicious SSL Certificate Detected
- [ ] ET MALWARE JS/WSF Downloader Dec 08 2016
- [ ] ET MALWARE JS/WSF Downloader Dec 08 2016 M2
- [ ] ET MALWARE Mirai Botnet Domain Observed
- [ ] ET MALWARE Mirai Botnet Domain Observed
- [x] ET MALWARE Mirai Botnet Domain Observed

- [x] ET MALWARE Mirai Botnet Domain Observed
- [ ] ET MALWARE Mirai Botnet Domain Observed
- [ ] ET MALWARE Mirai Botnet Domain Observed
- [x] ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 107
- [x] ET MALWARE Ransomware/Cerber Checkin M3 (2)
- [x] ET MALWARE Ransomware/Cerber Checkin M3 (4)
- [x] ET MALWARE Ransomware/Cerber Checkin M3 (6)
- [x] ET MALWARE Ransomware/Cerber Checkin M3 (8)
- [x] ET MALWARE Ransomware/Cerber Checkin M3 (10)
- [x] ET MALWARE Ransomware/Cerber Checkin M3 (12)
- [x] ET MALWARE Ransomware/Cerber Checkin M3 (14)
- [x] ET MALWARE Ransomware/Cerber Checkin M3 (16)
- [ ] ET MALWARE Mirai Botnet Domain Observed
- [x] ET MALWARE Mirai Botnet Domain Observed
- [x] ET MALWARE Mirai Botnet Domain Observed
- [x] ET MALWARE Mirai Botnet Domain Observed
- [ ] ET MALWARE NEODYMIUM Wingbird DNS Lookup (srv601 .ddns.net)
- [x] ET MALWARE PROMETHIUM/StrongPity DNS Lookup (updatesync .com)
- [x] ET MALWARE PROMETHIUM/StrongPity DNS Lookup (mynetenergy .com)
- [x] ET MALWARE PROMETHIUM/StrongPity DNS Lookup (truecrypte .org)
- [x] ET MALWARE PROMETHIUM/StrongPity DNS Lookup (jourrapid .com)
- [x] ET MALWARE PROMETHIUM/StrongPity DNS Lookup (myrappid .com)
- [x] ET MALWARE TeleBots BCS-server User-Agent
- [ ] ET MALWARE Ransomware Maktub .onion Payment Domain (maktubebz6z6cgtw)
- [x] ET MALWARE APT28 DealersChoice DNS Lookup
- [x] ET MALWARE APT28 DealersChoice DNS Lookup
- [x] ET MALWARE APT28 DealersChoice DNS Lookup
- [x] ET MALWARE APT28 DealersChoice DNS Lookup
- [x] ET MALWARE APT28 DealersChoice DNS Lookup
- [x] ET MALWARE Click Fraud Checkin
- [x] ET MALWARE JS/WSF Downloader Dec 08 2016 M4
- [x] ET MALWARE Possible Linux.Mirai DaHua Default Credentials Login
- [ ] ET MALWARE Tofsee DGA (2016-12-15 to 2017-05-04)
- [x] ET MALWARE JS/WSF Downloader Dec 08 2016 M6
- [x] ET MALWARE Ransomware/Cerber Onion Domain Lookup
- [x] ET MALWARE MRCR1 Ransomware Checkin M2
- [x] ET MALWARE Blackmoon/Banbra Configuration Request M2
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected (Locky C2)
- [x] ET MALWARE JS/WSF Downloader Dec 08 2016 M7
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi CnC)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Malware CnC)
- [x] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TrickBot CnC)
- [ ] ET MALWARE DeepEnd Research Ransomware PadCrypt .onion Proxy Domain
- [ ] ET MALWARE DeepEnd Research Ransomware CrypMIC Payment Onion Domain
- [ ] ET MALWARE DeepEnd Research Ransomware PadCrypt .onion Proxy Domain

- [ ] ET MALWARE Mirai Botnet Domain Observed
- [ ] ET MALWARE Mirai Botnet Domain Observed
- [ ] ET MALWARE Mirai Botnet Domain Observed
- [x] ET MALWARE Ransomware/Cerber Checkin M3 (1)
- [x] ET MALWARE Ransomware/Cerber Checkin M3 (3)
- [x] ET MALWARE Ransomware/Cerber Checkin M3 (5)
- [x] ET MALWARE Ransomware/Cerber Checkin M3 (7)
- [x] ET MALWARE Ransomware/Cerber Checkin M3 (9)
- [x] ET MALWARE Ransomware/Cerber Checkin M3 (11)
- [x] ET MALWARE Ransomware/Cerber Checkin M3 (13)
- [x] ET MALWARE Ransomware/Cerber Checkin M3 (15)
- [ ] ET MALWARE Mirai Botnet Domain Observed
- [x] ET MALWARE Mirai Botnet Domain Observed
- [ ] ET MALWARE Mirai Botnet Domain Observed
- [x] ET MALWARE Mirai Botnet Domain Observed
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gootkit C2)
- [x] ET MALWARE NEODYMIUM Wingbird DNS Lookup (srv602 .ddns.net)
- [x] ET MALWARE PROMETHIUM/StrongPity DNS Lookup (svnservices .com)
- [x] ET MALWARE PROMETHIUM/StrongPity DNS Lookup (windriversupport .com)
- [x] ET MALWARE PROMETHIUM/StrongPity DNS Lookup (edicupd002 .com)
- [x] ET MALWARE PROMETHIUM/StrongPity DNS Lookup (true-crypte .website)
- [x] ET MALWARE TeleBots BCS-server CnC Beacon
- [x] ET MALWARE TeleBots VBS Backdoor CnC Beacon 1
- [x] ET MALWARE TeleBots VBS Backdoor CnC Beacon 2
- [x] ET MALWARE APT28 DealersChoice DNS Lookup
- [x] ET MALWARE APT28 DealersChoice DNS Lookup
- [x] ET MALWARE APT28 DealersChoice DNS Lookup
- [x] ET MALWARE APT28 DealersChoice DNS Lookup
- [x] ET MALWARE APT28/SEDNIT Uploader Variant DNS Lookup
- [x] ET MALWARE JS/WSF Downloader Dec 08 2016 M3
- [ ] ET MALWARE JS/WSF Downloader Dec 08 2016 M5
- [x] ET MALWARE Win32/Braincrypt Ransomware CnC Checkin
- [ ] ET MALWARE Tofsee DGA (2017-05-04 to 2017-11-02)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Gootkit CnC)
- [x] ET MALWARE MRCR1 Ransomware Checkin M1
- [x] ET MALWARE Win32.Banker.bqba Checkin
- [ ] ET MALWARE W32/Cerber.Ransomware CnC Checkin M4
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker Payment)
- [x] ET MALWARE Linux/Venom CnC Beacon
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Quakbot CnC)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Chthonic CnC)
- [x] ET MALWARE Spora Ransomware DNS Query
- [ ] ET MALWARE DeepEnd Research Ransomware CrypMIC Payment Onion Domain
- [ ] ET MALWARE DeepEnd Research Ransomware CrypMIC Payment Onion Domain
- [ ] ET MALWARE DeepEnd Research Ransomware PadCrypt .onion Proxy Domain

- [ ] ET MALWARE DeepEnd Research Ransomware CrypMIC Payment Onion Domain
- [ ] ET MALWARE DeepEnd Research Ransomware CryptoWall .onion Proxy Domain
- [ ] ET MALWARE Ransomware CrypMIC Payment Onion Domain
- [x] ET MALWARE Maldoc Second Stage VBS Downloader with URL Padding
- [x] ET MALWARE Possible Pony Payload DL
- [x] ET MALWARE Pony DLL Download M2
- [x] ET MALWARE User-Agent (Xmaker)
- [x] ET MALWARE Evil JS Ransomware
- [x] ET MALWARE Malicious JS.Nemucod to PS Dropping PE Nov 14 M2
- [x] ET MALWARE APT28 DealersChoice DNS Lookup (gtranm .com)
- [x] ET MALWARE APT28 DealersChoice DNS Lookup (zpfgr .com)
- [x] ET MALWARE OSX Backdoor Quimitchin DNS Lookup
- [x] ET MALWARE X2000M.Agent Checkin Jan 24 2017
- [x] ET MALWARE Betabot Checkin 5
- [x] ET MALWARE Sage Ransomware Checkin Primer
- [x] ET MALWARE Sage Ransomware Checkin
- [ ] ET MALWARE Possible Unknown Trojan Checkin Jan 26 2017
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (webfile .myq-see.com)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (downloadmyhost .zapto.org)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (help2014 .linkpc.net)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (safara .sytes.net)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (exportball .servegame.org)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (viewnet .better-than.tv)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (down .downloadoneyoutube.co.vu)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (netstreamag .publicvm.com)
- [ ] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (hostgatero .ddns.net)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (subsidiaryohio .linkpc.net)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (helpyoume .linkpc.net)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (downloadtesting .com)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (gameoolines .com)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (onlinesoft .space)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (newphoneapp .com)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (gamestoplay .bid)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (smartsftp .pw)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (galaxysupdates .com)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (galaxy-s .com)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (datasamsung .com)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (progsupdate .com)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (topgamse .com)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (bandtester .com)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (speedbind .com)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (ukgames .tech)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (wallanews .publicvm.com)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (wallanews .sytes.net)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (noredirecto .redirectme.net)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (dynamicipaddress .linkpc.net)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (downloadlog .linkpc.net)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (havan .qhigh.com)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (kolabdown .sytes.net)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (rotter2 .publicvm.com)
- [x] ET MALWARE DustySky Downeks/Quasar/other DNS Lookup (ftpserverit .otzo.com)
- [x] ET MALWARE Downeks Variant CnC Beacon
- [ ] ET MALWARE Possible DustySky PoisonIvy CnC Beacon
- [ ] ET MALWARE DustySky QuasarRAT CnC Beacon
- [x] ET MALWARE CryptoShield Ransomware Checkin
- [x] ET MALWARE Shafttt MySQL Bruteforce Bot CnC Beacon
- [x] ET MALWARE WSF/JS Downloader Jan 30 2017 M1
- [x] ET MALWARE Turla Kopiluwak User-Agent
- [x] ET MALWARE Ursnif Variant CnC Beacon
- [x] ET MALWARE Ursnif Variant Retrieving Payload (x32)
- [x] ET MALWARE Ursnif Variant Retrieving Payload (x64)
- [x] ET MALWARE JS/Nemucod requesting EXE payload 2016-02-06
- [x] ET MALWARE Possible iKittens OSX MacDownloader CNC Beacon
- [x] ET MALWARE iKittens OSX MacDownloader DNS Lookup (officialswebsites .info)
- [ ] ET MALWARE Banker.Win32.Alreay DNS Lookup (tradeboard .mefound .com)
- [ ] ET MALWARE Banker.Win32.Alreay DNS Lookup (movis-es .ignorelist .com)
- [ ] ET MALWARE Banker.Win32.Alreay DNS Lookup (exbonus .mrbasic .com)
- [x] ET MALWARE Spora Ransomware DNS Query
- [ ] ET MALWARE Qadars CnC DNS Lookup (bst2bgxin81a.org)
- [x] ET MALWARE Qadars CnC DNS Lookup (websecuranalityc.com)
- [x] ET MALWARE Qadars CnC DNS Lookup (liveskansys.com)
- [x] ET MALWARE Possible Pegasus Related DNS Lookup (iusacell-movil .com.mx)
- [x] ET MALWARE Possible Pegasus Related DNS Lookup (smsmensaje .mx)
- [ ] ET MALWARE Unknown Malicious SSL Cert 1
- [ ] ET MALWARE Unknown Malicious SSL Cert 2
- [ ] ET MALWARE Unknown Malicious SSL Cert 3
- [ ] ET MALWARE Unknown Malicious SSL Cert 4
- [ ] ET MALWARE Unknown Malicious SSL Cert 5
- [ ] ET MALWARE Unknown Malicious SSL Cert 6
- [ ] ET MALWARE Unknown Malicious SSL Cert 7
- [x] ET MALWARE Miniduke variant C&C activity
- [x] ET MALWARE CosmicDuke Exfiltrating Data via FTP STOR
- [x] ET MALWARE Miniduke variant FTP upload
- [x] ET MALWARE APT28 SEDNIT Variant CnC Beacon 1
- [x] ET MALWARE APT28 SEDNIT Variant CnC Beacon 2
- [x] ET MALWARE APT28 SEDNIT Variant CnC Beacon 3

☑ ET MALWARE APT28 SEDNIT Variant CnC Beacon 4
☑ ET MALWARE APT28 Uploader Variant CnC Beacon
☑ ET MALWARE APT28 Uploader Variant Fake Request to Google
☑ ET MALWARE MiniDuke CnC Beacon (string1_slide_1_1)
☑ ET MALWARE MiniDuke CnC Beacon (string1_slide_1_2)
☑ ET MALWARE MiniDuke CnC Beacon (string1_slide_2_1)
☑ ET MALWARE MiniDuke CnC Beacon (string1_slide_2_2)
☑ ET MALWARE MiniDuke CnC Beacon (string1_slide_3_1)
☑ ET MALWARE MiniDuke CnC Beacon (string1_slide_3_2)
☑ ET MALWARE MiniDuke CnC Beacon (string2_slide_1_1)
☑ ET MALWARE MiniDuke CnC Beacon (string2_slide_1_2)
☑ ET MALWARE MiniDuke CnC Beacon (string2_slide_2_1)
☑ ET MALWARE MiniDuke CnC Beacon (string2_slide_2_2)
☑ ET MALWARE MiniDuke CnC Beacon (string2_slide_3_1)
☑ ET MALWARE MiniDuke CnC Beacon (string2_slide_3_2)
☑ ET MALWARE Miniduke Variant CnC Beacon via WebDAV
☑ ET MALWARE APT29 Cache_DLL SSL Cert
☑ ET MALWARE Qadars CnC DNS Lookup (zkdef09i7ola.net)
☑ ET MALWARE MAGICHOUND.MPK Activity via IRC
☑ ET MALWARE Possibly Malicious Base64 Unicode WebClient DownloadString M1
☐ ET MALWARE Possibly Malicious Base64 Unicode WebClient DownloadString M2
☑ ET MALWARE Possibly Malicious Base64 Unicode WebClient DownloadString M3
☑ ET MALWARE Possibly Malicious Double Base64 Unicode Net.ServicePointManager M1
☑ ET MALWARE Possibly Malicious Double Base64 Unicode Net.ServicePointManager M2
☑ ET MALWARE Possibly Malicious Double Base64 Unicode Net.ServicePointManager M3
☑ ET MALWARE Possible Malicious PowerSploit PowerShell Script Observed over HTTP
☑ ET MALWARE MAGICHOUND.FETCH Retrieving Malicious PowerShell
☑ ET MALWARE Likely MAGICHOUND.FETCH Receiving PowerSploit PowerShell over HTTP
☑ ET MALWARE MAGICHOUND.RETRIEVER CnC Beacon
☑ ET MALWARE MAGICHOUND.FETCH CnC Beacon
☐ ET MALWARE MAGICHOUND.FETCH SSL Cert
☑ ET MALWARE MAGICHOUND-related DNS Lookup (chrome-up .date)
☑ ET MALWARE MAGICHOUND-related DNS Lookup (timezone .live)
☑ ET MALWARE MAGICHOUND-related DNS Lookup (servicesystem .serveirc.com)
☑ ET MALWARE MAGICHOUND-related DNS Lookup (analytics-google .org)
☑ ET MALWARE MAGICHOUND-related DNS Lookup (com-adm .in)
☑ ET MALWARE MAGICHOUND-related DNS Lookup (microsoftexplorerservices .cloud)
☑ ET MALWARE MAGICHOUND-related DNS Lookup (msservice .site)
☑ ET MALWARE MAGICHOUND-related DNS Lookup (com-ho .me)
☑ ET MALWARE MAGICHOUND-related DNS Lookup (ntg-sa .com)
☑ ET MALWARE MAGICHOUND-related DNS Lookup (briefl .ink)
☑ ET MALWARE MAGICHOUND.LEASH IRC CnC Beacon
☑ ET MALWARE CozyCar CnC Beacon
☑ ET MALWARE CozyCar V2 CnC Beacon
☑ ET MALWARE APT29 Implant8 - Evil Twitter Callback
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 1
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 2
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 3
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 4
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 5
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 6
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 7
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 8
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 9
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 10
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 11
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 12
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 13
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 14
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 15
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 16
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 17
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 18
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 19
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 20
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 21
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 22
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 23
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 24
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 25
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 26
☑ ET MALWARE ShellCrew.APT StreamEx DNS Lookup 27
☑ ET MALWARE ABUSE.CH Ransomware Domain Detected (TorrentLocker C2)
☑ ET MALWARE APT29 Implant8 - MAL_REFERER
☑ ET MALWARE FakeM SSL DNS Lookup (islamhood .net)
☑ ET MALWARE Pteranodon Backdoor Checkin
☑ ET MALWARE Pteranodon Backdoor CnC POST
☑ ET MALWARE Pteranodon Variant 1 Backdoor Checkin
☑ ET MALWARE Pteranodon Variant 2 Backdoor Checkin
☑ ET MALWARE Pteranodon Variant 3 Backdoor Checkin
☑ ET MALWARE Gamaredon File Stealer POST
☑ ET MALWARE Infostealer.Bancos ProxyChanger Checkin
☑ ET MALWARE WS/JS Downloader Mar 07 2017 M1
☑ ET MALWARE WS/JS Downloader Mar 07 2017 M2
☑ ET MALWARE Spora Ransomware Checkin
☑ ET MALWARE Spora Ransomware SSL Certificate Detected
☑ ET MALWARE Win32/CryptFile2 / Revenge Ransomware Checkin M3
☑ ET MALWARE MagikPOS Downloader Retrieving Payload
☑ ET MALWARE MagikPOS Downloader Checkin
☑ ET MALWARE MagikPOS CnC Beacon
☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Android Marcher C2)
☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Chthonic MITM)
☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)

- ☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
- ☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
- ☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
- ☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
- ☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
- ☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
- ☑ ET MALWARE ABUSE.CH Ransomware/Cerber Onion Domain Lookup
- ☑ ET MALWARE Win32/Teslacrypt Ransomware .onion domain (7tno4hib47vlep5o)
- ☐ ET MALWARE DeepEnd Research Ransomware CrypMIC Payment Onion Domain
- ☐ ET MALWARE DeepEnd Research Ransomware CrypMIC Payment Onion Domain
- ☐ ET MALWARE DeepEnd Research Ransomware CrypMIC Payment Onion Domain
- ☐ ET MALWARE DeepEnd Research Ransomware CrypMIC Payment Onion Domain
- ☑ ET MALWARE Ransomware CrypMIC Payment Onion Domain
- ☑ ET MALWARE MSIL/Matrix Ransomware CnC Activity
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (1e100 .tech)
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (ads-youtube .online)
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (alkamaihd .net)
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (broadcast-microsoft .tech)
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (cloudmicrosoft .net)
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (elasticbeanstalk .tech)
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (jguery .net)
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (microsoft-ds .com)
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (nameserver .win)
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (owa-microsoft .online)
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (qoldenlines .net)
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (ssl-gstatic .online)
- ☑ ET MALWARE Red Leaves magic packet detected (APT10 implant)
- ☑ ET MALWARE Red Leaves HTTP CnC Beacon (APT10 implant)
- ☑ ET MALWARE Felismus CnC Beacon 2
- ☑ ET MALWARE Win32/Neutrino Checkin 6
- ☑ ET MALWARE Possible Turla Carbon Paper CnC Beacon (Fake User-Agent)
- ☑ ET MALWARE DeepEnd Research Ransomware CrypMIC Payment Onion Domain
- ☑ ET MALWARE MSIL/Hidden-Tear Variant Ransomware CnC Checkin
- ☑ ET MALWARE Quant Loader Download Response M2
- ☑ ET MALWARE MSIL/Runsome Ransomware CnC Checkin
- ☑ ET MALWARE Unknown Possibly Ransomware (Dropped by RIG) CnC Beacon
- ☑ ET MALWARE ARM Binary Downloaded via WGET Containing GoAhead and Multiple Camera RCE 0Day Vulnerabilities
- ☑ ET MALWARE Known IoT Malware Domain
- ☐ ET MALWARE Observed Malicious SSL cert (pyteHole Ransomware)
- ☑ ET MALWARE Possible DANDERSPRITZ HTTP Beacon
- ☑ ET MALWARE DeepEnd Research Ransomware CrypMIC Payment Onion Domain
- ☑ ET MALWARE Turla Snake OSX DNS Lookup (car-service .effers.com)
- ☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
- ☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
- ☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
- ☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
- ☐ ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gozi MITM)
- ☑ ET MALWARE Win32/Spy.Banker.ACUT CnC Checkin
- ☑ ET MALWARE Win32/Teslacrypt Ransomware .onion domain (2kjb7.net)
- ☑ ET MALWARE KHRAT DragonOK DNS Lookup (inter-ctrip .com)
- ☐ ET MALWARE DeepEnd Research Ransomware CrypMIC Payment Onion Domain
- ☐ ET MALWARE DeepEnd Research Ransomware CrypMIC Payment Onion Domain
- ☐ ET MALWARE DeepEnd Research Ransomware CrypMIC Payment Onion Domain
- ☐ ET MALWARE Ransomware CrypMIC Payment Onion Domain
- ☑ ET MALWARE Ransomware CrypMIC Payment Onion Domain
- ☑ ET MALWARE MalDoc Retrieving Payload March 30 2017
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (1m100 .tech)
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (akamaitechnology .com)
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (azurewebsites .tech)
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (chromeupdates .online)
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (dnsserv .host)
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (fdgdsg .xyz)
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (jguery .online)
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (microsoft-security .host)
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (newsfeeds-microsoft .press)
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (primeminister-goverment-techcenter .tech)
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (sharepoint-microsoft .co)
- ☑ ET MALWARE Possible CopyKitten DNS Lookup (trendmicro .tech)
- ☑ ET MALWARE Red Leaves magic packet response detected (APT10 implant)
- ☑ ET MALWARE Felismus CnC Beacon 1
- ☑ ET MALWARE MSIL/Matrix Ransomware Sending Encrypted Filelist
- ☑ ET MALWARE MSIL/NR42 Bot Parsing Config From Webpage
- ☑ ET MALWARE DeepEnd Research Ransomware CrypMIC Payment Onion Domain
- ☑ ET MALWARE Win32/Mole Ransomware CnC Beacon
- ☐ ET MALWARE Win32/Cradle Ransomware Onion Domain
- ☑ ET MALWARE Possible Malicious Gzip PowerShell over HTTP
- ☑ ET MALWARE Known Malicious Expires Header Seen In Malicious JavaScript Downloader Campaign
- ☑ ET MALWARE MSIL/Karmen Ransomware CnC Activity
- ☑ ET MALWARE ARM Binary Requested via WGET to Known IoT Malware Domain
- ☐ ET MALWARE Known IoT Malware Domain
- ☑ ET MALWARE Possible DANDERSPRITZ Default HTTP Headers
- ☑ ET MALWARE DeepEnd Research Ransomware CrypMIC Payment Onion Domain
- ☐ ET MALWARE Kazuar CnC Beacon
- ☑ ET MALWARE W32.Geodo/Emotet Checkin

- [x] ET MALWARE SuperCMD CnC Beacon
- [ ] ET MALWARE W32/Emotet CnC Beacon 2
- [x] ET MALWARE MSIL/NewHT Ransomware CnC Checkin
- [x] ET MALWARE OSX/Proton.B DNS Lookup
- [x] ET MALWARE Turla SHIRIME DNS Lookup
- [x] ET MALWARE DNS Query to Jaff Domain (fkksjobnn43 . org)
- [x] ET MALWARE Possible WannaCry DNS Lookup 1
- [x] ET MALWARE Possible WannaCry DNS Lookup 3
- [x] ET MALWARE Possible WannaCry DNS Lookup 5
- [ ] ET MALWARE W32/WannaCry.Ransomware Killswitch Domain HTTP Request 2
- [ ] ET MALWARE W32/WannaCry.Ransomware Killswitch Domain HTTP Request 4
- [ ] ET MALWARE MSIL/May Ransomware SSL Cert Observed
- [x] ET MALWARE MWI Maldoc Posting Host Data
- [x] ET MALWARE LokiBot Application/Credential Data Exfiltration Detected M1
- [x] ET MALWARE LokiBot File Exfiltration Detected
- [x] ET MALWARE LokiBot Screenshot Exfiltration Detected
- [x] ET MALWARE LokiBot Request for C2 Commands Detected M2
- [x] ET MALWARE MSIL/EasyLocker Ransomware CnC Activity
- [x] ET MALWARE Win32/ASPC Bot CnC Checkin M1
- [ ] ET MALWARE Spora Ransomware DNS Query
- [x] ET MALWARE APT32 Komprogo DNS Lookup
- [x] ET MALWARE APT32 Komprogo DNS Lookup
- [x] ET MALWARE APT32 Komprogo DNS Lookup
- [x] ET MALWARE DNS Query to Jaff Domain (orhangazitur . com)
- [ ] ET MALWARE DNS Query to Jaff Domain (comboratiogferrdto . com)
- [x] ET MALWARE Executioner Ransomware Reporting Infection via SMTP
- [x] ET MALWARE OpenSSH in ICMP Payload - Possible Covert Channel
- [x] ET MALWARE Win32/Spectre Ransomware CnC Checkin
- [x] ET MALWARE Nemucod JS Downloader June 12 2017
- [x] ET MALWARE DPRK HIDDEN COBRA Botnet C2 Host Beacon
- [x] ET MALWARE Possible Pegasus Related DNS Lookup (network190 .com)
- [x] ET MALWARE Possible Pegasus Related DNS Lookup (smscentro .com)
- [x] ET MALWARE Possible Pegasus Related DNS Lookup (twiitter .com.mx)
- [x] ET MALWARE DragonOK KHRAT Downloader Receiving Payload
- [ ] ET MALWARE x0Proto File Contents Exfil Request
- [x] ET MALWARE OSX/OceanLotus / ELF/RotaJakario CnC Checkin
- [x] ET MALWARE Win32/Parite.B Checkin 3
- [x] ET MALWARE Formbook 0.3 Checkin
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected (Locky C2)
- [x] ET MALWARE ABUSE.CH Ransomware/Cerber Onion Domain Lookup
- [x] ET MALWARE Tinba Banker CnC Response
- [x] ET MALWARE Quant Loader Download Request
- [x] ET MALWARE Possible Winnti-related DNS Lookup (vps2java .securitytactics .com)
- [x] ET MALWARE Possible Winnti-related DNS Lookup (resume .immigrantlol .com)
- [x] ET MALWARE Possible Winnti-related DNS Lookup (css .google-statics .com)
- [x] ET MALWARE Win32/Striked Ransomware CnC Checkin
- [x] ET MALWARE Observed Malicious DNS Query (Reyptson Ransomware CnC)
- [x] ET MALWARE CDT Credphish/Netwire Campaign DNS Lookup
- [x] ET MALWARE CDT Credphish/Netwire Campaign DNS Lookup
- [x] ET MALWARE CDT Credphish/Netwire Campaign DNS Lookup
- [x] ET MALWARE CDT Credphish/Netwire Campaign DNS Lookup
- [x] ET MALWARE W32/Emotet CnC Beacon 1
- [ ] ET MALWARE MSIL/OzazaLocker Ransomware CnC Checkin
- [x] ET MALWARE Known Hostile Domain ant.trenz .pl Lookup
- [x] ET MALWARE OSX/Proton.B Domain in SNI
- [x] ET MALWARE Jaff Ransomware Checkin
- [x] ET MALWARE Jaff Ransomware Checkin M1
- [x] ET MALWARE Possible WannaCry DNS Lookup 2
- [x] ET MALWARE Possible WannaCry DNS Lookup 4
- [x] ET MALWARE W32/WannaCry.Ransomware Killswitch Domain HTTP Request 1
- [x] ET MALWARE W32/WannaCry.Ransomware Killswitch Domain HTTP Request 3
- [ ] ET MALWARE W32/WannaCry.Ransomware Killswitch Domain HTTP Request 5
- [x] ET MALWARE MWI Maldoc Load Payload
- [x] ET MALWARE LokiBot Cryptocurrency Wallet Exfiltration Detected
- [x] ET MALWARE LokiBot Request for C2 Commands Detected M1
- [x] ET MALWARE LokiBot Keylogger Data Exfiltration Detected M1
- [x] ET MALWARE LokiBot Application/Credential Data Exfiltration Detected M2
- [x] ET MALWARE LokiBot Keylogger Data Exfiltration Detected M2
- [x] ET MALWARE Win32/ASPC Bot CnC Checkin M2
- [x] ET MALWARE UIWIX Ransomware .onion Payment Domain (4ujngbdqqm6t2c53)
- [x] ET MALWARE MalDoc Retrieving Payload May 23 2017 2
- [x] ET MALWARE APT32 Komprogo DNS Lookup
- [x] ET MALWARE APT32 Komprogo DNS Lookup
- [x] ET MALWARE Observed GET Request to Jaff Domain (orhangazitur . com)
- [x] ET MALWARE Jaff Ransomware Checkin
- [x] ET MALWARE Win32/Fireball Activity
- [x] ET MALWARE MSIL/Unk.HT-Based Ransomware CnC Checkin
- [x] ET MALWARE PLATINUM Dipsind CnC Beacon
- [x] ET MALWARE X-Malware-Sinkhole Header in HTTP Response
- [x] ET MALWARE DPRK HIDDEN COBRA DDoS Handshake Success
- [x] ET MALWARE Possible Pegasus Related DNS Lookup (secure-access10 .mx)
- [x] ET MALWARE Possible Pegasus Related DNS Lookup (mymensaje-sms .com)
- [x] ET MALWARE Possible Pegasus Related DNS Lookup (ideas-telcel .com.mx)
- [x] ET MALWARE Fake Windows Scam ScreenLocker
- [x] ET MALWARE FF-RAT Stage 1 CnC Checkin
- [x] ET MALWARE x0Proto File Info Request
- [x] ET MALWARE Naoinstalad Checkin
- [ ] ET MALWARE Observed Malicious SSL Cert (HiddenTear Variant CnC)
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected (Locky C2)
- [x] ET MALWARE ABUSE.CH Ransomware/Cerber Onion Domain Lookup
- [ ] ET MALWARE Tinba CnC Checkin
- [x] ET MALWARE Possible Win32/Petya Conn Check
- [x] ET MALWARE MSIL/PSW.Agent.QJK Stealer Data Exfil Via HTTP
- [x] ET MALWARE Possible Winnti-related DNS Lookup (job .yoyakuweb .technology)
- [x] ET MALWARE Possible Winnti-related DNS Lookup (macos .exoticlol .com)
- [x] ET MALWARE LockPOS CnC
- [x] ET MALWARE Observed DNS Query to Known Fenrir Ransomware CnC Domain
- [x] ET MALWARE CDT Credphish/Netwire Campaign DNS Lookup
- [x] ET MALWARE CDT Credphish/Netwire Campaign DNS Lookup
- [x] ET MALWARE CDT Credphish/Netwire Campaign DNS Lookup
- [ ] ET MALWARE CDT Credphish/Netwire Campaign DNS Lookup
- [x] ET MALWARE DarkHotel Downloader CnC Beacon 1

- [x] ET MALWARE DarkHotel Downloader CnC Beacon 2
- [ ] ET MALWARE Shifr Ransomware Malicious Domain in SNI Observed
- [x] ET MALWARE LokiBot Related DNS query
- [x] ET MALWARE HTTP Andromeda File Request
- [x] ET MALWARE Shifr Ransomware CnC DNS Query (ojdue4474qghybjb)
- [x] ET MALWARE CopyKittens Matryoshka DNS Lookup 2 (twiter-statics . info)
- [x] ET MALWARE TDTESS Backdoor User-Agent
- [x] ET MALWARE Revcode RAT CnC
- [x] ET MALWARE ISMAgent CnC Checkin 1
- [x] ET MALWARE ISMAgent DNS Tunneling (microsoft-publisher . com)
- [x] ET MALWARE Nemucod JS Downloader Aug 01 2017
- [x] ET MALWARE [PTsecurity] Win32/TinyNuke Payload ACF40 Inbound
- [x] ET MALWARE CryptON/Nemesis/X3M Ransomware Onion Domain
- [x] ET MALWARE CryptON/Nemesis/X3M Ransomware Onion Domain
- [x] ET MALWARE CryptON/Nemesis/X3M Ransomware Onion Domain
- [x] ET MALWARE CryptON/Nemesis/X3M Ransomware Onion Domain
- [x] ET MALWARE CryptON/Nemesis/X3M Ransomware Onion Domain
- [x] ET MALWARE OSX/Mughthesec/SafeFinder/OperatorMac DNS Query Observed
- [x] ET MALWARE MSIL/CoalaBot CnC Activity
- [x] ET MALWARE Possible AMSI Powershell Bypass Attempt B641
- [x] ET MALWARE Possible AMSI Powershell Bypass Attempt B643
- [x] ET MALWARE Possible Veil Powershell Encoder B641
- [x] ET MALWARE Possible Veil Powershell Encoder B643
- [x] ET MALWARE Windows Scriptlet Invoking Powershell Likely Malicious
- [x] ET MALWARE Likely Malicious Windows SCT Download MSXMLHTTP M2
- [x] ET MALWARE Likely Malicious Windows SCT Download MSXMLHTTP AX
- [x] ET MALWARE DNS Query for known ShadowPad CnC 2
- [x] ET MALWARE DNS Query for known ShadowPad CnC 4
- [x] ET MALWARE DNS Query for known ShadowPad CnC 6
- [x] ET MALWARE DNS Query for known ShadowPad CnC 8
- [x] ET MALWARE DNS Query for known ShadowPad CnC 10
- [x] ET MALWARE Possible Maldoc Downloader Aug 18 2017
- [x] ET MALWARE Likely Malicious Windows SCT Download MSXMLHTTP AX M2
- [ ] ET MALWARE Hancitor/Tordal Document Request
- [x] ET MALWARE APT12 THREEBYTE DNS Lookup
- [x] ET MALWARE Win32/ASPC Bot CnC Checkin M3
- [x] ET MALWARE DeepEnd Research Ransomware Domain Detected
- [x] ET MALWARE DeepEnd Research Ransomware Domain Detected
- [x] ET MALWARE DeepEnd Research Ransomware Domain Detected
- [x] ET MALWARE DeepEnd Research Ransomware Domain Detected
- [x] ET MALWARE ABUSE.CH Cerber Ransomware Domain Detected
- [x] ET MALWARE Gazer HTTP POST Checkin
- [x] ET MALWARE Gazer DNS query observed (mydreamhoroscope . com)
- [x] ET MALWARE CobianRAT Receiving Commands From CnC
- [x] ET MALWARE CobianRAT Receiving Config Commands from CnC
- [ ] ET MALWARE KHRAT DNS Lookup (upload-dropbox .com)
- [x] ET MALWARE ApolloLocker Ransomware CnC Checkin
- [x] ET MALWARE Possible Locky VB/JS Loader Download Sep 08 2017
- [x] ET MALWARE ABUSE.CH Zloader CnC Domain Detected
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Adwind)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (ZeusPanda MITM)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (ZeusPanda MITM)
- [ ] ET MALWARE Observed Malicious Domain SSL Cert in SNI (RansomBlocker CnC)
- [x] ET MALWARE LokiBot Related DNS query
- [ ] ET MALWARE Win32/Bitshifter Ransomware CnC Checkin
- [x] ET MALWARE Shifr Ransomware CnC DNS Query (v5t5z6a55ksmt3oh)
- [x] ET MALWARE CopyKittens Matryoshka DNS Lookup 1 (winupdate64 . com)
- [x] ET MALWARE CopyKittens Cobalt Strike DNS Lookup (cloudflare-analyse . com)
- [x] ET MALWARE Win32/BanloadDownloader.XZY Retrieving Payload
- [x] ET MALWARE Revcode RAT CnC 2
- [x] ET MALWARE ISMAgent Receiving Commands from CnC Server
- [x] ET MALWARE Observed DNS Query to Reborn/Ovidiy Stealer CnC Domain
- [ ] ET MALWARE Observed Malicious Domain SSL Cert in SNI (JS_POWMET)
- [x] ET MALWARE CryptON/Nemesis/X3M Ransomware Onion Domain
- [x] ET MALWARE CryptON/Nemesis/X3M Ransomware Onion Domain
- [x] ET MALWARE CryptON/Nemesis/X3M Ransomware Onion Domain
- [x] ET MALWARE CryptON/Nemesis/X3M Ransomware Onion Domain
- [x] ET MALWARE CryptON/Nemesis/X3M Ransomware Onion Domain
- [x] ET MALWARE MSIL/Agent.ATS CnC Activity
- [x] ET MALWARE OSX/Mughthesec/SafeFinder/OperatorMac Rogue Search Engine DNS Query Observed
- [x] ET MALWARE [PTsecurity] Gozi/Ursnif Payload v12
- [x] ET MALWARE Possible AMSI Powershell Bypass Attempt B642
- [x] ET MALWARE Possible AMSI Powershell Bypass Attempt
- [x] ET MALWARE Possible Veil Powershell Encoder B642
- [x] ET MALWARE Observed DNS Query to Gryphon CnC Domain / GlobeImposter Payment Domain
- [x] ET MALWARE Likely Malicious Windows SCT Download MSXMLHTTP M1
- [x] ET MALWARE Likely Malicious Windows SCT Download MSXMLHTTP M3
- [x] ET MALWARE DNS Query for known ShadowPad CnC 1
- [x] ET MALWARE DNS Query for known ShadowPad CnC 3
- [x] ET MALWARE DNS Query for known ShadowPad CnC 5
- [x] ET MALWARE DNS Query for known ShadowPad CnC 7
- [x] ET MALWARE DNS Query for known ShadowPad CnC 9
- [x] ET MALWARE DNS Query for known ShadowPad CnC 11
- [x] ET MALWARE Win32/Datper CnC Activity
- [x] ET MALWARE Spora Ransomware DNS Query
- [ ] ET MALWARE OSX.Pwnet.A Certificate Observed
- [x] ET MALWARE ISMAgent DNS Lookup (msoffice-cdn . com)
- [x] ET MALWARE DeepEnd Research Ransomware Domain Detected
- [x] ET MALWARE DeepEnd Research Ransomware Domain Detected
- [x] ET MALWARE DeepEnd Research Ransomware Domain Detected
- [x] ET MALWARE DeepEnd Research Ransomware Domain Detected
- [x] ET MALWARE DeepEnd Research Ransomware Domain Detected
- [x] ET MALWARE ABUSE.CH Cerber Ransomware Domain Detected
- [x] ET MALWARE Gazer DNS query observed (soligro . com)
- [x] ET MALWARE CobianRAT Checkin to CnC
- [x] ET MALWARE CobianRAT Receiving Additional Commands From CnC
- [x] ET MALWARE CobianRAT Screenshot Exfil to CnC
- [x] ET MALWARE [PTsecurity] Tinba Checkin 4
- [x] ET MALWARE ApolloLocker Ransomware CnC Checkin 2
- [ ] ET MALWARE Win32/Unk.Bot CnC Checkin
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (URLzone)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (ZeusPanda MITM)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (ZeusPanda MITM)
- [ ] ET MALWARE ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (ZeusPanda MITM)

- [x] ET MALWARE Win32/Kryptik.FVVZ Variant CnC Checkin 2
- [ ] ET MALWARE [PTsecurity] pkt checker 0
- [ ] ET MALWARE [PTsecurity] pkt checker 1
- [ ] ET MALWARE [PTsecurity] pkt checker 2
- [ ] ET MALWARE [PTsecurity] pkt checker 3
- [ ] ET MALWARE [PTsecurity] Backdoor.Win32/Remcos RAT pkt checker 4
- [x] ET MALWARE [PTsecurity] JS.Trojan-Downloader.Nemucod.yo HTTP POST (:Exec:)
- [x] ET MALWARE CCleaner Backdoor DGA Domain (ab6d54340c1a .com) Feb 2017
- [x] ET MALWARE CCleaner Backdoor DGA Domain (aba9a949bc1d .com) Mar 2017
- [x] ET MALWARE CCleaner Backdoor DGA Domain (ab2da3d400c20 .com) Apr 2017
- [x] ET MALWARE CCleaner Backdoor DGA Domain (ab3520430c23 .com) May 2017
- [x] ET MALWARE CCleaner Backdoor DGA Domain (ab1c403220c27 .com) Jun 2017
- [x] ET MALWARE CCleaner Backdoor DGA Domain (ab1abad1d0c2a .com) Jul 2017
- [x] ET MALWARE CCleaner Backdoor DGA Domain (ab8cee60c2d .com) Aug 2017
- [x] ET MALWARE CCleaner Backdoor DGA Domain (ab1145b758c30 .com) Sep 2017
- [x] ET MALWARE CCleaner Backdoor DGA Domain (ab890e964c34 .com) Oct 2017
- [x] ET MALWARE CCleaner Backdoor DGA Domain (ab3d685a0c37 .com) Nov 2017
- [x] ET MALWARE CCleaner Backdoor DGA Domain (ab70a139cc3a.com) Dec 2017
- [ ] ET MALWARE Lucifer Loader Requesting Payload
- [x] ET MALWARE ABUSE.CH Ransomware Domain Detected
- [x] ET MALWARE DNS Query For TURNEDUP.Backdoor CnC (chromup)
- [x] ET MALWARE DNS Query For TURNEDUP.Backdoor CnC (securityupdated)
- [x] ET MALWARE DNS Query For TURNEDUP.Backdoor CnC (googlmail)
- [x] ET MALWARE DNS Query For TURNEDUP.Backdoor / NanoCore CnC (microsoftupdated)
- [x] ET MALWARE DNS Query For TURNEDUP.Backdoor CnC (syn.broadcaster)
- [ ] ET MALWARE [PTsecurity] Backdoor.Java.Adwind.cu Certificate flowbit set 1
- [ ] ET MALWARE [PTsecurity] Backdoor.Java.Adwind.cu pkt Checker flowbit set 2
- [ ] ET MALWARE [PTsecurity] Backdoor.Java.Adwind.cu pkt Checker flowbit set 3
- [ ] ET MALWARE [PTsecurity] Backdoor.Java.Adwind.cu pkt Checker flowbit set 4
- [ ] ET MALWARE [PTsecurity] Backdoor.Java.Adwind.cu pkt Checker flowbit set 5
- [ ] ET MALWARE [PTsecurity] Backdoor.Java.Adwind.cu
- [ ] ET MALWARE Observed Malicious SSL Cert (MalDoc DL)
- [x] ET MALWARE Win32/Scarsi Variant CnC Activity
- [x] ET MALWARE [PTsecurity] Possible Cobalt Strike payload
- [ ] ET MALWARE [PTsecurity] Malicious SSL connection (Upatre Downloader CnC) cert
- [ ] ET MALWARE [PTsecurity] Malicious SSL connection (Upatre Downloader CnC) 0
- [ ] ET MALWARE [PTsecurity] Malicious SSL connection (Upatre Downloader CnC) 1
- [ ] ET MALWARE [PTsecurity] Malicious SSL connection (Upatre Downloader CnC) 2
- [ ] ET MALWARE [PTsecurity] Malicious SSL connection (Upatre Downloader CnC) 3
- [ ] ET MALWARE [PTsecurity] Malicious SSL connection (Upatre Downloader CnC) 4
- [ ] ET MALWARE [PTsecurity] Malicious SSL connection (Upatre Downloader CnC) 5
- [x] ET MALWARE [PTsecurity] TR/Spy.Banker.agdtw Checkin
- [x] ET MALWARE Win32/Formgrabber Data Exfil
- [ ] ET MALWARE [PTsecurity] Black Stealer Exfil System Info
- [x] ET MALWARE [PTsecurity] Black Stealer Exfil FTP STOR
- [x] ET MALWARE Lazarus Decafett DNS Lookup 1
- [x] ET MALWARE Lazarus Decafett DNS Lookup 2
- [x] ET MALWARE Lazarus Decafett DNS Lookup 3
- [x] ET MALWARE Lazarus Decafett DNS Lookup 4
- [ ] ET MALWARE CCleaner Backdoor DGA Domain (ab3c2b0d28ba6 .com) Jan 2018
- [ ] ET MALWARE CCleaner Backdoor DGA Domain (ab99c24c0ba9 .com) Feb 2018
- [ ] ET MALWARE CCleaner Backdoor DGA Domain (ab2e1b782bad .com) Mar 2018
- [ ] ET MALWARE CCleaner Backdoor DGA Domain (ab253af862bb0 .com) Apr 2018
- [ ] ET MALWARE CCleaner Backdoor DGA Domain (ab2d02b02bb3 .com) May 2018
- [ ] ET MALWARE CCleaner Backdoor DGA Domain (ab1b0eaa24bb6 .com) Jun 2018
- [ ] ET MALWARE CCleaner Backdoor DGA Domain (abf09fc5abba .com) Jul 2018
- [ ] ET MALWARE CCleaner Backdoor DGA Domain (abce85a51bbd .com) Aug 2018
- [ ] ET MALWARE CCleaner Backdoor DGA Domain (abccc097dbc0.com) Sep 2018
- [ ] ET MALWARE CCleaner Backdoor DGA Domain (ab33b8aa69bc4 .com) Oct 2018
- [ ] ET MALWARE CCleaner Backdoor DGA Domain (ab693f4c0bc7 .com) Nov 2018
- [ ] ET MALWARE CCleaner Backdoor DGA Domain (ab23660730bca .com) Dec 2018
- [x] ET MALWARE [PTsecurity] Ursnif Encoded Payload Inbound
- [x] ET MALWARE DNSMessenger Payload (TXT base64 gzip header)
- [x] ET MALWARE Trojan.JS.Agent.dwz Checkin
- [x] ET MALWARE [PTsecurity] Trojan.JS.Agent.dwz Checkin 1
- [x] ET MALWARE Possible Winnti-related Destination
- [ ] ET MALWARE Possible Winnti-related DNS Lookup
- [x] ET MALWARE Possible Winnti-related Destination
- [x] ET MALWARE Possible Winnti-related DNS Lookup
- [x] ET MALWARE Possible Winnti-related Destination
- [x] ET MALWARE Possible Winnti-related DNS Lookup
- [x] ET MALWARE Possible Winnti-related Destination
- [x] ET MALWARE Possible Winnti-related DNS Lookup
- [x] ET MALWARE Possible Winnti-related Destination
- [x] ET MALWARE Possible Winnti-related DNS Lookup
- [x] ET MALWARE Possible Winnti-related Destination
- [ ] ET MALWARE Possible Winnti-related Destination
- [x] ET MALWARE Possible Winnti-related DNS Lookup
- [x] ET MALWARE Possible Winnti-related Destination
- [x] ET MALWARE Possible Winnti-related DNS Lookup
- [x] ET MALWARE Possible Winnti-related Destination
- [x] ET MALWARE Possible Winnti-related DNS Lookup
- [x] ET MALWARE Possible Winnti-related Destination
- [x] ET MALWARE Possible Winnti-related DNS Lookup
- [x] ET MALWARE Possible Winnti-related DNS Lookup (google-statics .com)
- [x] ET MALWARE Possible Winnti-related DNS Lookup (google-searching .com)
- [x] ET MALWARE Possible Winnti-related DNS Lookup
- [x] ET MALWARE Possible Winnti-related DNS Lookup

- [x] ET MALWARE Possible Winnti-related Destination (google-searching .com)
- [x] ET MALWARE Possible Winnti-related Destination
- [x] ET MALWARE OSX/Proton.C/D Domain (eltima .in in TLS SNI)
- [x] ET MALWARE OSX/Proton.C/D Domain (handbrakestore .com in TLS SNI)
- [x] ET MALWARE OSX/Proton.C/D Domain (handbrake .cc) in TLS SNI
- [x] ET MALWARE Possible Dragonfly APT Activity - SMB credential harvesting
- [x] ET MALWARE Locky Intermediate Downloader
- [ ] ET MALWARE Observed Malicious SSL Cert (Snatch CnC)
- [x] ET MALWARE BadRabbit Ransomware Activity Via WebDAV (cscc)
- [x] ET MALWARE Qtloader encrypted check-in Oct 19 M1
- [x] ET MALWARE IoT_reaper DNS Lookup M1 (hl852 .com)
- [x] ET MALWARE IoT_reaper DNS Lookup M3 (hi8529 .com)
- [x] ET MALWARE Possible IoT_reaper ELF Binary Request M2 (set)
- [x] ET MALWARE Possible IoT_reaper ELF Binary Request M4 (set)
- [x] ET MALWARE Possible IoT_reaper ELF Binary Download
- [x] ET MALWARE IoT_reaper DNS Lookup M4 (cbk99 .com)
- [x] ET MALWARE IoT_reaper DNS Lookup M6 (bbk86 .com)
- [ ] ET MALWARE Downeks/Quasar DNS Lookup (download .data-server .cloudns .club)
- [ ] ET MALWARE Downeks/Quasar DNS Lookup (signup .updatesforme .club)
- [x] ET MALWARE SAD Ransomware CnC Activity
- [x] ET MALWARE RouteX CnC Domain (cba4a6e5d3c956548a337c52388473f1 .com) in DNS Lookup
- [x] ET MALWARE RouteX CnC Domain (73780fbd309561e201a4aee9914d882d .org) in DNS Lookup
- [x] ET MALWARE RouteX CnC Domain (322ffbbc7c1b312c2f9d942f20422f8d .com) in DNS Lookup
- [x] ET MALWARE RouteX CnC Domain (aaafc94b3a37b75ae9cb60afc42e86fe .org) in DNS Lookup
- [x] ET MALWARE RouteX CnC Domain (2fa3c2fa16c47d9b9bff8986a42b048f .com) in DNS Lookup
- [x] ET MALWARE Volex - OceanLotus JavaScript Load (connect.js)
- [x] ET MALWARE Volex - OceanLotus System Profiling JavaScript (linkStorage.x00SOCKET)
- [x] ET MALWARE DeepEnd Research Ransomware CrypMIC Payment Onion Domain
- [x] ET MALWARE DeepEnd Research Ransomware CrypMIC Payment Onion Domain
- [ ] ET MALWARE SunOrcal Reaver Domain Observed (tashdqdxp .com) in DNS Lookup
- [ ] ET MALWARE SunOrcal Reaver Domain Observed (fyoutside .com) in DNS Lookup
- [x] ET MALWARE Lazarus FALLCHILL Fake SSL Checkin 1
- [x] ET MALWARE Lazarus FALLCHILL Fake SSL Checkin 2
- [x] ET MALWARE Powershell commands sent B64 1
- [x] ET MALWARE Powershell commands sent B64 3
- [x] ET MALWARE Win32/Nivdort Checkin
- [x] ET MALWARE Netwire RAT Check-in 2
- [x] ET MALWARE Win32/Ropest.H CnC - INBOUND set
- [x] ET MALWARE Win32/Atraps Receiving Config via Image File (steganography)
- [x] ET MALWARE Patchwork Domain (randreports .org in DNS Lookup)
- [x] ET MALWARE Brazilian Banker SSL Cert
- [x] ET MALWARE [PTsecurity] Bladabindi/njRAT (Dd19271927)
- [x] ET MALWARE Mirai Variant Domain (blacklister .nl in DNS Lookup)
- [x] ET MALWARE Vawtrak/NeverQuest Posting Data
- [x] ET MALWARE Vawtrak/NeverQuest CnC Beacon
- [x] ET MALWARE Observed SluttyPutty Maldoc User-Agent
- [x] ET MALWARE Possible Winnti-related Destination
- [x] ET MALWARE OSX/Proton.C/D Domain (eltima .in) in DNS Lookup
- [x] ET MALWARE OSX/Proton.C/D Domain (handbrakestore .com) in DNS Lookup
- [x] ET MALWARE OSX/Proton.C/D Domain (handbrake .cc) in DNS Lookup
- [x] ET MALWARE Dragonfly Backdoor.Goodor Go Implant CnC Beacon 1
- [x] ET MALWARE Possible Dragonfly APT Activity HTTP URI OPTIONS
- [x] ET MALWARE Trickbot Payload Request
- [ ] ET MALWARE Observed Malicious SSL Cert (Snatch CnC)
- [x] ET MALWARE BadRabbit Ransomware Activity Via WebDAV (infpub)
- [ ] ET MALWARE BadRabbit Ransomware Payment Onion Domain
- [x] ET MALWARE IoT_reaper DNS Lookup M2 (hl859 .com)
- [x] ET MALWARE Possible IoT_reaper ELF Binary Request M1 (set)
- [x] ET MALWARE Possible IoT_reaper ELF Binary Request M3 (set)
- [x] ET MALWARE Possible IoT_reaper ELF Binary Request M5 (set)
- [x] ET MALWARE Possible BACKSWING JS Framework POST Observed
- [x] ET MALWARE IoT_reaper DNS Lookup M5 (bbk80 .com)
- [x] ET MALWARE IoT_reaper DNS Lookup M7 (ha859 .com)
- [ ] ET MALWARE Downeks/Quasar DNS Lookup (ping .topsite .life)
- [ ] ET MALWARE Downeks/Quasar DNS Lookup (moreoffer .life)
- [x] ET MALWARE [PTsecurity] Win32/Randrew!rfn CnC Activity
- [x] ET MALWARE RouteX CnC Domain (0a0074066c49886a39b5a3072582f5d6 .net) in DNS Lookup
- [x] ET MALWARE RouteX CnC Domain (dcb5684707f6c66492aaa9f7d9bfb5a6 .biz) in DNS Lookup
- [x] ET MALWARE RouteX CnC Domain (18bca7c5fd709ac468ba148c590ef6bf .net) in DNS Lookup
- [x] ET MALWARE RouteX CnC Domain (c13a856f4a879a89e9a638207efd6c94 .biz) in DNS Lookup
- [x] ET MALWARE RouteX CnC Domain (3ec9b600789b3bacf2c72ebae142a9c3 .net) in DNS Lookup
- [x] ET MALWARE Volex - OceanLotus JavaScript Fake Page URL Builder Response
- [x] ET MALWARE OceanLotus System Profiling JavaScript HTTP Request
- [x] ET MALWARE DeepEnd Research Ransomware CrypMIC Payment Onion Domain
- [x] ET MALWARE Win32/RCAP CnC Checkin
- [ ] ET MALWARE SunOrcal Reaver Domain Observed (weryhstui .com) in DNS Lookup
- [ ] ET MALWARE SunOrcal Reaver Domain Observed (olinaodi .com) in DNS Lookup
- [x] ET MALWARE Win32/TinyNuke CnC Checkin
- [x] ET MALWARE Powershell commands sent when remote host claims to send an image
- [x] ET MALWARE Powershell commands sent B64 2
- [ ] ET MALWARE Possible NanoCore C2 60B
- [x] ET MALWARE Netwire RAT Check-in 2
- [x] ET MALWARE Backdoor.Perl.Shellbot.cd IRC Bot that have DoS/DDoS functions
- [x] ET MALWARE Win32/Ropest.H CnC - INBOUND
- [x] ET MALWARE Patchwork DNS Tunneling (nsn1.winodwsupdates .me)
- [x] ET MALWARE [PTsecurity] Bladabindi/njRAT (HAMAD versions)
- [ ] ET MALWARE Brazilian Banker SSL Cert
- [x] ET MALWARE Mirai Variant Domain (bigboatreps .pw in DNS Lookup)
- [x] ET MALWARE Patchwork Domain (rannd .org in DNS Lookup)
- [x] ET MALWARE Vawtrak/NeverQuest Posting Data
- [x] ET MALWARE UBoatRAT CnC Check-in
- [x] ET MALWARE Sharik/Smoke CnC Beacon 7

- [x] ET MALWARE Possible Sharik/Smoke Loader Microsoft Connectivity check
- [x] ET MALWARE [PTsecurity] Botnet Nitol.B Checkin
- [x] ET MALWARE Injected WP Keylogger/Coinminer Domain Detected (cloudflare .solutions in DNS Lookup)
- [x] ET MALWARE MSIL/NxRansomware C2 Domain Detected (0cf5ff34 .ngrok .io in DNS Lookup)
- [x] ET MALWARE Win32/Backdoor.Randrew.A CnC Checkin
- [x] ET MALWARE Win32/Bot.Sezin CnC Checkin
- [x] ET MALWARE [PTsecurity] DorkBot.Downloader CnC Beacon
- [ ] ET MALWARE Possible Trickbot/Dyre Serial Number in SSL Cert
- [ ] ET MALWARE Windows executable sent when remote host claims to send an image M4
- [x] ET MALWARE W32/Patchwork.Backdoor CnC Check-in M2
- [x] ET MALWARE WooSIP Downloader CnC DeleteFileOnServer
- [x] ET MALWARE Smurf2 CnC Checkin
- [x] ET MALWARE Win32/Backdoor.Agent.qweydh CnC Checkin M1
- [x] ET MALWARE Win32/Backdoor.Agent.qweydh CnC Activity
- [x] ET MALWARE Sharik/Smoke CnC Beacon 9
- [x] ET MALWARE Oilrig Stealer CnC Checkin
- [ ] ET MALWARE MedusaHTTP CnC Checkin
- [x] ET MALWARE OSX/Mami CnC Checkin
- [x] ET MALWARE Observed Evrial Domain (cryptoclipper .ru in TLS SNI)
- [x] ET MALWARE [PTsecurity] Possible Trojan.Downloader UserAgent (binary_getter)
- [x] ET MALWARE [PTsecurity] Gozi/Ursnif Payload v14
- [x] ET MALWARE Malicious Chrome Extension Domain Request (change-request .info in DNS Lookup)
- [x] ET MALWARE Malicious Chrome Extension Click Fraud Activity via Websocket
- [x] ET MALWARE Win32.Drun Checkin
- [x] ET MALWARE VBS.ARS Checkin
- [x] ET MALWARE MSIL/SamMiner CnC Checkin M1
- [x] ET MALWARE Banload CnC Activity
- [x] ET MALWARE W32/SchwSonne CnC Beacon M2
- [x] ET MALWARE Win32/GandCrab Ransomware CnC Activity
- [x] ET MALWARE Observed Evrial Domain (projectevrial .ru in TLS SNI)
- [x] ET MALWARE Trojan-Dropper.Delf Checkin
- [x] ET MALWARE Operation EvilTraffic Initial Redirect M2
- [x] ET MALWARE Backdoor.Elise CnC Beacon 2 M2
- [x] ET MALWARE [Flashpoint] Possible CVE-2018-4878 Check-in
- [x] ET MALWARE W32/SPARS/ARS Stealer Checkin
- [x] ET MALWARE MSIL/Agent.BIC Variant CnC Checkin
- [x] ET MALWARE Evrial Stealer CnC Activity M2
- [x] ET MALWARE Known Malicious Redirector in DNS Lookup (vip.rm028 .cn)
- [x] ET MALWARE Mirai/OMG Proxy Variant CnC in DNS Lookup (ccnew.mm .my)
- [x] ET MALWARE SteamStealer DNS Lookup (steamdesktopauthenticator)
- [ ] ET MALWARE SteamStealer Malicious SSL Certificate Detected
- [x] ET MALWARE SteamStealer DNS Lookup (steamdesktop)
- [x] ET MALWARE QRat.Java.RAT Checkin Response
- [x] ET MALWARE Observed Princess Ransomware Payment Domain (royal25fphqilqft in DNS Lookup)
- [x] ET MALWARE Observed GandCrab Ransomware CnC/IP Check Domain (malwarehunterteam .bit in DNS Lookup)
- [x] ET MALWARE Win32/FlawedAmmyy RAT CnC Checkin
- [x] ET MALWARE [PTsecurity] Fake SSL Certificate Observed (Oracle America)
- [x] ET MALWARE MewsSpy.AE Onion Domain (cxkefbwo7qcmlelb in DNS Lookup)
- [x] ET MALWARE njRAT/Bladabindi Variant (Lime) CnC Checkin
- [x] ET MALWARE Sharik/Smoke CnC Beacon 8
- [x] ET MALWARE GratefulPOS Covert DNS CnC Initial Checkin
- [ ] ET MALWARE Win32/Downloader.Small.BIL CnC Checkin
- [x] ET MALWARE [PTsecurity] DorkBot.Downloader CnC Response
- [ ] ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TrickBot CnC)
- [x] ET MALWARE Win32/Backdoor.YesMaster CnC Checkin
- [x] ET MALWARE W32/Patchwork.Backdoor Communicating with CnC
- [x] ET MALWARE WooSIP Downloader CnC CreateFolderOnServer
- [x] ET MALWARE WooSIP Downloader CnC WriteMetadataOnServer
- [x] ET MALWARE Windows Executable Downloaded With Image Content-Type Header
- [ ] ET MALWARE Win32/Backdoor.Agent.qweydh CnC Checkin M2
- [x] ET MALWARE Zeus Panda CnC Domain (in DNS Lookup)
- [x] ET MALWARE Qasar Variant Domain (datapeople-cn .com in DNS Lookup)
- [x] ET MALWARE Python Monero Miner CnC DNS Query
- [x] ET MALWARE Bitter RAT HTTP CnC Beacon M2
- [x] ET MALWARE OSX/Mami Possible DNS Query to Evil DNS Server
- [x] ET MALWARE [PTsecurity] Trojan.Downloader VBA Script obfuscation (binary_getter)
- [x] ET MALWARE MoneroPay Ransomware Payment Activity
- [x] ET MALWARE [PTsecurity] Adwind SSL Certificate Observed
- [x] ET MALWARE Malicious Chrome Extension Requesting Websocket
- [x] ET MALWARE RocketMan Win32/Drun
- [x] ET MALWARE Observed Evrial Domain (projectevrial .ru in DNS Lookup)
- [x] ET MALWARE Win32/Rodecap/Travle/PYLOT CnC Checkin M2
- [x] ET MALWARE MSIL/SamMiner CnC Checkin M2
- [x] ET MALWARE ELF/TooEasy Miner CnC Checkin
- [x] ET MALWARE [PTsecurity] Kuriyama Loader Checkin
- [x] ET MALWARE Observed Evrial Domain (cryptoclipper .ru in DNS Lookup)
- [x] ET MALWARE Evrial Stealer CnC Activity
- [x] ET MALWARE Operation EvilTraffic Initial Redirect M1
- [x] ET MALWARE Backdoor.Elise Style IP Check
- [x] ET MALWARE Observed ExecPS/Cobolt Domain (getfreshnews .com in DNS Lookup)
- [x] ET MALWARE Shurl0ckr Ransomware CnC (kdvm5fd6tn6jsbwh .onion .to in DNS Lookup)
- [x] ET MALWARE Evrial Stealer Retrieving CnC Information
- [ ] ET MALWARE Win32/Backdoor.Small.ao CnC Checkin
- [x] ET MALWARE LokiBot Checkin
- [x] ET MALWARE Known Malicious Redirector in DNS Lookup (by007 .cn)
- [x] ET MALWARE Mirai/OMG Proxy Variant CnC in DNS Lookup (rpnew.mm .my)
- [ ] ET MALWARE SteamStealer Domain in SNI
- [x] ET MALWARE SteamStealer DNS Lookup (lightalex)
- [x] ET MALWARE [PTsecurity] QRat.Java.RAT (state_alive)
- [x] ET MALWARE QRat.Java.RAT Post-Checkin Request
- [x] ET MALWARE Observed GandCrab Ransomware CnC/IP Check Domain (politiaromana .bit in DNS Lookup)
- [x] ET MALWARE Observed GandCrab Ransomware CnC/IP Check Domain (gdcb .bit in DNS Lookup)
- [x] ET MALWARE [PTsecurity] Fake SSL Certificate Observed (Yahoo)
- [x] ET MALWARE [PTsecurity] Fake SSL Certificate Observed (Google)

- [x] ET MALWARE [PTsecurity] Fake SSL Certificate Observed (Oracle canada)
- [x] ET MALWARE Arkei Stealer IP Lookup
- [x] ET MALWARE Vidar/Arkei Stealer Client Data Upload
- [x] ET MALWARE Observed Sofacy CnC Domain (ndpmedia24 .com in DNS Lookup)
- [x] ET MALWARE Possible Sharik/Smoke Loader Microsoft Connectivity check M2
- [x] ET MALWARE Sharik/Smoke CnC Beacon 10
- [ ] ET MALWARE [PTsecurity] Ursnif Socks5 Proxy Connection
- [x] ET MALWARE Observed GandCrab Ransomware Domain (zonealarm .bit in DNS Lookup)
- [x] ET MALWARE Win32/GandCrab Ransomware CnC Activity M2
- [ ] ET MALWARE [PTsecurity] Win32/SocStealer.Socelars C2 Response
- [x] ET MALWARE Win32/InnaputRAT CnC DNS Lookup (ajdhsfhiudsfhsi .top)
- [x] ET MALWARE OSX/OceanLotus.D Requesting Commands from CnC
- [x] ET MALWARE OSX/OceanLotus.D CnC DNS Lookup (s3 .hiahornber .com)
- [ ] ET MALWARE Win32/DanijBot User-Agent
- [x] ET MALWARE Win32/DanijBot CnC Task Status
- [x] ET MALWARE Pontoeb CnC
- [x] ET MALWARE Iron/Maktub Locker Ransomware CnC Checkin
- [x] ET MALWARE [PTsecurity] Trojan.JS.Agent.dwz Checkin 2
- [x] ET MALWARE MSIL/G1 Stealer/GravityRAT Requesting Payload
- [ ] ET MALWARE MSIL/GX Stealer/GravityRAT Uploading File
- [x] ET MALWARE MSIL/GravityRAT CnC Domain (msoftupdates .eu in DNS Lookup)
- [x] ET MALWARE Observed GandCrab Ransomware Domain (carder .bit in DNS Lookup)
- [x] ET MALWARE Likely GandCrab Ransomware Domain in HTTP Host M2
- [x] ET MALWARE RedLeaves HOGFISH APT Implant CnC
- [x] ET MALWARE BKransomware Domain (3whyfziey2vr41yq in DNS Lookup)
- [x] ET MALWARE ELF/Muhstik Attempting to Download Payload
- [ ] ET MALWARE InfoBot Sending LAN Details
- [x] ET MALWARE Win32/Vibem.C CnC Activity
- [x] ET MALWARE Known Sinkhole Response Header INetSim
- [x] ET MALWARE [PTsecurity] Donut Ransomware CnC Checkin
- [x] ET MALWARE BackSwap Trojan C2 Domain Observed (debasuin .nl in TLS SNI)
- [x] ET MALWARE Win32/Autophyte.F C2 Domain (tpddata .com in DNS Lookup)
- [x] ET MALWARE Win32/Autophyte.F C2 Domain (www .anlway .com in DNS Lookup)
- [x] ET MALWARE Win32/Autophyte.F C2 Domain (www .ap8898 .com in DNS Lookup)
- [x] ET MALWARE Win32/Autophyte.F C2 Domain (www .apshenyihl .com in DNS Lookup)
- [x] ET MALWARE [eSentire] VBS Retrieving Malicious Payload
- [x] ET MALWARE [PTsecurity] Win32/SpyAgent.Raptor (realtime-spy) CnC activity 1
- [x] ET MALWARE [eSentire] Cobalt Strike Beacon
- [x] ET MALWARE Remcos RAT Checkin 23
- [x] ET MALWARE Possible Metasploit Payload Common Construct Bind_API (from server)
- [x] ET MALWARE [eSentire] Win32/Spy.Banker.ADIO CnC Checkin
- [x] ET MALWARE JS Sniffer Framework Sending to CnC
- [x] ET MALWARE OilRig QUADAGENT CnC Domain in SNI
- [x] ET MALWARE OilRig QUADAGENT DNS Tunneling
- [ ] ET MALWARE StrongPity APT SSL Certificate Detected
- [x] ET MALWARE Arkei Stealer Config Download Request
- [x] ET MALWARE Observed Malicious SSL Cert (Bancos Variant CnC)
- [ ] ET MALWARE Cobalt Group SSL Certificate Detected
- [x] ET MALWARE Possible Sharik/Smoke Loader Microsoft Connectivity check M3
- [ ] ET MALWARE [PTsecurity] Ursnif Socks Proxy Check-in
- [x] ET MALWARE Observed GandCrab Ransomware Domain (ransomware .bit in DNS Lookup)
- [x] ET MALWARE Observed GandCrab Ransomware Domain (chlenaverasiskihe .sex in DNS Lookup)
- [x] ET MALWARE [PTsecurity] W32/Rodecap.StealRat C2 Payload (GIF)
- [x] ET MALWARE Win32/InnaputRAT CnC DNS Lookup (ninjagames .top)
- [x] ET MALWARE OSX/OceanLotus.D Sending Data to CnC
- [x] ET MALWARE OSX/OceanLotus.D CnC DNS Lookup (ssl .arkouthrie .com)
- [x] ET MALWARE OSX/OceanLotus.D CnC DNS Lookup (widget .shoreoa .com)
- [x] ET MALWARE Win32/DanijBot CnC Checkin
- [x] ET MALWARE LokiBot Fake 404 Response
- [x] ET MALWARE Observed Malicious SSL Cert (CoreBot C2)
- [x] ET MALWARE Observed GandCrab Payment Domain (gandcrab in DNS Lookup)
- [x] ET MALWARE MSIL/G1 Stealer/GravityRAT Uploading File
- [x] ET MALWARE MSIL/G2 Stealer/GravityRAT CnC Checkin
- [x] ET MALWARE MSIL/GravityRAT CnC Domain (msoftupdates .com in DNS Lookup)
- [x] ET MALWARE MSIL/GravityRAT CnC Domain (mylogisoft .com in DNS Lookup)
- [x] ET MALWARE Likely GandCrab Ransomware Domain in HTTP Host M1
- [x] ET MALWARE Java/QRat Variant Checkin
- [x] ET MALWARE [PTsecurity] Possible Malicious (HTA-VBS-PowerShell) obfuscated command
- [x] ET MALWARE Iron Ransomware Domain (y5mogzal2w25p6bn .ml in DNS Lookup)
- [x] ET MALWARE InfoBot Sending Machine Details
- [x] ET MALWARE Win32/Rarog Stealer CnC Keep-Alive
- [x] ET MALWARE [PTsecurity] PS/TrojanDownloader.Agent.NNR XORed Zip payload (key 0x91)
- [x] ET MALWARE Aurora/OneKeyLocker Ransomware CnC Checkin
- [x] ET MALWARE BackSwap Trojan C2 Domain Observed (debasuin .nl in DNS Lookup)
- [x] ET MALWARE Win32/AutoIt.NU Miner Dropper CnC Checkin
- [x] ET MALWARE Win32/Autophyte.F C2 Domain (tpddata .com in TLS SNI)
- [x] ET MALWARE Win32/Autophyte.F C2 Domain (www .anlway .com in TLS SNI)
- [x] ET MALWARE Win32/Autophyte.F C2 Domain (www .ap8898 .com in TLS SNI)
- [x] ET MALWARE Win32/Autophyte.F C2 Domain (www .apshenyihl .com in TLS SNI)
- [ ] ET MALWARE [PTsecurity] Paradise Ransomware Check-in
- [x] ET MALWARE [PTsecurity] Win32/SpyAgent.Raptor (realtime-spy) CnC activity 2
- [x] ET MALWARE Cobalt Strike Exfiltration
- [x] ET MALWARE [eSentire] Win32/GandCrab v4/5 Ransomware CnC Activity
- [x] ET MALWARE [eSentire] Win32/Spy.Banker CnC Command (DOWNLOAD)
- [x] ET MALWARE Rostpay Downloader User-Agent
- [x] ET MALWARE AZORult Variant.4 Checkin M2
- [x] ET MALWARE Observed Malicious SSL Cert (OilRig QUADAGENT CnC)
- [x] ET MALWARE Observed Malicious SSL Cert (MICROPSIA CnC Domain)

- [x] ET MALWARE [eSentire] Remcos RAT Checkin 24
- [x] ET MALWARE Win32/Bisonal RC4 Encrypted 8 Byte Static CnC Checkin
- [x] ET MALWARE Win32/Bisonal DNS Lookup 2
- [x] ET MALWARE Win32/Bisonal DNS Lookup 4
- [x] ET MALWARE Aurora Ransomware CnC Checkin
- [x] ET MALWARE [eSentire] Remcos RAT Checkin 25
- [x] ET MALWARE Lazarus Downloader (JEUSD) CnC Beacon
- [x] ET MALWARE [PTsecurity] Win32/Spy.Agent.PMJ (MICROPSIA)
- [x] ET MALWARE Observed Malicious SSL Cert (Panda Banker Injects)
- [x] ET MALWARE Panda Banker C2 Domain (uiaoduiiej .chimkent .su in TLS SNI)
- [x] ET MALWARE Panda Banker Injects Domain (urimchi3dt4 .website in TLS SNI)
- [x] ET MALWARE [PTsecurity] Tinba (Banking Trojan) Check-in
- [x] ET MALWARE [PTsecurity] MSIL/Biskvit.A Check-in
- [x] ET MALWARE Win32/Remcos RAT Checkin 27
- [x] ET MALWARE Win32/Remcos RAT Checkin 29
- [x] ET MALWARE MSIL/BISKVIT DNS Lookup (bigboss .x24hr .com)
- [x] ET MALWARE [PT MALWARE] Hacked Mikrotik C2 Request
- [x] ET MALWARE W32.FakeEzQ.kr Checkin
- [x] ET MALWARE Malicious Mega Chrome Extension Exfil Domain (www .megaopac .host in TLS SNI)
- [x] ET MALWARE OilRig CnC DNS Lookup (windowspatch .com)
- [x] ET MALWARE OilRig OopsIE CnC Checkin M3
- [x] ET MALWARE Suspected Monero Miner CnC Channel TXT Lookup
- [x] ET MALWARE Win32/Aura Ransomware CnC Activity
- [x] ET MALWARE Observed Malicious SSL Cert (MageCart Exfil Domain)
- [x] ET MALWARE [PTsecurity] Win32/Ramnit Stage 0 Communicating with CnC
- [x] ET MALWARE Fbot Blockchain Based CnC DNS Lookup (musl .lib)
- [x] ET MALWARE Fbot/Satori CnC DNS Lookup (rippr .cc)
- [x] ET MALWARE Xbash CnC DNS Lookup (leakingprivacy .tk)
- [x] ET MALWARE Xbash CnC DNS Lookup (scanaan .tk)
- [x] ET MALWARE HTML/Xbash Hex Encoded PowerShell Args Inbound - Stage 1
- [x] ET MALWARE HTML/Xbash Hex Encoded PS WebClient Object Inbound - Stage 1
- [x] ET MALWARE Xbash CnC DNS Lookup (3g2upl4pq6kufc4m .tk)
- [x] ET MALWARE MS_D0wnl0ad3r Checkin
- [x] ET MALWARE Suspected DNS2TCP Connect
- [x] ET MALWARE VPNFilter htpx Module C2 Request
- [x] ET MALWARE Reaper (APT37) DNS Lookup (kmbr1 .nitesbr1 .org)
- [ ] ET MALWARE VBScript Redirect Style Exe File Download
- [x] ET MALWARE Win32.YordanyanActiveAgent Generic CnC Pattern
- [x] ET MALWARE NCSC XAgent itwm beacon v1
- [ ] ET MALWARE NCSC APT28 - CompuTrace_Beacon_UserAgent
- [ ] ET MALWARE Possible Locky JS Downloading Payload
- [x] ET MALWARE Observed Malicious SSL Cert (Win32/Gadwats Banker CnC Domain)
- [x] ET MALWARE FruityArmor DNS Lookup (shelves-design .com)
- [ ] ET MALWARE [PTsecurity] Kraken Ransomware Start Activity 2
- [x] ET MALWARE XLS.Unk DDE rar Drop Attempt (.online)
- [x] ET MALWARE Malicious XLS DDE rar Drop Fake 404 Response
- [x] ET MALWARE Win32/Remcos RAT Checkin 55
- [x] ET MALWARE Win32/Remcos RAT Checkin 57
- [x] ET MALWARE Win32/Remcos RAT Checkin 59
- [x] ET MALWARE Win32/Remcos RAT Checkin 61
- [x] ET MALWARE Win32/Remcos RAT Checkin 63
- [x] ET MALWARE Win32/Remcos RAT Checkin 65
- [x] ET MALWARE Win32/Remcos RAT Checkin 67
- [x] ET MALWARE Win32/Bisonal CnC Checkin
- [x] ET MALWARE Win32/Bisonal DNS Lookup 1
- [x] ET MALWARE Win32/Bisonal DNS Lookup 3
- [x] ET MALWARE Win32/Bisonal DNS Lookup 5
- [x] ET MALWARE MSIL/Eredel Stealer CnC Checkin
- [x] ET MALWARE SSL Cert Associated with Lazarus Downloader (JEUSD)
- [x] ET MALWARE Sharik/Smoke CnC Beacon 11
- [x] ET MALWARE Observed Malicious SSL Cert (Panda Banker C2)
- [x] ET MALWARE Panda Banker C2 Domain (uiaoduiiej .chimkent .su in DNS Lookup)
- [x] ET MALWARE Panda Banker Injects Domain (urimchi3dt4 .website in DNS Lookup)
- [x] ET MALWARE [PTsecurity] Tinba (Banking Trojan) HTTP Header
- [x] ET MALWARE [PTsecurity] Remcos RAT Checkin 26
- [x] ET MALWARE Win32/Remcos RAT Checkin 26
- [x] ET MALWARE Win32/Remcos RAT Checkin 28
- [x] ET MALWARE Win32/Remcos RAT Checkin 30
- [x] ET MALWARE MSIL/BISKVIT DNS Lookup (secured-links .org)
- [x] ET MALWARE CobaltStrike DNS Beacon Response
- [x] ET MALWARE Malicious Mega Chrome Extension Exfil Domain (www .megaopac .host in DNS Lookup)
- [x] ET MALWARE OilRig CnC DNS Lookup (defender-update .com)
- [x] ET MALWARE OilRig OopsIE CnC Checkin M2
- [x] ET MALWARE OilRig OopsIE CnC Checkin M4
- [x] ET MALWARE Suspected Monero Miner CnC Channel Secondary Domain Lookup
- [ ] ET MALWARE Aura Ransomware User-Agent
- [x] ET MALWARE Observed Malicious SSL Cert (MageCart Exfil)
- [x] ET MALWARE Observed Malicious SSL Cert (MageCart Exfil Domain)
- [x] ET MALWARE Fbot/Satori CnC DNS Lookup (ukrainianhorseriding .com)
- [x] ET MALWARE Xbash CnC DNS Lookup (censys .xyz)
- [x] ET MALWARE Xbash CnC DNS Lookup (realnewstime .xyz)
- [x] ET MALWARE Xbash CnC DNS Lookup (blockbitcoin .com)
- [x] ET MALWARE HTML/Xbash Hex Encoded WScript.Shell Inbound - Stage 1
- [x] ET MALWARE Xbash CnC DNS Lookup (vfk2k5s5tfjr27tz .tk)
- [x] ET MALWARE MS_D0wnl0ad3r Screenshot Upload
- [x] ET MALWARE Suspected DNS2TCP Auth
- [x] ET MALWARE Suspected fraud-bridge DNS Tunnel
- [x] ET MALWARE Win32/Final1stspy CnC Checkin (Reaper/APT37 Stage 1 Payload)
- [x] ET MALWARE [PTsecurity] Win32/Remcos RAT Checkin 51
- [x] ET MALWARE Win32.YordanyanActiveAgent CnC Reporting
- [x] ET MALWARE NCSC XAgent Beacon
- [x] ET MALWARE NCSC XAgent itwm beacon v2
- [x] ET MALWARE NCSC APT28 - Web/request -FILE- contenttype
- [x] ET MALWARE Observed Malicious SSL Cert (Win32/Gadwats Banker CnC Domain)
- [x] ET MALWARE FruityArmor DNS Lookup (weekendstrips .net)
- [ ] ET MALWARE Kraken Ransomware Start Activity 1
- [x] ET MALWARE Kraken Ransomware End Activity
- [x] ET MALWARE XLS.Unk DDE rar Drop Attempt (.club)
- [x] ET MALWARE Win32/Remcos RAT Checkin 54
- [x] ET MALWARE Win32/Remcos RAT Checkin 56
- [x] ET MALWARE Win32/Remcos RAT Checkin 58
- [x] ET MALWARE Win32/Remcos RAT Checkin 60
- [x] ET MALWARE Win32/Remcos RAT Checkin 62
- [x] ET MALWARE Win32/Remcos RAT Checkin 64
- [x] ET MALWARE Win32/Remcos RAT Checkin 66
- [x] ET MALWARE Win32/Remcos RAT Checkin 68