```
# Emerging Threats
#
# This distribution may contain rules under two different licenses.
#
#  Rules with sids 1 through 3464, and 100000000 through 100000908 are under the GPLv2.
#  A copy of that license is available at http://www.gnu.org/licenses/gpl-2.0.html
#
#  Rules with sids 2000000 through 2799999 are from Emerging Threats and are covered under the BSD License
#  as follows:
#
#*************************************************************
#  Copyright (c) 2003-2024, Emerging Threats
#  All rights reserved.
#
#  Redistribution and use in source and binary forms, with or without modification, are permitted provided that
the
#  following conditions are met:
#
#  * Redistributions of source code must retain the above copyright notice, this list of conditions and the
following
#    disclaimer.
#  * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the
#    following disclaimer in the documentation and/or other materials provided with the distribution.
#  * Neither the name of the nor the names of its contributors may be used to endorse or promote products derived
#    from this software without specific prior written permission.
#
#  THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS AS IS AND ANY EXPRESS OR IMPLIED
WARRANTIES,
#  INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE
#  DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL,
#  SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
#  SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY,
#  WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF
THE
#  USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
#
#*************************************************************
#
#
#
#

# This Ruleset is EmergingThreats Open optimized for snort-2.9.0-enhanced.

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (_)";
flow:to_server,established; content:"User-Agent|3a| _|0d 0a|"; http_header; classtype:trojan-activity;
sid:2007942; rev:6; metadata:created_at 2010_07_30, signature_severity Major, updated_at 2010_08_05;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (ScrapeBox)";
flow:to_server,established; content:"|0d 0a|User-Agent|3a| ScrapeBox"; http_header; classtype:trojan-activity;
sid:2011282; rev:2; metadata:created_at 2010_09_28, signature_severity Major, updated_at 2010_09_28;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS sgrunt Dialer User Agent (sgrunt)";
flow:to_server,established; content:"sgrunt"; http_header; fast_pattern:only; pcre:"/User-Agent\:[^\n]+sgrunt/iH";
reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=453096347; classtype:trojan-activity; sid:2003385;
rev:12; metadata:created_at 2010_07_30, updated_at 2010_10_07;)
```

```
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS User Agent Containing http Suspicious -
Likely Spyware/Trojan"; flow:to_server,established; content:"User-Agent|3a|"; nocase; http_header; content:!"rss";
nocase; http_header; pcre:"/User-Agent\:[^\n]+http\:\/\//iH"; classtype:trojan-activity; sid:2003394; rev:9;
metadata:created_at 2010_07_30, updated_at 2010_10_12;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent no space";
flow:established,to_server; content:"User-Agent|3a|"; http_header; content:!"User-Agent|3a 20|"; http_raw_header;
classtype:bad-unknown; sid:2012180; rev:1; metadata:created_at 2011_01_15, updated_at 2011_01_15;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS suspicious user-agent (REKOM)";
flow:established,to_server; content:"GET"; http_method; content:"|0d 0a|User-Agent|3a| REKOM"; nocase;
http_header; classtype:trojan-activity; sid:2012295; rev:2; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2011_02_07, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2011_02_07;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent VCTestClient";
flow:to_server,established; content:"|0d 0a|User-Agent|3a| VCTestClient"; nocase; http_header; classtype:trojan-
activity; sid:2012386; rev:1; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2011_02_27,
deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2011_02_27;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent
PrivacyInfoUpdate"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| PrivacyInfoUpdate"; nocase;
http_header; classtype:trojan-activity; sid:2012387; rev:1; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2011_02_27, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2011_02_27;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent Moxilla";
flow:established,to_server; content:"User-Agent|3a| Moxilla"; http_header; classtype:trojan-activity; sid:2012313;
rev:4; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2011_02_14, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2011_03_17;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (VMozilla)";
flow:to_server,established; content:"User-Agent|3a| VMozilla"; http_header; nocase;
reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3aWin32%2fNeeris.BF;
reference:url,www.avira.com/en/support-threats-description/tid/6259/tlang/en; classtype:trojan-activity;
sid:2012555; rev:1; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2011_03_25,
deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2011_03_25;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent Sample";
flow:established,to_server; content:"User-Agent|3A| sample"; nocase; http_header; classtype:trojan-activity;
sid:2012611; rev:3; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2011_03_31,
deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2011_04_01;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS suspicious User Agent (Lotto)";
flow:to_server,established; content:"User-Agent|3a| Lotto"; http_header; classtype:trojan-activity; sid:2012695;
rev:2; metadata:created_at 2011_04_20, signature_severity Major, updated_at 2011_04_20;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent String
(AskPartnerCobranding)"; flow:to_server,established; content:"User-Agent|3a| AskPartner"; http_header;
fast_pattern:only; classtype:trojan-activity; sid:2012734; rev:2; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2011_04_28, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2011_04_28;)

alert tcp $HOME_NET any -> $EXTERNAL_NET 808 (msg:"ET USER_AGENTS suspicious user agent string (changhuatong)";
flow:to_server,established; content:"|0d 0a|User-Agent|3a 20|changhuatong|0d 0a|"; classtype:trojan-activity;
sid:2012751; rev:1; metadata:created_at 2011_04_29, signature_severity Major, updated_at 2011_04_29;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious user agent (mdms)";
flow:to_server,established; content:"GET"; http_method; content:"User-Agent|3a| mdms|0d 0a|"; http_header;
classtype:trojan-activity; sid:2012761; rev:2; metadata:created_at 2011_05_03, signature_severity Major,
updated_at 2011_05_03;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious user agent (asd)";
flow:to_server,established; content:"GET"; http_method; content:"User-Agent|3a| asd|0d 0a|"; nocase; http_header;
classtype:trojan-activity; sid:2012762; rev:2; metadata:created_at 2011_05_03, signature_severity Major,
updated_at 2011_05_03;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS suspicious user agent string
(CholTBAgent)"; flow:to_server,established; content:"User-Agent|3a 20|CholTBAgent"; http_header;
detection_filter:track by_dst, count 4, seconds 20; classtype:trojan-activity; sid:2012757; rev:4;
metadata:created_at 2011_04_30, signature_severity Major, updated_at 2011_05_25;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Updater)";
flow:to_server,established; content:"User-Agent|3a| Updater"; http_header; threshold: type limit, count 3, seconds
300, track by_src; classtype:trojan-activity; sid:2003584; rev:10; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2011_05_26;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS EmailSiphon Suspicious User-Agent
Outbound"; flow:established,to_server; content:"User-Agent|3a| EmailSiphon"; nocase; http_header;
reference:url,www.useragentstring.com/pages/useragentstring.php; classtype:attempted-recon; sid:2013033; rev:1;
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2011_06_14, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2011_06_14;)

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET USER_AGENTS EmailSiphon Suspicious User-Agent
Inbound"; flow:established,to_server; content:"User-Agent|3a| EmailSiphon"; nocase; http_header;
reference:url,www.useragentstring.com/pages/useragentstring.php; classtype:attempted-recon; sid:2013032; rev:2;
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2011_06_14, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2011_06_14;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Binget PHP Library User Agent Outbound";
flow:established,to_server; content:"User-Agent|3a| Binget/"; nocase; http_header; reference:url,www.bin-
co.com/php/scripts/load/; reference:url,www.useragentstring.com/pages/useragentstring.php; classtype:attempted-
recon; sid:2013050; rev:1; metadata:created_at 2011_06_17, updated_at 2011_06_17;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS pxyscand/ Suspicious User Agent
Outbound"; flow:established,to_server; content:"User-Agent|3a| pxyscand/"; nocase; http_header;
reference:url,www.useragentstring.com/pages/useragentstring.php; classtype:attempted-recon; sid:2013052; rev:1;
metadata:created_at 2011_06_17, updated_at 2011_06_17;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS PyCurl Suspicious User Agent Outbound";
flow:established,to_server; content:"User-Agent|3a| PyCurl"; nocase; http_header;
reference:url,www.useragentstring.com/pages/useragentstring.php; classtype:attempted-recon; sid:2013054; rev:1;
metadata:created_at 2011_06_17, updated_at 2011_06_17;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent Fragment
(WORKED)"; flow:established,to_server; content:"WORKED"; http_header; pcre:"/User-Agent\x3a[^\n]+WORKED/H";
classtype:trojan-activity; sid:2012909; rev:2; metadata:affected_product Any, attack_target Client_Endpoint,
created_at 2011_05_31, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2011_07_23;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (BlackSun)";
flow:to_server,established; content:"User-Agent|3a| BlackSun"; http_header; nocase;
reference:url,www.bitdefender.com/VIRUS-1000328-en--Trojan.Pws.Wow.NCY.html; classtype:trojan-activity;
sid:2008983; rev:7; metadata:created_at 2010_07_30, signature_severity Major, updated_at 2011_08_06;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Win32/OnLineGames User-Agent (Revolution
Win32)"; flow:established,to_server; content:"User-Agent|3A 20|Revolution"; http_header;
reference:md5,1431f4ab4bbe3ad1087eb14cf4d7dff9; classtype:trojan-activity; sid:2013542; rev:1; metadata:created_at
2011_09_06, signature_severity Major, updated_at 2011_09_06;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS badly formatted User-Agent string (no
closing parenthesis)"; flow:established,to_server; content:"User-Agent|3a| Mozilla/4.0 (compatible|3b| ";
```

```
fast_pattern:16,20; http_header; content:!")|0d 0a|"; within:100; http_header; pcre:"/User-
Agent\x3a\sMozilla\/4\.0\s\(compatible[^\)]+\r\n/H"; classtype:bad-unknown; sid:2010906; rev:9;
metadata:created_at 2010_07_30, updated_at 2011_10_19;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Our_Agent)";
flow:established,to_server; content:" Our_Agent"; http_header; classtype:trojan-activity; sid:2012278; rev:5;
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2011_02_03, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2011_10_19;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Lowercase User-Agent header purporting
to be MSIE"; flow:established,to_server; content:"user-agent|3a 20|Mozilla/4.0|20|(compatible|3b 20|MSIE|20|";
http_header; content:!"|0d 0a|VIA|3a 20|"; http_header; classtype:trojan-activity; sid:2012607; rev:3;
metadata:created_at 2011_03_31, updated_at 2011_10_19;)

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET USER_AGENTS Atomic_Email_Hunter User-Agent Inbound";
flow:established,to_server; content:"User-Agent|3a| Atomic_Email_Hunter/"; fast_pattern:12,20; http_header;
reference:url,www.useragentstring.com/pages/useragentstring.php; classtype:attempted-recon; sid:2013173; rev:3;
metadata:created_at 2011_07_04, updated_at 2012_01_18;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Atomic_Email_Hunter User-Agent
Outbound"; flow:established,to_server; content:"User-Agent|3a| Atomic_Email_Hunter/"; fast_pattern:12,20;
http_header; reference:url,www.useragentstring.com/pages/useragentstring.php; classtype:attempted-recon;
sid:2013174; rev:2; metadata:created_at 2011_07_04, updated_at 2012_01_18;)

#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious Non-Escaping backslash in
User-Agent Inbound"; flow:established,to_server; content:"User-Agent|3a|"; nocase; http_header; content:"|5C|";
http_header; content:!"|5C|Citrix|5C|ICA Client|5C|"; nocase; http_header; pcre:"/User-Agent\:.*
[^\x5c]\x5c[^\x5c\x3d\x2f\x3b\x28\x29]/iH"; reference:url,www.w3.org/Protocols/rfc2616/rfc2616-sec14.html;
reference:url,mws.amazon.com/docs/devGuide/UserAgent.html; classtype:bad-unknown; sid:2010722; rev:7;
metadata:created_at 2010_07_30, updated_at 2012_06_22;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent SimpleClient 1.0";
flow:established,to_server; content:"User-Agent|3A| SimpleClient "; http_header;
reference:url,www.fortiguard.com/encyclopedia/virus/symbos_sagasi.a!tr.html; classtype:bad-unknown; sid:2012860;
rev:3; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2011_05_26, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2012_08_17;)

alert tcp $HOME_NET 1024: -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious Win32 User Agent";
flow:to_server,established; content:"User-Agent|3a| Win32"; nocase; http_header; classtype:trojan-activity;
sid:2012249; rev:2; metadata:created_at 2011_02_02, signature_severity Major, updated_at 2013_01_24;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS User-Agent (ChilkatUpload)";
flow:to_server,established; content:"User-Agent|3a| ChilkatUpload"; http_header; nocase;
reference:url,chilkatsoft.com; classtype:trojan-activity; sid:2016904; rev:1; metadata:created_at 2013_05_21,
signature_severity Major, updated_at 2013_05_21;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious user agent (Google page)";
flow:to_server,established; content:"User-Agent|3a| Google page"; nocase; http_header; classtype:trojan-activity;
sid:2017067; rev:3; metadata:created_at 2011_05_31, signature_severity Major, updated_at 2013_06_25;)

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET USER_AGENTS FOCA User-Agent";
flow:established,to_server; content:"GET"; http_method; content:"User-Agent|3a 20|FOCA|0d 0a|"; http_header;
fast_pattern:only; content:!"Referer|3a 20|"; http_header; content:!"Accept|3a 20|"; http_header;
reference:url,blog.bannasties.com/2013/08/vulnerability-scans/; classtype:attempted-recon; sid:2017949; rev:3;
metadata:created_at 2014_01_10, updated_at 2014_01_10;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (DownloadMR)";
flow:to_server,established; content:"User-Agent|3a| DownloadMR"; nocase; http_header;
reference:url,www.virustotal.com/en/file/93236b781e147e3ac983be1374a5f807fabd27ee2b92e6d99e293a6eb070ac2b/analysis
/; reference:md5,0da0d8e664f44400c19898b4c9e71456; classtype:trojan-activity; sid:2016903; rev:2;
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2013_05_21, deployment Perimeter,
```

```
signature_severity Major, tag User_Agent, updated_at 2014_03_24;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS 2search.org User Agent (2search)";
flow:to_server,established; content:"User-Agent|3a| "; http_header; content:"2search"; fast_pattern; within:150;
http_header; pcre:"/^User-Agent\x3a\x20[^\r\n]+?2search/Hmi"; classtype:trojan-activity; sid:2003335; rev:18;
metadata:created_at 2010_07_30, updated_at 2014_04_14;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious Non-Escaping backslash in
User-Agent Outbound"; flow:established,to_server; content:"User-Agent|3a|"; nocase; http_header; content:"|5C|";
http_header; content:!"|5C|Citrix|5C|ICA Client|5C|"; nocase; http_header; pcre:"/User-Agent\:.*
[^\x5c]\x5c[^\x5c\x3d\x2f\x3b\x28\x29]/iH"; reference:url,www.w3.org/Protocols/rfc2616/rfc2616-sec14.html;
reference:url,mws.amazon.com/docs/devGuide/UserAgent.html; classtype:bad-unknown; sid:2010721; rev:8;
metadata:created_at 2010_07_30, updated_at 2014_08_28;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS MSF Meterpreter Default User Agent";
flow:established,to_server; content:"User-Agent|3a 20|Mozilla/4.0 (compatible|3b 20|MSIE 6.1|3b 20|Windows NT|29
0d 0a|"; http_header; fast_pattern:40,20; reference:url,blog.didierstevens.com/2015/03/16/quickpost-metasploit-
user-agent-strings; classtype:bad-unknown; sid:2021060; rev:1; metadata:created_at 2015_05_06, updated_at
2015_05_06;)

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET USER_AGENTS BLEXBot User-Agent";
flow:established,to_server; content:"User-Agent|3a 20|Mozilla/5.0 (compatible|3b| BLEXBot/"; fast_pattern:25,20;
http_header; threshold:type limit, track by_dst, count 1, seconds 300; reference:url,webmeup.com/about.html;
classtype:misc-activity; sid:2022775; rev:1; metadata:created_at 2016_05_02, updated_at 2016_05_02;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (USERAGENT)";
flow:to_server,established; content:"User-Agent|3a| USERAGENT|0d 0a|"; nocase; http_header;
reference:md5,cd0e98508657b208219d435f9ac9d76c; reference:md5,cd100abc8eedf2119c7e6746975d7773; classtype:trojan-
activity; sid:2034066; rev:4; metadata:created_at 2011_11_22, signature_severity Major, updated_at 2016_11_21;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS SideStep User-Agent"; flow:
to_server,established; content:" SideStep"; http_header; fast_pattern:only; pcre:"/User-Agent\:[^\n]+SideStep/iH";
reference:url,github.com/chetan51/sidestep/; classtype:misc-activity; sid:2002078; rev:31; metadata:attack_target
Client_Endpoint, created_at 2010_07_30, deployment Perimeter, performance_impact Low, signature_severity Minor,
tag User_Agent, updated_at 2017_01_20;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS User-Agent (Unknown)";
flow:to_server,established; content:"User-Agent|3a| Unknown|0d 0a|"; http_header; classtype:trojan-activity;
sid:2007991; rev:7; metadata:created_at 2010_07_30, signature_severity Major, updated_at 2017_09_13;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Metafisher/Goldun User-Agent (z)";
flow:to_server,established; content:"User-Agent|3a| z|0d 0a|"; http_header; classtype:trojan-activity;
sid:2002874; rev:12; metadata:created_at 2010_07_30, signature_severity Major, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (WinXP Pro
Service Pack 2)"; flow:to_server,established; content:"User-Agent|3a| WinXP Pro Service Pack"; http_header;
threshold: type limit, count 3, seconds 300, track by_src; classtype:trojan-activity; sid:2003586; rev:12;
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent outbound (bot)";
flow:to_server,established; content:"User-Agent|3a| bot/"; nocase; http_header; threshold: type limit, count 3,
seconds 300, track by_src; classtype:trojan-activity; sid:2003622; rev:12; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (MSIE)";
flow:to_server,established; content:"User-Agent|3a| MSIE"; http_header; threshold: type limit, count 2, track
by_src, seconds 300; content:!"www.msftncsi.com"; http_header; classtype:trojan-activity; sid:2003657; rev:14;
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2017_10_30;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (HTTPTEST) - Seen
used by downloaders"; flow:to_server,established; content:"User-Agent|3a| HTTPTEST"; nocase; http_header;
content:!"PlayStation"; http_header; threshold: type limit, count 2, track by_src, seconds 300; classtype:trojan-
activity; sid:2003927; rev:10; metadata:affected_product Any, attack_target Client_Endpoint, created_at
2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Snatch-System)";
flow:to_server,established; content:"User-Agent|3a| Snatch-System"; nocase; http_header; threshold: type limit,
count 2, track by_src, seconds 300; classtype:trojan-activity; sid:2003930; rev:9; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS KKtone Suspicious User-Agent (KKTone)";
flow:to_server,established; content:"User-Agent|3a| KKTone"; nocase; http_header; threshold: type limit, count 2,
track by_src, seconds 300; classtype:trojan-activity; sid:2004443; rev:9; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Dialer-967 User-Agent";
flow:to_server,established; content:"User-Agent|3a| del|0d 0a|"; http_header; nocase; classtype:trojan-activity;
sid:2006364; rev:6; metadata:created_at 2010_07_30, signature_severity Major, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (MYURL)";
flow:to_server,established; content:"User-Agent|3a| MYURL|0d 0a|"; http_header; threshold: type limit, count 2,
track by_src, seconds 300; classtype:trojan-activity; sid:2006365; rev:9; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Matcash or related downloader User-
Agent Detected"; flow:established,to_server; content:"User-Agent|3a| x"; http_header; pcre:"/^User-Agent\:
x\w\wx\w\w\!x\w\wx\w\wx\w\w/Hm"; classtype:trojan-activity; sid:2006382; rev:9; metadata:created_at 2010_07_30,
updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Downloader User-Agent Detected (Windows
Updates Manager|3.12|...)"; flow:established,to_server; content:"User-Agent|3a| Windows Updates Manager|7c|";
http_header; classtype:trojan-activity; sid:2006387; rev:8; metadata:created_at 2010_07_30, signature_severity
Major, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Downloader User-Agent Detected (ld)";
flow:established,to_server; content:"User-Agent|3a| ld|0d 0a|"; http_header; classtype:trojan-activity;
sid:2006394; rev:7; metadata:created_at 2010_07_30, signature_severity Major, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Eldorado.BHO User-Agent Detected
(netcfg)"; flow:established,to_server; content:"GET"; nocase; http_method; content:"User-Agent|3a| netcfg|0d 0a|";
http_header; classtype:trojan-activity; sid:2007758; rev:8; metadata:created_at 2010_07_30, updated_at
2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Win32/Feebs.kw Worm User-Agent
Detected"; flow:established,to_server; content:"User-Agent|3a| Mozilla/4.7 [en] (WinNT"; http_header;
fast_pattern:20,15; classtype:trojan-activity; sid:2007767; rev:6; metadata:created_at 2010_07_30,
signature_severity Major, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Tear Application User-Agent Detected";
flow:established,to_server; content:"User-Agent|3a| Tear Application|0d 0a|"; http_header; classtype:trojan-
activity; sid:2007770; rev:5; metadata:created_at 2010_07_30, signature_severity Major, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS User-agent DownloadNetFile
Win32.small.hsh downloader"; flow:established,to_server; content:"GET"; nocase; http_method; content:"User-
Agent|3A| DownloadNetFile|0D 0A|"; http_header; nocase; classtype:trojan-activity; sid:2007778; rev:12;
metadata:created_at 2010_07_30, signature_severity Major, updated_at 2017_10_30;)
```

```
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Cashpoint.com Related checkin User-Agent (inetinst)"; flow:established,to_server; content:"User-Agent|3a| inetinst|0d 0a|"; http_header; classtype:trojan-activity; sid:2007808; rev:5; metadata:created_at 2010_07_30, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Cashpoint.com Related checkin User-Agent (okcpmgr)"; flow:established,to_server; content:"User-Agent|3a| okcpmgr|0d 0a|"; http_header; classtype:trojan-activity; sid:2007810; rev:5; metadata:created_at 2010_07_30, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Eldorado.BHO User-Agent Detected (MSIE 5.5)"; flow:established,to_server; content:"GET"; nocase; http_method; content:"User-Agent|3a| MSIE 5.5|0d 0a|"; http_header; classtype:trojan-activity; sid:2007833; rev:6; metadata:created_at 2010_07_30, signature_severity Major, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent - Possible Trojan Downloader (https)"; flow:established,to_server; content:"User-Agent|3a| https|0d 0a|"; http_header; nocase; classtype:trojan-activity; sid:2008019; rev:4; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, tag Trojan_Downloader, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (c \windows)"; flow:to_server,established; content:"User-Agent|3a| c|3a 5c|"; http_header; threshold: type limit, count 2, track by_src, seconds 300; classtype:trojan-activity; sid:2008043; rev:12; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Rf-cheats.ru Trojan Related User-Agent (RFRudokop v.1.1 account verification)"; flow:to_server,established; content:"User-Agent|3a| RFRudokop "; http_header; classtype:trojan-activity; sid:2008046; rev:7; metadata:created_at 2010_07_30, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Version 1.23)"; flow:to_server,established; content:"User-Agent|3a| Version "; http_header; threshold: type limit, count 2, track by_src, seconds 300; classtype:trojan-activity; sid:2008048; rev:9; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (App4)"; flow:to_server,established; content:"User-Agent|3a| App"; http_header; content:!"Host|3a| liveupdate.symantecliveupdate.com|0d 0a|"; http_header; pcre:"/^User-Agent\x3a App\d/Hm"; threshold: type limit, count 2, track by_src, seconds 300; classtype:trojan-activity; sid:2008073; rev:13; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Mozilla-web)"; flow:to_server,established; content:"User-Agent|3a| Mozilla-web"; http_header; threshold: type limit, count 2, track by_src, seconds 300; classtype:trojan-activity; sid:2008084; rev:10; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (INSTALLER)"; flow:to_server,established; content:"User-Agent|3a| INSTALLER|0d 0a|"; http_header; threshold: type limit, count 2, track by_src, seconds 300; classtype:trojan-activity; sid:2008096; rev:9; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (IEMGR)"; flow:to_server,established; content:"User-Agent|3a| IEMGR|0d 0a|"; http_header; threshold: type limit, count 2, track by_src, seconds 300; classtype:trojan-activity; sid:2008097; rev:8; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2017_10_30;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (GOOGLE)";
flow:to_server,established; content:"User-Agent|3a| GOOGLE|0d 0a|"; http_header; threshold: type limit, count 2,
track by_src, seconds 300; classtype:trojan-activity; sid:2008098; rev:8; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Vapsup User-Agent (doshowmeanad loader
v2.1)"; flow:to_server,established; content:"User-Agent|3a| doshowmeanad "; http_header; classtype:trojan-
activity; sid:2008142; rev:6; metadata:created_at 2010_07_30, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (RBR)";
flow:to_server,established; content:"User-Agent|3a| RBR|0d 0a|"; http_header; threshold: type limit, count 2,
track by_src, seconds 300; classtype:trojan-activity; sid:2008147; rev:8; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Otwycal User-Agent (Downing)";
flow:to_server,established; content:"User-Agent|3a| Downing|0d 0a|"; http_header; classtype:trojan-activity;
sid:2008159; rev:4; metadata:created_at 2010_07_30, signature_severity Major, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (MS Internet
Explorer)"; flow:to_server,established; content:"User-Agent|3a| MS Internet Explorer|0d 0a|"; http_header;
threshold:type limit,count 2,track by_src,seconds 300; classtype:trojan-activity; sid:2008181; rev:8;
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Installer)";
flow:to_server,established; content:"User-Agent|3a| Installer|0d 0a|"; http_header; threshold:type limit,count
2,track by_src,seconds 300; classtype:trojan-activity; sid:2008184; rev:9; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (QQ)";
flow:to_server,established; content:"User-Agent|3a| QQ|0d 0a|"; http_header; content:!"|0d 0a|Q-UA|3a 20|";
http_header; threshold:type limit,count 2,track by_src,seconds 300; classtype:trojan-activity; sid:2008199;
rev:15; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (TestAgent)";
flow:to_server,established; content:"User-Agent|3a| TestAgent|0d 0a|"; http_header; threshold:type limit,count
2,track by_src,seconds 300; classtype:trojan-activity; sid:2008208; rev:8; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (SERVER2_03)";
flow:to_server,established; content:"User-Agent|3a| SERVER"; http_header; threshold:type limit,count 2,track
by_src,seconds 300; classtype:trojan-activity; sid:2008209; rev:8; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (WinProxy)";
flow:to_server,established; content:"User-Agent|3a| WinProxy|0d 0a|"; nocase; http_header; threshold:type
limit,count 2,track by_src,seconds 300; classtype:trojan-activity; sid:2008211; rev:8; metadata:affected_product
Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent
(sickness29a/0.1)"; flow:to_server,established; content:"User-Agent|3a| sickness"; nocase; http_header;
threshold:type limit,count 2,track by_src,seconds 300; classtype:trojan-activity; sid:2008214; rev:8;
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter,
```

```
signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (up2dash
updater)"; flow:to_server,established; content:"User-Agent|3a| up2dash"; nocase; http_header; threshold:type
limit,count 2,track by_src,seconds 300; classtype:trojan-activity; sid:2008215; rev:8; metadata:affected_product
Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Mozilla 1.02.45
biz)"; flow:to_server,established; content:"User-Agent|3a| Mozilla "; http_header; content:" biz|0d 0a|";
within:15; http_header; threshold:type limit,count 2,track by_src,seconds 300; classtype:trojan-activity;
sid:2008231; rev:9; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30,
deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (chek)";
flow:to_server,established; content:"User-Agent|3a| chek|0d 0a|"; http_header; threshold:type limit,count 2,track
by_src,seconds 300; classtype:trojan-activity; sid:2008253; rev:8; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (IE)";
flow:to_server,established; content:"User-Agent|3a| IE|0d 0a|"; http_header; threshold:type limit,count 2,track
by_src,seconds 300; classtype:trojan-activity; sid:2008255; rev:8; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (AutoHotkey)";
flow:to_server,established; content:"User-Agent|3a| AutoHotkey"; http_header; threshold:type limit,count 2,track
by_src,seconds 300; content:!".ahk4.net|0d 0a|"; http_header; classtype:trojan-activity; sid:2008259; rev:9;
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (WebForm 1)";
flow:to_server,established; content:"User-Agent|3a| WebForm"; http_header; threshold:type limit,count 2,track
by_src,seconds 300; classtype:trojan-activity; sid:2008262; rev:8; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (opera)";
flow:to_server,established; content:"User-Agent|3a| opera|0d 0a|"; http_header; threshold:type limit,count 2,track
by_src,seconds 300; classtype:trojan-activity; sid:2008264; rev:8; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Zilla)";
flow:to_server,established; content:"User-Agent|3a| Zilla|0d 0a|"; http_header; threshold:type limit,count 2,track
by_src,seconds 300; classtype:trojan-activity; sid:2008266; rev:9; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (contains
loader)"; flow:to_server,established; content:" loader"; http_header; fast_pattern:only; pcre:"/User-
Agent\x3a[^\n]+loader/iH"; threshold:type limit,count 2,track by_src,seconds 300; classtype:trojan-activity;
sid:2008276; rev:14; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30,
deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (123)";
flow:to_server,established; content:"User-Agent|3a| 123|0d 0a|"; http_header; threshold: type limit, count 2,
track by_src, seconds 300; classtype:trojan-activity; sid:2008343; rev:8; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (angel)";
flow:to_server,established; content:"User-Agent|3a| angel|0d 0a|"; http_header; threshold: type limit, count 2,
track by_src, seconds 300; classtype:trojan-activity; sid:2008355; rev:8; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Accessing)";
flow:to_server,established; content:"User-Agent|3a| Accessing|0d 0a|"; http_header; threshold: type limit, count
2, track by_src, seconds 300; classtype:trojan-activity; sid:2008361; rev:8; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (ISMYIE)";
flow:to_server,established; content:"User-Agent|3a| ISMYIE|0d 0a|"; http_header; threshold: type limit, count 2,
track by_src, seconds 300; classtype:trojan-activity; sid:2008363; rev:8; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (ErrCode)";
flow:established,to_server; content:"User-Agent|3a| ErrCode"; http_header; classtype:trojan-activity; sid:2008378;
rev:13; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (svchost)";
flow:established,to_server; content:"User-Agent|3a| svchost"; nocase; http_header; threshold: type limit, count 2,
track by_src, seconds 300; classtype:trojan-activity; sid:2008391; rev:12; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (ReadFileURL)";
flow:established,to_server; content:"User-Agent|3a| ReadFileURL|0d 0a|"; http_header; threshold: type limit, count
2, track by_src, seconds 300; classtype:trojan-activity; sid:2008400; rev:11; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (PcPcUpdater)";
flow:established,to_server; content:"User-Agent|3a| PcPcUpdater"; http_header; threshold: type limit, count 2,
track by_src, seconds 300; classtype:trojan-activity; sid:2008413; rev:10; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Inet_read)";
flow:established,to_server; content:"User-Agent|3a| Inet_read"; http_header; threshold: type limit, count 2, track
by_src, seconds 300; classtype:trojan-activity; sid:2008422; rev:11; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (CFS Agent)";
flow:established,to_server; content:"User-Agent|3a| CFS Agent"; http_header; threshold: type limit, count 2, track
by_src, seconds 300; classtype:trojan-activity; sid:2008423; rev:10; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (CFS_DOWNLOAD)";
flow:established,to_server; content:"User-Agent|3a| CFS_DOWNLOAD"; http_header; threshold: type limit, count 2,
track by_src, seconds 300; classtype:trojan-activity; sid:2008424; rev:10; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (AdiseExplorer)";
```

```
flow:established,to_server; content:"User-Agent|3a| AdiseExplorer"; http_header; threshold: type limit, count 2,
track by_src, seconds 300; classtype:trojan-activity; sid:2008427; rev:10; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (HTTP
Downloader)"; flow: established,to_server; content:"User-Agent|3a| HTTP Downloader"; http_header; threshold: type
limit, count 2, track by_src, seconds 300; classtype:trojan-activity; sid:2008428; rev:10;
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (HttpDownload)";
flow:established,to_server; content:"User-Agent|3a| HttpDownload"; http_header; threshold: type limit, count 2,
track by_src, seconds 300; classtype:trojan-activity; sid:2008429; rev:10; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Download App)";
flow:established,to_server; content:"User-Agent|3a| Download App"; http_header; threshold: type limit, count 2,
track by_src, seconds 300; classtype:trojan-activity; sid:2008440; rev:11; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Downloader User-Agent (AutoDL\/1.0)";
flow:established,to_server; content:"GET"; nocase; http_method; content:"User-Agent|3a| AutoDL/1.0|0d 0a|";
http_header; classtype:trojan-activity; sid:2008458; rev:6; metadata:created_at 2010_07_30, signature_severity
Major, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (hacker)";
flow:established,to_server; content:"User-Agent|3a| hacker"; http_header; threshold: type limit, count 2, track
by_src, seconds 300; classtype:trojan-activity; sid:2008460; rev:10; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (ieguideupdate)";
flow:established,to_server; content:"User-Agent|3a| ieguideupdate"; http_header; threshold: type limit, count 2,
track by_src, seconds 300; classtype:trojan-activity; sid:2008463; rev:9; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (adsntD)";
flow:established,to_server; content:"User-Agent|3a| adsntD"; http_header; threshold: type limit, count 2, track
by_src, seconds 300; classtype:trojan-activity; sid:2008464; rev:8; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (NULL)";
flow:established,to_server; content:"User-Agent|3a| NULL"; http_header; threshold: type limit, count 2, track
by_src, seconds 300; classtype:trojan-activity; sid:2008488; rev:8; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (ieagent)";
flow:established,to_server; content:"User-Agent|3a| ieagent"; http_header; threshold:type limit,count 2,track
by_src,seconds 300; classtype:trojan-activity; sid:2008494; rev:8; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent
(antispyprogram)"; flow:established,to_server; content:"User-Agent|3a| antispyprogram"; http_header;
threshold:type limit,count 2,track by_src,seconds 300; classtype:trojan-activity; sid:2008495; rev:8;
```

```
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (SUiCiDE/1.5)";
flow:established,to_server; content:"User-Agent|3a| SUiCiDE"; http_header; threshold:type limit,count 2,track
by_src,seconds 300; classtype:trojan-activity; sid:2008504; rev:8; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (C slash)";
flow:established,to_server; content:"User-Agent|3a| C|3a 5c|"; http_header; content:!"|5c|Citrix|5c|";
http_header; content:!"|5c|Panda S"; nocase; http_header; content:!"|5c|Mapinfo"; http_header; nocase;
threshold:type limit,count 2,track by_src,seconds 300; classtype:trojan-activity; sid:2008512; rev:19;
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (msIE 7.0)";
flow:established,to_server; content:"User-Agent|3a| msIE"; http_header; threshold:type limit,count 2,track
by_src,seconds 300; classtype:trojan-activity; sid:2008513; rev:8; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (AVP2006IE)";
flow:established,to_server; content:"User-Agent|3a| AVP200"; http_header; threshold:type limit,count 2,track
by_src,seconds 300; classtype:trojan-activity; sid:2008514; rev:8; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (winlogon)";
flow:established,to_server; content:"User-Agent|3a| winlogon"; http_header; threshold:type limit,count 2,track
by_src,seconds 300; classtype:trojan-activity; sid:2008544; rev:9; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Internet HTTP
Request)"; flow:established,to_server; content:"User-Agent|3a| Internet HTTP"; http_header; threshold:type
limit,count 2,track by_src,seconds 300; classtype:trojan-activity; sid:2008564; rev:9; metadata:affected_product
Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent Detected
(RLMultySocket)"; flow:established,to_server; content:"User-Agent|3a| RLMultySocket|0d 0a|"; http_header;
threshold:type limit,count 2,track by_src,seconds 300; classtype:trojan-activity; sid:2008603; rev:8;
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS WinFixer Trojan Related User-Agent
(ElectroSun)"; flow:established,to_server; content:"User-Agent|3a| ElectroSun "; http_header; classtype:trojan-
activity; sid:2008608; rev:9; metadata:created_at 2010_07_30, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent Detected
(Downloader1.2)"; flow:established,to_server; content:"User-Agent|3a| Downloader"; http_header; pcre:"/User-
Agent\: Downloader\d+\.\d/H"; threshold:type limit,count 2,track by_src,seconds 300; classtype:trojan-activity;
sid:2008643; rev:8; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30,
deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent Detected
(Compatible)"; flow:established,to_server; content:"User-Agent|3a| Compatible|0d 0a|"; http_header; threshold:type
limit,count 2,track by_src,seconds 300; classtype:trojan-activity; sid:2008657; rev:8; metadata:affected_product
Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent Detected
(GetUrlSize)"; flow:established,to_server; content:"User-Agent|3a| GetUrlSize|0d 0a|"; http_header; threshold:type
limit,count 2,track by_src,seconds 300; classtype:trojan-activity; sid:2008658; rev:8; metadata:affected_product
Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent Detected
(aguarovex-loader v3.221)"; flow:established,to_server; content:"User-Agent|3a| aguarovex-loader v"; http_header;
threshold:type limit,count 2,track by_src,seconds 300; classtype:trojan-activity; sid:2008663; rev:8;
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent Detected
(WINS_HTTP_SEND Program/1.0)"; flow:established,to_server; content:"User-Agent|3a| WINS_HTTP_SEND"; http_header;
threshold:type limit,count 2,track by_src,seconds 300; classtype:trojan-activity; sid:2008734; rev:8;
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (checkonline)";
flow:established,to_server; content:"User-Agent|3a| checkonline|0d 0a|"; http_header; threshold:type limit,count
2,track by_src,seconds 300; classtype:trojan-activity; sid:2008749; rev:8; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Kvadrlson 1.0)";
flow:established,to_server; content:"User-Agent|3a| Kvadrlson "; http_header; threshold:type limit,count 2,track
by_src,seconds 300; classtype:trojan-activity; sid:2008756; rev:8; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Kangkio User-Agent (lsosss)";
flow:established,to_server; content:"User-Agent|3a| lsosss|0d 0a|"; http_header; classtype:trojan-activity;
sid:2008767; rev:4; metadata:created_at 2010_07_30, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (miip)";
flow:established,to_server; content:"User-Agent|3a| miip|0d 0a|"; http_header; threshold:type limit,count 2,track
by_src,seconds 300; classtype:trojan-activity; sid:2008797; rev:8; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Mozil1a)";
flow:established,to_server; content:"User-Agent|3a| Mozil1a"; http_header; threshold:type limit,count 2,track
by_src,seconds 300; classtype:trojan-activity; sid:2008847; rev:9; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Errordigger.com
related)"; flow:established,to_server; content:"User-Agent|3a| min|0d 0a|"; http_header; threshold: type limit,
count 2, track by_src, seconds 300; classtype:trojan-activity; sid:2008912; rev:8; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent
(Trojan.Hijack.IrcBot.457 related)"; flow:established,to_server; content:"User-Agent|3a| Mozilla/1.0
(compatible|3b| MSIE 8.0|3b|"; fast_pattern:12,20; http_header; threshold: type limit, count 2, track by_src,
seconds 300; classtype:trojan-activity; sid:2008913; rev:10; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (xr -
```

```
Worm.Win32.VB.cj related)"; flow:established,to_server; content:"User-Agent|3a| xr|0d 0a|"; http_header;
threshold: type limit, count 2, track by_src, seconds 300; classtype:trojan-activity; sid:2008914; rev:10;
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Yandesk)";
flow:established,to_server; content:"User-Agent|3a| Yandesk|0d 0a|"; http_header; threshold: type limit, count 2,
track by_src, seconds 300; classtype:trojan-activity; sid:2008916; rev:8; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent pricers.info
related (section)"; flow:established,to_server; content:"User-Agent|3a| sections|0d 0a|"; http_header; threshold:
type limit, count 2, track by_src, seconds 300; classtype:trojan-activity; sid:2008919; rev:8;
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (HELLO)";
flow:established,to_server; content:"User-Agent|3a| HELLO|0d 0a|"; http_header; nocase; threshold: type limit,
count 2, track by_src, seconds 300; classtype:trojan-activity; sid:2008941; rev:10; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (IE/1.0)";
flow:to_server,established; content:"User-Agent|3a| IE/1.0|0d 0a|"; http_header; threshold: type limit, count 2,
track by_src, seconds 300; classtype:trojan-activity; sid:2008956; rev:8; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent
(runUpdater.html)"; flow:established,to_server; content:"User-Agent|3a| runUpdater|2e|html"; http_header;
threshold: type limit, count 2, track by_src, seconds 300; classtype:trojan-activity; sid:2009355; rev:8;
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (runPatch.html)";
flow:established,to_server; content:"User-Agent|3a| runPatch|2e|html"; http_header; threshold: type limit, count
2, track by_src, seconds 300; classtype:trojan-activity; sid:2009356; rev:8; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Session) -
Possible Trojan-Clicker"; flow:established,to_server; content:"User-Agent|3a| Session|0d 0a|"; nocase;
http_header; threshold: type limit, count 2, track by_src, seconds 300; classtype:trojan-activity; sid:2009512;
rev:9; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Poker)";
flow:to_server,established; content:"User-Agent|3a| Poker|0d 0a|"; http_header; threshold: type limit, count 2,
track by_src, seconds 300; reference:url,vil.nai.com/vil/content/v_130975.htm; classtype:trojan-activity;
sid:2009534; rev:8; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30,
deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Loands) -
Possible Trojan Downloader GET Request"; flow:established,to_server; content:"User-Agent\: Loands|0d 0a|";
http_header; nocase; threshold: type limit, count 2, track by_src, seconds 300; classtype:trojan-activity;
sid:2009537; rev:6; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30,
deployment Perimeter, signature_severity Major, tag User_Agent, tag Trojan_Downloader, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (ms_ie) -
Crypt.ZPACK Gen Trojan Downloader GET Request"; flow:established,to_server; content:"User-Agent\: ms_ie|0d 0a|";
```

```
http_header; nocase; threshold: type limit, count 2, track by_src, seconds 300; classtype:trojan-activity;
sid:2009538; rev:6; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30,
deployment Perimeter, signature_severity Major, tag User_Agent, tag Trojan_Downloader, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent filled with
System Details - GET Request"; flow:established,to_server; content:"GET"; nocase; http_method; content:"User-
Agent|3a| mac="; http_header; nocase; content:"&hdid="; nocase; http_header; content:"&wlid="; nocase;
content:"&start="; nocase; content:"&os="; nocase; content:"&mem="; nocase; content:"&alive"; nocase;
content:"&ver="; nocase; content:"&mode="; nocase; content:"&guid"; content:"&install="; nocase; content:"&auto=";
nocase; content:"&serveid"; nocase; content:"&area="; nocase; depth:400; classtype:trojan-activity; sid:2009541;
rev:7; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (InHold) -
Possible Trojan Downloader GET Request"; flow:established,to_server; content:"User-Agent|3a| InHold|0d 0a|";
http_header; nocase; threshold: type limit, count 2, track by_src, seconds 300; classtype:trojan-activity;
sid:2009544; rev:7; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30,
deployment Perimeter, signature_severity Major, tag User_Agent, tag Trojan_Downloader, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Forthgoner) -
Possible Trojan Downloader GET Request"; flow:established,to_server; content:"User-Agent\: Forthgoner|0d 0a|";
http_header; nocase; threshold: type limit, count 2, track by_src, seconds 300; classtype:trojan-activity;
sid:2009547; rev:6; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30,
deployment Perimeter, signature_severity Major, tag User_Agent, tag Trojan_Downloader, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (INet)";
flow:established,to_server; content:"User-Agent|3a| INet|0d 0a|"; http_header; threshold: type limit, count 2,
track by_src, seconds 300; classtype:trojan-activity; sid:2009703; rev:8; metadata:affected_product Any,
attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag
User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS User-Agent (STEROID Download)";
flow:established,to_server; content:"User-Agent|3a| STEROID Download|0D 0A|"; nocase; http_header;
reference:url,anubis.iseclab.org/?action=result&task_id=17b118a86edba30f4f588db66eaf55d10;
reference:url,security.thejoshmeister.com/2009/09/new-malware-ddos-botexe-etc-and.html; classtype:trojan-activity;
sid:2009994; rev:7; metadata:created_at 2010_07_30, signature_severity Major, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS WindowsEnterpriseSuite FakeAV User-
Agent TALWinHttpClient"; flow:established,to_server; content:"User-Agent|3a| Mozilla/3.0(compatible|3b|
TALWinHttpClient)|0d 0a|"; http_header; fast_pattern:21,19; reference:md5,d9bcb4e4d650a6ed4402fab8f9ef1387;
classtype:trojan-activity; sid:2010261; rev:5; metadata:created_at 2010_07_30, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Win32.OnLineGames User-Agent (BigFoot)";
flow:to_server,established; content:"User-Agent|3a| BigFoot"; nocase; http_header; classtype:trojan-activity;
sid:2010678; rev:6; metadata:created_at 2010_07_30, signature_severity Major, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Nine Ball User-Agent Detected
(NQX315)"; flow:established,to_server; content:"User-Agent|3a| NQX315|0d 0a|"; http_header; classtype:trojan-
activity; sid:2011188; rev:5; metadata:created_at 2010_07_30, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Si25f_302 User-Agent";
flow:established,to_server; content:"User-Agent|3a| Si25"; http_header; classtype:trojan-activity; sid:2012310;
rev:4; metadata:created_at 2011_02_14, signature_severity Major, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Presto)";
flow:established,to_server; content:"User-Agent|3a| Opera/10.60 Presto/2.2.30"; http_header; content:!"Accept";
http_header; classtype:trojan-activity; sid:2012491; rev:8; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2011_03_12, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at
2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent Im Luo";
```

```
flow:established,to_server; content:"User-Agent|3A| Im|27|Luo"; http_header; classtype:trojan-activity;
sid:2012586; rev:5; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2011_03_28,
deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS MacShield User-Agent Likely Malware";
flow:established,to_server; content:"User-Agent|3a 20|MacShield"; http_header;
reference:url,blog.spiderlabs.com/2011/06/analysis-and-evolution-of-macdefender-os-x-fake-av-scareware.html;
classtype:trojan-activity; sid:2012959; rev:3; metadata:created_at 2011_06_09, signature_severity Major,
updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Long Fake wget 3.0 User-Agent Detected";
flow:established,to_server; content:"User-Agent|3a|"; http_header; content:"wget 3.0"; fast_pattern; distance:10;
within:100; http_header; classtype:trojan-activity; sid:2013178; rev:3; metadata:created_at 2011_07_04,
signature_severity Major, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Ufasoft bitcoin Related User-Agent";
flow:established,to_server; content:"User-Agent|3A 20|Ufasoft"; http_header; classtype:trojan-activity;
sid:2013391; rev:3; metadata:created_at 2011_08_10, signature_severity Major, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent _updater_agent";
flow:established,to_server; content:"User-Agent|3A 20|_updater_agent"; http_header; classtype:trojan-activity;
sid:2013395; rev:2; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2011_08_10,
deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (GUIDTracker)";
flow:to_server,established; content:"User-Agent|3a| GUIDTracker"; http_header;
reference:md5,7a8807f4de0999dba66a8749b2366def; classtype:trojan-activity; sid:2013455; rev:2;
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2011_08_24, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Downloader User-Agent HTTPGET";
flow:established,to_server; content:"User-Agent|3A 20|HTTPGET"; http_header; content:!"autodesk.com|0d 0a|";
http_header; content:!"rsa.com"; http_header; content:!"consumersentinel.gov"; http_header;
content:!"technet.microsoft.com"; http_header; content:!"metropolis.com"; http_header;
content:!"www.catalog.update.microsoft.com|0d|"; http_header; classtype:trojan-activity; sid:2013508; rev:9;
metadata:created_at 2011_08_31, signature_severity Major, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (MadeByLc)";
flow:established,to_server; content:"User-Agent|3A 20|MadeBy"; http_header; classtype:trojan-activity;
sid:2013512; rev:3; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2011_08_31,
deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (windsoft)";
flow:established,to_server; content:"User-Agent|3a| WindSoft|0d 0a|"; http_header; classtype:trojan-activity;
sid:2013561; rev:3; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2011_09_12,
deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS W32/OnlineGames User-Agent (LockXLS)";
flow:established,to_server; content:"User-Agent|3A 20|LockXLS"; http_header; classtype:trojan-activity;
sid:2013724; rev:2; metadata:created_at 2011_10_01, signature_severity Major, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Win32/OnLineGames User-Agent
(Revolution Win32)"; flow:established,to_server; content:"User-Agent|3A 20|Revolution|20 28|Win32|29|";
http_header; classtype:trojan-activity; sid:2013725; rev:2; metadata:created_at 2011_10_01, updated_at
2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (FULLSTUFF)";
flow: established,to_server; content:"User-Agent|3A| FULLSTUFF"; nocase; http_header;
reference:url,threatexpert.com/reports.aspx?find=mrb.mail.ru; classtype:trojan-activity; sid:2013880; rev:4;
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2011_11_08, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2017_10_30;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (NateFinder)";
flow:to_server,established; content:"User-Agent|3a| NateFinder"; http_header; classtype:trojan-activity;
sid:2013881; rev:3; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2011_11_08,
deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (webfile)";
flow:to_server,established; content:"User-Agent|3a| webfile"; http_header;
reference:url,threatexpert.com/reports.aspx?find=upsh.playmusic.co.kr; classtype:trojan-activity; sid:2013883;
rev:3; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2011_11_08, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (DARecover)";
flow:to_server,established; content:"User-Agent|3a| DARecover"; http_header;
reference:url,threatexpert.com/reports.aspx?find=clients.mydealassistant.com; classtype:trojan-activity;
sid:2013884; rev:3; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2011_11_08,
deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (HardCore Software
For)"; flow:to_server,established; content:"User-Agent|3a| HardCore Software For"; http_header; nocase;
classtype:trojan-activity; sid:2018608; rev:3; metadata:affected_product Any, attack_target Client_Endpoint,
created_at 2011_07_06, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2017_10_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS WildTangent User-Agent (WT Games App)";
flow:established,to_server; content:"|0d 0a|WT-User-Agent|3a 20|WT|20|Games|20|App|20|"; http_header;
classtype:policy-violation; sid:2021384; rev:2; metadata:created_at 2015_07_07, updated_at 2017_11_27;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS MtGox Leak wallet stealer UA";
flow:established,to_server; content:"User-Agent|3a 20|MtGoxBackOffice"; fast_pattern:only; http_header;
reference:url,www.securelist.com/en/blog/8196/Analysis_of_Malware_from_the_MtGox_leak_archive;
reference:md5,c4e99fdcd40bee6eb6ce85167969348d; classtype:trojan-activity; sid:2018279; rev:2; metadata:created_at
2014_03_14, updated_at 2017_11_28;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (=Mozilla)";
flow:established,to_server; content:"User-Agent|3a|=Mozilla/5"; http_header; fast_pattern:1,20; classtype:trojan-
activity; sid:2025456; rev:2; metadata:affected_product Web_Browsers, attack_target Client_and_Server, created_at
2018_03_27, deployment Perimeter, performance_impact Low, signature_severity Major, updated_at 2018_03_27;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (InfoBot)";
flow:to_server,established; content:"User-Agent|3a| InfoBot"; http_header; nocase; classtype:trojan-activity;
sid:2011276; rev:9; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30,
deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2018_05_16;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET USER_AGENTS VPNFilter Related UA (Gemini/2.0)";
flow:established,to_server; content:"User-Agent|3a 20|Gemini/2.0|0d 0a|"; http_header; fast_pattern:4,20;
reference:url,twitter.com/m0rb/status/1021626709307805696; classtype:trojan-activity; sid:2025889; rev:2;
metadata:attack_target Server, created_at 2018_07_25, deployment Perimeter, malware_family VPNFilter,
performance_impact Low, signature_severity Major, updated_at 2018_07_25;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET USER_AGENTS VPNFilter Related UA (Hakai/2.0)";
flow:established,to_server; content:"User-Agent|3a 20|Hakai/2.0|0d 0a|"; http_header; fast_pattern:3,20;
reference:url,twitter.com/m0rb/status/1021626709307805696; classtype:trojan-activity; sid:2025890; rev:2;
metadata:attack_target Server, created_at 2018_07_25, deployment Perimeter, malware_family VPNFilter,
performance_impact Low, signature_severity Major, updated_at 2018_07_25;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (HTTP_CONNECT_)";
flow:established,to_server; content:"User-Agent|3a| HTTP_Connect_"; http_header; classtype:bad-unknown;
sid:2007821; rev:5; metadata:attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter,
signature_severity Minor, tag Spyware_User_Agent, updated_at 2018_08_15;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS MSIL/Peppy User-Agent";
```

```
flow:established,to_server; content:"User-Agent|3a 20|onedru/"; http_header; fast_pattern;
reference:md5,ebffb046d0e12b46ba5f27c0176b01c5; classtype:trojan-activity; sid:2026101; rev:2;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at
2018_09_07, deployment Perimeter, malware_family Peppy, performance_impact Moderate, signature_severity Major,
updated_at 2018_09_07;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS VPNFilter Related UA (curl53)";
flow:established,to_server; content:"-Agent|3a 20|curl53|0d 0a|"; http_header; fast_pattern; isdataat:!1,relative;
reference:url,blog.talosintelligence.com/2018/09/vpnfilter-part-3.html; classtype:trojan-activity; sid:2026428;
rev:2; metadata:affected_product Linux, attack_target Networking_Equipment, created_at 2018_10_01, deployment
Perimeter, malware_family VPNFilter, signature_severity Major, updated_at 2018_10_01;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Windows XP)";
flow:to_server,established; content:"User-Agent|3a 20|Windows XP"; http_header; classtype:bad-unknown;
sid:2026519; rev:2; metadata:affected_product Web_Browsers, attack_target Client_Endpoint, created_at 2018_10_18,
deployment Perimeter, signature_severity Minor, updated_at 2018_10_18;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Windows 7)";
flow:to_server,established; content:"User-Agent|3a 20|Windows 7"; http_header; classtype:bad-unknown; sid:2026522;
rev:2; metadata:affected_product Web_Browsers, attack_target Client_Endpoint, created_at 2018_10_18, deployment
Perimeter, signature_severity Minor, updated_at 2018_10_18;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Windows 10)";
flow:to_server,established; content:"User-Agent|3a 20|Windows 10"; http_header; content:!"google-analytics.com|0d
0a|"; http_header; classtype:bad-unknown; sid:2026521; rev:3; metadata:affected_product Web_Browsers,
attack_target Client_Endpoint, created_at 2018_10_18, deployment Perimeter, signature_severity Minor, updated_at
2018_10_22;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious UA Observed (IEhook)";
flow:established,to_server; content:"User-Agent|3a 20|IEhook|0d|"; http_header; fast_pattern;
reference:md5,f0483493bcb352bd2f474b52f3b2f273; classtype:trojan-activity; sid:2026558; rev:2;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at
2018_10_26, deployment Perimeter, performance_impact Low, signature_severity Minor, tag User_Agent, updated_at
2018_10_26;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Peppy/KeeOIL Google User-Agent
(google/dance)"; flow:established,to_server; content:"User-Agent|3a 20|google/dance|0d|"; http_header;
fast_pattern:12,13; reference:url,www.malcrawler.com/team-simbaa-targets-indian-government-using-united-nations-
military-observers-themed-malware-nicked-named-keeoil/; classtype:trojan-activity; sid:2026883; rev:2;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at
2019_02_05, deployment Perimeter, malware_family Peppy, malware_family KeeOIL, performance_impact Low,
signature_severity Major, updated_at 2019_02_05;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Peppy/KeeOIL User-Agent (ekeoil)";
flow:established,to_server; content:"User-Agent|3a 20|ekeoil/"; http_header; fast_pattern:12,7;
reference:url,www.malcrawler.com/team-simbaa-targets-indian-government-using-united-nations-military-observers-
themed-malware-nicked-named-keeoil/; classtype:trojan-activity; sid:2026885; rev:2; metadata:affected_product
Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2019_02_05, deployment
Perimeter, malware_family Peppy, malware_family KeeOIL, performance_impact Low, signature_severity Major,
updated_at 2019_02_05;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (SomeTimes)";
flow:established,to_server; content:"User-Agent|3a 20|SomeTimes|0d|"; http_header; fast_pattern;
reference:md5,a86d4e17389a37bfc291f4a8da51a9b8; classtype:trojan-activity; sid:2026898; rev:2;
metadata:attack_target Client_Endpoint, created_at 2019_02_11, deployment Perimeter, performance_impact Low,
signature_severity Minor, tag User_Agent, updated_at 2019_02_11;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS SFML User-Agent (libsfml-network)";
flow:established,to_server; content:"User-Agent|3a 20|libsfml-network/"; http_header; fast_pattern:8,20;
reference:url,github.com/SFML; classtype:trojan-activity; sid:2026914; rev:2; metadata:affected_product
Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2019_02_14, deployment
```

```
Perimeter, performance_impact Low, signature_severity Minor, updated_at 2019_02_14;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Clever Internet
Suite)"; flow:established,to_server; content:"User-Agent|3a 20|"; http_header; content:"Clever Internet Suite";
http_header; distance:0; classtype:trojan-activity; sid:2027045; rev:2; metadata:affected_product
Windows_XP_Vista_7_8_10_Server_32_64_Bit, created_at 2019_03_05, deployment Perimeter, performance_impact Low,
signature_severity Major, updated_at 2019_03_05;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA (Mozilla 6.0)";
flow:established,to_server; content:"User-Agent|3a 20|Mozilla 6.0|0d 0a|"; http_header; fast_pattern:5,20;
classtype:bad-unknown; sid:2027142; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit,
attack_target Client_Endpoint, created_at 2019_04_01, deployment Perimeter, performance_impact Low,
signature_severity Minor, updated_at 2019_04_01;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS ESET Installer";
flow:established,to_server; content:"User-Agent|3a 20|ESET Installer|0d 0a|"; http_header; fast_pattern:12,14;
threshold: type limit, track by_src, seconds 180, count 1; classtype:policy-violation; sid:2027219; rev:2;
metadata:attack_target Client_Endpoint, created_at 2019_04_17, deployment Perimeter, performance_impact Low,
signature_severity Minor, tag PUA, updated_at 2019_04_17;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Aria2 User-Agent";
flow:to_server,established; content:"User-Agent|3a 20|aria2/"; http_header; fast_pattern;
reference:url,github.com/aria2/aria2; reference:md5,eb042fe28b8a235286df2c7f4ed1d8a8; classtype:trojan-activity;
sid:2027286; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target
Client_Endpoint, created_at 2019_04_25, deployment Perimeter, signature_severity Minor, updated_at 2019_04_25;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Node XMLHTTP User-Agent";
flow:established,to_server; content:"User-Agent|3a 20|node-XMLHttpRequest|0d 0a|"; http_header; fast_pattern;
classtype:unknown; sid:2027388; rev:2; metadata:affected_product Web_Browsers, attack_target Client_Endpoint,
created_at 2019_05_28, deployment Perimeter, performance_impact Low, signature_severity Minor, updated_at
2019_05_28;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Microsoft Device Metadata Retrieval
Client User-Agent"; flow:established,to_server; content:"User-Agent|3a
20|MICROSOFT_DEVICE_METADATA_RETRIEVAL_CLIENT|0d 0a|"; http_header; fast_pattern; classtype:misc-activity;
sid:2027390; rev:2; metadata:affected_product Web_Browsers, attack_target Client_Endpoint, created_at 2019_05_28,
deployment Perimeter, performance_impact Low, signature_severity Informational, updated_at 2019_05_28;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET USER_AGENTS Suspicious UA Observed (YourUserAgent)";
flow:established,to_server; content:"User-Agent|3a 20|YourUserAgent|0d|"; http_header; fast_pattern:6,20;
reference:md5,c1ca718e7304bf28b5c96559cbf69a06; classtype:bad-unknown; sid:2027484; rev:2; metadata:created_at
2019_06_17, deployment Perimeter, performance_impact Low, signature_severity Minor, updated_at 2019_06_17;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA (Hello, World)";
flow:established,to_server; content:"User-Agent|3a 20|Hello, World|0d 0a|"; http_header; fast_pattern:6,20;
classtype:bad-unknown; sid:2027503; rev:2; metadata:affected_product Any, attack_target Client_Endpoint,
created_at 2019_06_21, deployment Perimeter, performance_impact Low, signature_severity Informational, updated_at
2019_06_21;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA (Hello-World)";
flow:established,to_server; content:"User-Agent|3a 20|Hello-World|0d 0a|"; http_header; fast_pattern:5,20;
classtype:bad-unknown; sid:2027504; rev:2; metadata:affected_product Any, attack_target Client_Endpoint,
created_at 2019_06_21, deployment Perimeter, performance_impact Low, signature_severity Informational, updated_at
2019_06_21;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Fake Mozilla User-Agent String Observed
(M0zilla)"; flow:established,to_server; content:"User-Agent|3a 20|M0zilla|2f|"; http_header; fast_pattern;
content:"."; http_header; distance:1; within:1; reference:md5,c6c1292bf7dd1573b269afb203134b1d; classtype:trojan-
activity; sid:2027565; rev:2; metadata:created_at 2019_06_26, signature_severity Major, updated_at 2019_06_26;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious UA Observed (Ave, Caesar!)";
```

```
flow:established,to_server; content:"User-Agent|3a 20|Ave,|20|Caesar!|0d|"; http_header; fast_pattern:12,13;
classtype:bad-unknown; sid:2027648; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit,
created_at 2019_06_28, deployment Perimeter, performance_impact Low, signature_severity Major, updated_at
2019_06_28;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA (zwt)";
flow:established,to_server; content:"User-Agent|3a 20|zwt|0d 0a|"; http_header; classtype:bad-unknown;
sid:2027649; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target
Client_Endpoint, created_at 2019_07_01, deployment Perimeter, performance_impact Low, signature_severity
Informational, updated_at 2019_07_01;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA (My Agent)";
flow:established,to_server; content:"User-Agent|3a 20|My Agent|0d 0a|"; http_header; fast_pattern:2,20;
classtype:bad-unknown; sid:2027650; rev:2; metadata:attack_target Client_Endpoint, created_at 2019_07_01,
deployment Perimeter, performance_impact Low, signature_severity Informational, updated_at 2019_07_01;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious Custom Firefox UA Observed
(Firefox...)"; flow:established,to_server; content:"User-Agent|3a 20|Firefox...|0d|"; http_header;
fast_pattern:2,20; classtype:bad-unknown; sid:2027686; rev:2; metadata:created_at 2019_07_04, deployment
Perimeter, performance_impact Low, signature_severity Minor, updated_at 2019_07_04;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS User-Agent (single dash)";
flow:to_server,established; content:"User-Agent|3a| |2d 0d 0a|"; http_header; classtype:trojan-activity;
sid:2007880; rev:6; metadata:created_at 2010_07_30, signature_severity Major, updated_at 2019_07_16;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious UA Observed (Quick Macros)";
flow:established,to_server; content:"User-Agent|3a 20|Quick|20|Macros|0d|"; http_header; fast_pattern:5,20;
reference:md5,aa682f5d4a17307539a2bc7048be0745; classtype:trojan-activity; sid:2027755; rev:2; metadata:created_at
2019_07_24, deployment Perimeter, performance_impact Low, signature_severity Minor, updated_at 2019_07_24;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (agent)"; flow:
to_server,established; content:"User-Agent|3a| agent"; http_header; content:!".battle.net"; http_header;
content:".blizzard.com|0d|"; http_header; content:!"Host|3a 20|blz"; http_header;
content:!"cn.patch.battlenet.com.cn"; http_header; classtype:trojan-activity; sid:2001891; rev:20;
metadata:created_at 2010_07_30, signature_severity Major, updated_at 2019_08_05;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA (NSIS_Inetc
(Mozilla))"; flow:to_server,established; content:"User-Agent|3a 20|NSIS|5f|Inetc|20 28|Mozilla|29|"; http_header;
classtype:bad-unknown; sid:2011227; rev:4; metadata:attack_target Client_Endpoint, created_at 2010_07_30,
deployment Perimeter, signature_severity Minor, updated_at 2019_08_07;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious Generic Style UA Observed
(My_App)"; flow:established,to_server; content:"User-Agent|3a 20|My_App|0d|"; http_header; fast_pattern;
reference:md5,2978dbadd8fda7d842298fbd476b47b2; classtype:trojan-activity; sid:2027833; rev:2;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, created_at 2019_08_09, updated_at 2019_08_09;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (Microsoft
Internet Explorer)"; flow: to_server,established; content:"User-Agent|3a| Microsoft Internet Explorer";
fast_pattern:11,25; http_header; content:!"bbc.co.uk|0d 0a|"; nocase; http_header; content:!"vmware.com|0d 0a|";
nocase; http_header; content:!"rc.itsupport247.net|0d 0a|"; nocase; http_header; content:!"msn.com|0d 0a|";
nocase; http_header; content:!"msn.es|0d 0a|"; nocase; http_header; content:!"live.com|0d 0a|"; nocase;
http_header; content:!"gocyberlink.com|0d 0a|"; nocase; http_header; content:!"ultraedit.com|0d 0a|"; nocase;
http_header; content:!"windowsupdate.com"; http_header; content:!"cyberlink.com"; http_header;
content:!"lenovo.com"; http_header; content:!"itsupport247.net|0d 0a|"; nocase; http_header;
content:!"msn.co.uk|0d 0a|"; http_header; content:!"support.weixin.qq.com"; http_header; threshold:type limit,
track by_src, count 2, seconds 360; classtype:trojan-activity; sid:2002400; rev:35; metadata:created_at
2010_07_30, signature_severity Major, updated_at 2019_08_13;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS User-Agent (_TEST_)"; flow:
to_server,established; content:"User-Agent|3a| _TEST_"; nocase; http_header; classtype:unknown; sid:2009545;
rev:7; metadata:created_at 2010_07_30, updated_at 2019_08_14;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA (Chrome)";
flow:established,to_server; content:"User-Agent|3a 20|Chrome|0d 0a|"; http_header; fast_pattern; classtype:bad-
unknown; sid:2027916; rev:2; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2019_08_26,
deployment Perimeter, performance_impact Low, signature_severity Informational, updated_at 2019_08_26, reviewed_at
2024_02_20;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA (Absent)";
flow:established,to_server; content:"User-Agent|3a 20|Absent|0d 0a|"; http_header; fast_pattern:0,20;
classtype:bad-unknown; sid:2028571; rev:2; metadata:affected_product Any, attack_target Client_Endpoint,
created_at 2019_09_12, deployment Perimeter, performance_impact Low, signature_severity Informational, updated_at
2019_09_12;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Steam HTTP Client User-Agent";
flow:established,to_server; content:"User-Agent|3a 20|Valve/Steam HTTP Client"; http_header; nocase; threshold:
type limit, track by_src, count 1, seconds 300; classtype:policy-violation; sid:2028651; rev:3;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at
2019_10_07, deployment Perimeter, signature_severity Informational, updated_at 2019_10_16;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Microsoft Dr Watson User-Agent (MSDW)";
flow:established,to_server; content:"User-Agent|3a 20|MSDW|0d 0a|"; http_header; fast_pattern; threshold: type
limit, track by_src, count 1, seconds 300; classtype:unknown; sid:2027389; rev:3; metadata:affected_product
Web_Browsers, attack_target Client_Endpoint, created_at 2019_05_28, deployment Perimeter, performance_impact Low,
signature_severity Minor, updated_at 2019_10_16;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA (IExplorer 34)";
flow:established,to_server; content:"User-Agent|3a 20|IExplorer 34|0d 0a|"; http_header; fast_pattern:6,20;
classtype:bad-unknown; sid:2028834; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit,
attack_target Client_Endpoint, created_at 2019_10_16, deployment Perimeter, performance_impact Low,
signature_severity Minor, updated_at 2019_10_16;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (reqwest/)";
flow:established,to_server; content:"User-Agent|3a 20|"; http_header; nocase; content:"reqwest/"; http_header;
distance:0; fast_pattern; reference:md5,be59ae5fab354d29e53f11a08d805db7; classtype:bad-unknown; sid:2028842;
rev:2; metadata:attack_target Client_Endpoint, created_at 2019_10_16, deployment Perimeter, performance_impact
Low, signature_severity Informational, updated_at 2019_10_16;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA (Windows)";
flow:established,to_server; content:"User-Agent|3a 20|Windows|0d 0a|"; http_header; fast_pattern:1,20;
classtype:bad-unknown; sid:2028879; rev:2; metadata:affected_product Any, attack_target Client_Endpoint,
created_at 2019_10_21, deployment Perimeter, performance_impact Low, signature_severity Minor, updated_at
2019_10_21;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Steam HTTP Client User-Agent";
flow:established,to_server; content:"User-Agent|3a 20|SteamHTTPClient|0d 0a|"; http_header; threshold: type limit,
track by_src, count 1, seconds 300; classtype:policy-violation; sid:2028650; rev:3; metadata:affected_product
Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2019_10_07, deployment
Perimeter, signature_severity Informational, updated_at 2019_10_22;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA (Client)";
flow:established,to_server; content:"User-Agent|3a 20|Client|0d 0a|"; http_header; fast_pattern; classtype:bad-
unknown; sid:2028912; rev:2; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2019_10_28,
deployment Perimeter, signature_severity Informational, updated_at 2019_10_28;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Random String)";
flow:established,to_server; content:"User-Agent|3a 20|Random String|0d 0a|"; http_header;
reference:md5,a1e56bd465d1c1b5fc19384a3a7ec461; classtype:bad-unknown; sid:2028947; rev:2; metadata:attack_target
Client_Endpoint, created_at 2019_11_07, deployment Perimeter, performance_impact Low, signature_severity
Informational, updated_at 2019_11_07;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA
```

```
(system_file/2.0)"; flow:established,to_server; content:"User-Agent|3a 20|system_file/2.0|0d 0a|"; http_header;
fast_pattern:9,20; classtype:bad-unknown; sid:2028983; rev:2; metadata:affected_product Any, attack_target
Client_Endpoint, created_at 2019_11_15, deployment Perimeter, signature_severity Informational, updated_at
2019_11_15;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA (DxD)";
flow:established,to_server; content:"User-Agent|3a 20|DxD|0d 0a|"; http_header; fast_pattern; classtype:bad-
unknown; sid:2029232; rev:2; metadata:attack_target Client_Endpoint, created_at 2020_01_06, deployment Perimeter,
performance_impact Low, signature_severity Minor, updated_at 2020_01_06;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS ABBCCoin Activity Observed";
flow:established,to_server; content:"User-Agent|3a 20|ABBCCoin"; fast_pattern; http_header;
reference:md5,77ec579347955cfa32f219386337f5bb; classtype:misc-activity; sid:2029423; rev:2;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at
2020_02_12, deployment Perimeter, signature_severity Minor, updated_at 2020_02_12;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (VB OpenUrl)";
flow:to_server,established; content:"User-Agent|3a 20|VB OpenURL|0d 0a|"; http_header; classtype:bad-unknown;
sid:2029544; rev:2; metadata:attack_target Client_Endpoint, created_at 2020_02_27, deployment Perimeter,
signature_severity Informational, updated_at 2020_02_27;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA (\xa4)";
flow:established,to_server; content:"|0d 0a|User-Agent|3a 20 a4 0d 0a|"; fast_pattern; http_header; classtype:bad-
unknown; sid:2029554; rev:2; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2020_03_02,
deployment Perimeter, signature_severity Minor, updated_at 2020_03_02;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA (easyhttp
client)"; flow:established,to_server; content:"User-Agent|3a 20|easyhttp client|0d 0a|"; http_header;
fast_pattern:9,20; classtype:bad-unknown; sid:2029569; rev:2; metadata:attack_target Client_Endpoint, created_at
2020_03_04, deployment Perimeter, signature_severity Informational, updated_at 2020_03_04;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (explorersvc)";
flow:established,to_server; content:"User-Agent|3a 20|explorersvc|0d 0a|"; http_header; classtype:bad-unknown;
sid:2029749; rev:2; metadata:attack_target Client_Endpoint, created_at 2020_03_27, deployment Perimeter,
signature_severity Informational, updated_at 2020_03_27;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (KtulhuBrowser)";
flow:established,to_server; content:"User-Agent|3a 20|KtulhuBrowser|0d 0a|"; http_header; nocase; classtype:bad-
unknown; sid:2029750; rev:2; metadata:attack_target Client_Endpoint, created_at 2020_03_27, deployment Perimeter,
signature_severity Informational, updated_at 2020_03_27;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA (xPCAP)";
flow:established,to_server; content:"User-Agent|3a 20|xPCAP|0d 0a|"; http_header; fast_pattern; classtype:bad-
unknown; sid:2029748; rev:2; metadata:attack_target Client_Endpoint, created_at 2020_03_27, deployment Perimeter,
signature_severity Informational, updated_at 2020_03_27;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA (Http-connect)";
flow:established,to_server; content:"User-Agent|3a 20|Http-connect|0d 0a|"; http_header; fast_pattern:6,20;
classtype:bad-unknown; sid:2029752; rev:2; metadata:affected_product Any, attack_target Client_Endpoint,
created_at 2020_03_30, deployment Perimeter, signature_severity Informational, updated_at 2020_03_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Shadowcoin Cryptocurrency UA Observed";
flow:established,to_server; content:"User-Agent|3a 20|ShadowCoin"; http_header; fast_pattern; classtype:misc-
activity; sid:2029771; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target
Client_Endpoint, created_at 2020_03_31, deployment Perimeter, signature_severity Minor, updated_at 2020_03_31;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Willowcoin Cryptocurrency UA Observed";
flow:established,to_server; content:"User-Agent|3a 20|WillowCoin"; http_header; fast_pattern; classtype:misc-
activity; sid:2029772; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target
Client_Endpoint, created_at 2020_03_31, deployment Perimeter, signature_severity Minor, updated_at 2020_03_31;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Malicious CASPER/Mirai UA";
flow:established,to_server; content:"|0d 0a|User-Agent|3a 20|Mozilla/4.0   (compatible|3b|   MSIE   5.01|3b|
Windows   NT   5.0)|0d 0a|"; fast_pattern:35,20; http_header;
reference:url,www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-decade-of-the-
rats.pdf; reference:md5,ea78869555018cdab3699e2df5d7e7f8; classtype:misc-activity; sid:2029892; rev:2;
metadata:created_at 2020_04_13, updated_at 2020_04_13;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA (PhoneMonitor)";
flow:established,to_server; content:"User-Agent|3a 20|PhoneMonitor|0d 0a|"; http_header;
reference:md5,09aa3bb05a55b0df864d1e1709c29960; reference:url,blog.trendmicro.com/trendlabs-security-
intelligence/coronavirus-update-app-leads-to-project-spy-android-and-ios-spyware/; classtype:trojan-activity;
sid:2029980; rev:2; metadata:attack_target Mobile_Client, created_at 2020_04_20, performance_impact Low,
signature_severity Major, updated_at 2020_04_20;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS BeeMovie Related Activity";
flow:to_server,established; content:"User-Agent|3a 20|BeeMovie/"; http_header; classtype:misc-activity;
sid:2030050; rev:2; metadata:affected_product Android, attack_target Client_Endpoint, created_at 2020_04_29,
deployment Perimeter, signature_severity Minor, updated_at 2020_04_29;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA (h55u4u4u5uii5)";
flow:established,to_server; content:"User-Agent|3a 20|h55u4u4u5uii5|0d 0a|"; http_header;
reference:url,www.welivesecurity.com/2020/04/28/grandoreiro-how-engorged-can-exe-get/; classtype:trojan-activity;
sid:2030058; rev:2; metadata:attack_target Client_Endpoint, created_at 2020_04_29, deployment Perimeter,
performance_impact Low, signature_severity Major, updated_at 2020_04_29;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Possible QBot User-Agent";
flow:established,to_server; content:"User-Agent|3a 20|MelindaMelinda|0d 0a|"; http_header;
reference:md5,d5129d51bf982b055ee00fe7ef4da3c0; classtype:trojan-activity; sid:2030149; rev:2; metadata:created_at
2020_05_11, signature_severity Major, updated_at 2020_05_11;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA (CODE)";
flow:established,to_server; content:"User-Agent|3a 20|CODE|0d 0a|"; http_header; fast_pattern;
reference:md5,f5ee4c57897687586202c15e98997ed; classtype:bad-unknown; sid:2030439; rev:2;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at
2020_07_01, deployment Perimeter, signature_severity Informational, updated_at 2020_07_01;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA (grab)";
flow:established,to_server; content:"User-Agent|3a 20|grab|0d 0a|"; http_header; fast_pattern; classtype:bad-
unknown; sid:2030492; rev:2; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2020_07_10,
deployment Perimeter, signature_severity Informational, updated_at 2020_07_10;)

alert tcp $EXTERNAL_NET any -> any $HTTP_PORTS (msg:"ET USER_AGENTS SAP CVE-2020-6287 PoC UA Observed";
flow:established,to_server; content:"CVE-2020-6287|20|PoC|0d 0a|"; http_header; fast_pattern;
reference:url,github.com/chipik/SAP_RECON/blob/master/RECON.py; classtype:attempted-recon; sid:2030548; rev:2;
metadata:created_at 2020_07_16, cve CVE_2020_6287, performance_impact Low, signature_severity Major, updated_at
2020_07_16;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA (justupdate)";
flow:established,to_server; content:"User-Agent|3a 20|justupdate|0d 0a|"; http_header;
reference:md5,7a814300b204e14467deff69c1159cbe; classtype:bad-unknown; sid:2030556; rev:2; metadata:created_at
2020_07_17, updated_at 2020_07_17;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA (.NET Framework
Client)"; flow:established,to_server; content:"User-Agent|3a 20|.NET Framework Client|0d 0a|"; http_header;
fast_pattern:12,20; classtype:bad-unknown; sid:2030586; rev:2; metadata:affected_product
Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2020_07_24, deployment
Perimeter, signature_severity Informational, updated_at 2020_07_24, reviewed_at 2024_03_05;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious UA (cctv.mtv)";
flow:established,to_server; content:"User-Agent|3a 20|cctv.mtv|0d 0a|"; http_header;
reference:md5,deffb804976c0531144d999ded0df8b9; classtype:bad-unknown; sid:2030598; rev:2; metadata:attack_target
```

Client_Endpoint, created_at 2020_07_27, deployment Perimeter, signature_severity Informational, updated_at 2020_07_27;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (cso)"; flow:established,to_server; content:"User-Agent|3a 20|cso v"; fast_pattern; http_header; pcre:"/User-Agent\x3a\x20cso\x20v[0-9][0-9]?\.[0-9][0-9]?/H"; reference:md5,5640851c35221c3ae7bbde053d1bb38e; reference:url,app.any.run/tasks/d94c1428-253d-432a-be65-53ea3a0505f4/; classtype:trojan-activity; sid:2030600; rev:2; metadata:attack_target Client_Endpoint, created_at 2020_07_27, deployment Perimeter, performance_impact Low, signature_severity Major, updated_at 2020_07_27;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (firefox)"; flow:established,to_server; content:"User-Agent|3a 20|firefox"; fast_pattern; http_header; pcre:"/User-Agent\x3a\x20firefox$/H"; reference:url,unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/; classtype:trojan-activity; sid:2030623; rev:2; metadata:attack_target Client_Endpoint, created_at 2020_07_30, deployment Perimeter, performance_impact Low, signature_severity Informational, updated_at 2020_07_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (chrome)"; flow:established,to_server; content:"User-Agent|3a 20|chrome|0d 0a|"; fast_pattern; http_header; reference:url,unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/; classtype:trojan-activity; sid:2030624; rev:2; metadata:attack_target Client_Endpoint, created_at 2020_07_30, deployment Perimeter, performance_impact Low, signature_severity Informational, updated_at 2020_07_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (MSIE)"; flow:established,to_server; content:"User-Agent|3a 20|MSIE|28|6.00.2900.5512|20 28|"; fast_pattern; http_header; content:"|3b 20|NT|28|"; distance:0; http_header; content:"|29 3b 20|AV|28|"; distance:0; http_header; content:"|29 3b 20|OV|28|"; distance:0; http_header; content:"|29 3b 20|NA|28|"; distance:0; http_header; content:"VR|28|PH"; distance:0; http_header; reference:url,documents.trendmicro.com/assets/Tech-Brief-Tropic-Trooper-s-Back-USBferry-Attack-Targets-Air-gapped-Environments.pdf; classtype:trojan-activity; sid:2030170; rev:3; metadata:attack_target Client_Endpoint, created_at 2020_05_15, deployment Perimeter, performance_impact Low, signature_severity Major, updated_at 2020_08_10;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspected Mekotio User-Agent (MyCustomUser)"; flow:established,to_server; content:"User-Agent|3a 20|MyCustomUser|0d 0a|"; fast_pattern; http_header; reference:url,www.welivesecurity.com/2020/08/13/mekotio-these-arent-the-security-updates-youre-looking-for/; classtype:trojan-activity; sid:2030721; rev:2; metadata:attack_target Client_Endpoint, created_at 2020_08_21, deployment Perimeter, performance_impact Low, signature_severity Major, updated_at 2020_08_21;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspected Mekotio User-Agent (4M5yC6u4stom5U8se3r)"; flow:established,to_server; content:"User-Agent|3a 20|4M5yC6u4stom5U8se3r|0d 0a|"; fast_pattern; http_header; reference:url,www.welivesecurity.com/2020/08/13/mekotio-these-arent-the-security-updates-youre-looking-for/; classtype:trojan-activity; sid:2030722; rev:2; metadata:attack_target Client_Endpoint, created_at 2020_08_21, deployment Perimeter, performance_impact Low, signature_severity Major, updated_at 2020_08_21;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (boostsoftware-urlexists)"; flow:established,to_server; content:"User-Agent|3a 20|boostsoftware-urlexists|0d 0a|"; http_header; classtype:bad-unknown; sid:2030814; rev:2; metadata:attack_target Client_Endpoint, created_at 2020_08_28, deployment Perimeter, performance_impact Low, signature_severity Informational, updated_at 2020_08_28;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Microsoft Malware Protection User-Agent Observed"; flow:to_server,established; content:"User-Agent|3a 20|MpCommunication"; http_header; classtype:misc-activity; sid:2030835; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2020_09_03, deployment Perimeter, signature_severity Major, updated_at 2020_09_04;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Installed OK)"; flow:established,to_server; content:"User-Agent|3a 20|Installed OK"; http_header; nocase; reference:md5,16035440878ec6e93d82c2aeea508630; classtype:bad-unknown; sid:2030880; rev:2; metadata:attack_target Client_Endpoint, created_at 2020_09_15, deployment Perimeter, performance_impact Low, signature_severity Informational, updated_at 2020_09_15;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS User-Agent (Internet Explorer)";

```
flow:to_server,established; content:"User-Agent|3a| Internet Explorer|0d 0a|"; http_header; nocase;
content:!"Host|3a| pnrws.skype.com|0d 0a|"; http_header; content:!"iecvlist.microsoft.com"; http_header;
content:!".lenovo.com|0d 0a|"; http_header; classtype:bad-unknown; sid:2008052; rev:17; metadata:created_at
2010_07_30, updated_at 2020_10_05;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Fire-Cloud)";
flow:established,to_server; content:"User-Agent|3a 20|Fire-Cloud|0d 0a|"; http_header;
reference:md5,804c8f7d3b10b421ab5c09d675644212; classtype:trojan-activity; sid:2031065; rev:2;
metadata:attack_target Client_Endpoint, created_at 2020_10_20, deployment Perimeter, performance_impact Low,
signature_severity Minor, updated_at 2020_10_20;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious HttpSocket User-Agent
Observed"; flow:established,to_server; content:"User-Agent|3a 20|HttpSocket By Xswallow"; http_header;
fast_pattern:12,20; classtype:misc-activity; sid:2031167; rev:2; metadata:affected_product
Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2020_11_03, deployment
Perimeter, signature_severity Major, updated_at 2020_11_03;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious User-Agent
(JWrapperDownloader)"; flow:established,to_server; content:"User-Agent|3a 20|JWrapperDownloader|0d 0a|";
fast_pattern:12,20; http_header; content:!"Referer|3a|"; http_header;
reference:md5,f50cd7bfe5c258c62f74a695e12f4760; classtype:bad-unknown; sid:2049862; rev:2;
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2020_11_16, deployment Perimeter,
signature_severity Informational, updated_at 2023_12_28, former_sid 2845478;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent Simple Bot";
flow:established,to_server; content:"User-Agent|3a 20|Simple Bot v"; fast_pattern; http_header;
reference:md5,3cf04350400299844abb17a0e1640975; classtype:bad-unknown; sid:2031471; rev:2; metadata:attack_target
Client_Endpoint, created_at 2020_12_31, deployment Perimeter, performance_impact Low, signature_severity
Informational, updated_at 2020_12_31;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (aaaa)";
flow:established,to_server; content:"User-Agent|3a 20|aaaa|0d 0a|"; http_header;
reference:md5,61e213e717cc8e156cec79a7c1cd0c64; classtype:bad-unknown; sid:2031613; rev:2; metadata:attack_target
Client_Endpoint, created_at 2021_02_11, deployment Perimeter, signature_severity Informational, updated_at
2021_02_11;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Collection
Info)"; flow:established,to_server; content:"User-Agent|3a 20|Collection Info/1.0|0d 0a|"; fast_pattern;
http_header; reference:md5,864eace6e6f67b77163d7ed5da4498c8;
reference:url,github.com/AmnestyTech/investigations/tree/master/2021-02-24_vietnam;
reference:url,www.amnesty.org/en/latest/research/2021/02/click-and-bait-vietnamese-human-rights-defenders-
targeted-with-spyware-attacks/; classtype:bad-unknown; sid:2031684; rev:2; metadata:created_at 2021_03_01,
performance_impact Low, updated_at 2021_03_01;)

alert tcp any any -> any $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (HaxerMen)";
flow:established,to_server; content:"User-Agent|3a 20|HaxerMen|0d 0a|"; fast_pattern; http_header;
reference:md5,19aa54bd0c5a4b78f47247bb432b689d; classtype:bad-unknown; sid:2032081; rev:2; metadata:attack_target
Client_Endpoint, created_at 2021_03_16, deployment Perimeter, signature_severity Major, updated_at 2021_03_16;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Non-standard User-Agent (PATCHER)";
flow:established,to_server; content:"User-Agent|3a 20|PATCHER|0d 0a|"; http_header; classtype:policy-violation;
sid:2032938; rev:1; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2021_05_11,
deployment Perimeter, signature_severity Informational, updated_at 2021_05_11;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious User-Agent (altera
forma)"; flow:established,to_server; content:"User-Agent|3a 20|altera|20|forma|0d 0a|"; fast_pattern; http_header;
reference:md5,f019d3031c3aaf45dbd3630a33ab0991; classtype:bad-unknown; sid:2032948; rev:1; metadata:attack_target
Client_Endpoint, created_at 2021_05_12, deployment Perimeter, performance_impact Low, signature_severity
Informational, updated_at 2021_05_12;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (MyAgent)";
```

```
flow:to_server,established; content:"User-Agent|3a| MyAgent"; http_header; content:!"Host|3a
20|driverdl.lenovo.com.cn|0d 0a|"; http_header; content:!"www.google-analytics.com"; http_header; threshold: type
limit, count 2, track by_src, seconds 300; classtype:trojan-activity; sid:2005320; rev:13;
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2021_06_15;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS WaterDropX PRISM UA Observed";
flow:established,to_server; content:"agent-waterdropx"; fast_pattern; http_header; pcre:"/^User-
Agent\x3a\x20[^\r\n]+agent-waterdropx/Hmi"; classtype:trojan-activity; sid:2033269; rev:1; metadata:created_at
2021_07_07, malware_family PRISM, signature_severity Major, tag WaterDropX, updated_at 2021_07_07;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Malicious User-Agent (Brute
Force Attacks)"; flow:established,to_server; content:"User-Agent|3a 20|Mozilla/5.0|20|(Windows|20|NT|20|10.0|3b
20|Win64|3b 20|x64)|20|AppleWebKit/537.36|20|(KHTML,|20|like|20|Gecko)|20|Chrome/70.|0d 0a|"; http_header;
reference:url,media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-
21.PDF; classtype:bad-unknown; sid:2033314; rev:1; metadata:created_at 2021_07_12, updated_at 2021_07_12;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Malicious User-Agent (Brute
Force Attacks)"; flow:established,to_server; content:"User-Agent|3a 20|Microsoft|20|Office/14.0|20|
(Windows|20|NT|20|6.1|3b 20|Microsoft|20|Outlook|20|14.0.7162|3b 20|Pro|0d 0a|"; http_header;
reference:url,media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-
21.PDF; classtype:bad-unknown; sid:2033315; rev:1; metadata:created_at 2021_07_12, updated_at 2021_07_12;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS sysWeb User-Agent";
flow:established,to_server; content:"|20|sysWeb/"; fast_pattern; http_header; pcre:"/^User-
Agent\x3a\x20[^\r\n]+\x20sysWeb\//Hmi"; reference:md5,3f295401fa59a32ff7a11551551ec607;
reference:url,twitter.com/starsSk87264403/status/1422543872853426198; classtype:trojan-activity; sid:2033665;
rev:1; metadata:created_at 2021_08_04, performance_impact Low, signature_severity Major, updated_at 2021_08_04;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (REBOL)";
flow:established,to_server; content:"User-Agent|3a 20|REBOL"; http_header; nocase;
reference:url,twitter.com/James_inthe_box/status/1441140639169609736; classtype:bad-unknown; sid:2034021; rev:2;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at
2021_09_24, deployment Perimeter, performance_impact Low, signature_severity Minor, updated_at 2021_09_24;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Embarcadero URI
Client/1.0)"; flow:established,to_server; content:"User-Agent|3a 20|Embarcadero URI Client/1.0|0d 0a|";
http_header; reference:md5,c0e620ed4e96aa1fe8452a3f8b7e2e8d; classtype:bad-unknown; sid:2034244; rev:2;
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2021_10_25, deployment Perimeter,
signature_severity Major, tag User_Agent, updated_at 2021_10_25;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Microsoft-ATL-
Native/9.00)"; flow:established,to_server; content:"Microsoft-ATL-Native/9.00"; http_header;
reference:md5,783aef84f5b315704ff6b064a00e2573; classtype:bad-unknown; sid:2034296; rev:1; metadata:attack_target
Client_Endpoint, created_at 2021_10_29, deployment Perimeter, signature_severity Informational, updated_at
2021_10_29;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (urlRequest)";
flow:established,to_server; content:"urlRequest"; http_header; reference:md5,988fbcfeebf2a49af4072030dead68f9;
classtype:bad-unknown; sid:2034298; rev:1; metadata:attack_target Client_Endpoint, created_at 2021_10_29,
deployment Perimeter, performance_impact Low, signature_severity Minor, updated_at 2021_10_29;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (test-upload)";
flow:established,to_server; content:"test-upload"; http_header; nocase; fast_pattern; pcre:"/^User-
Agent\x3a\x20[^\r\n]+test-upload/Hmi"; reference:md5,c110a5814451bbfba9eb41a2b2328213; classtype:bad-unknown;
sid:2034548; rev:2; metadata:attack_target Client_Endpoint, created_at 2021_11_29, deployment Perimeter,
signature_severity Informational, updated_at 2021_11_29;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (dBrowser
CallGetResponse)"; flow:to_server,established; threshold:type limit, count 2, track by_src, seconds 300;
content:"User-Agent|3a 20|dBrowser"; http_header; depth:20; content:"CallGetResponse:"; fast_pattern; http_header;
```

```
distance:3; within:16; pcre:"/^User\x2dAgent\x3a\x20dBrowser\x20\d\x20CallGetResponse\x3a\d/H";
reference:md5,e09ad59bff10bd4b730ee643809ec9a7; classtype:trojan-activity; sid:2034948; rev:2;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at
2022_01_19, deployment Perimeter, signature_severity Minor, updated_at 2022_01_19, reviewed_at 2024_05_07;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS websocket-sharp User-Agent Observed";
flow:established,to_server; content:"User-Agent|3a 20|websocket-sharp/"; fast_pattern; http_header;
reference:url,github.com/sta/websocket-sharp; classtype:bad-unknown; sid:2053849; rev:1; metadata:affected_product
Windows_XP_Vista_7_8_10_Server_32_64_Bit, affected_product Windows_11, attack_target Client_Endpoint, tls_state
TLSDecrypt, created_at 2022_02_01, deployment Perimeter, performance_impact Low, confidence High,
signature_severity Informational, updated_at 2024_06_25, former_sid 2851038;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (example/1.0)";
flow:to_server,established; content:"User-Agent|3a 20|example/1.0|0d 0a|"; http_header;
reference:url,cybereason.com/blog/strifewater-rat-iranian-apt-moses-staff-adds-new-trojan-to-ransomware-
operations; classtype:bad-unknown; sid:2035032; rev:2; metadata:affected_product
Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2022_02_01, deployment
Perimeter, signature_severity Minor, updated_at 2022_02_07, reviewed_at 2024_06_26;)

alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET USER_AGENTS Suspcious LeakIX User-Agent
(l9explore)"; flow:established,to_server; content:"User-Agent|3a 20|l9explore"; fast_pattern; http_header;
reference:url,ithub.com/LeakIX/l9format; classtype:bad-unknown; sid:2035314; rev:1; metadata:affected_product
Linux, attack_target Server, created_at 2022_02_28, deployment Perimeter, signature_severity Minor, updated_at
2022_02_28;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (ItIsMe)";
flow:to_server,established; content:"User-Agent|3a 20|ItIsMe"; fast_pattern; http_header;
reference:url,resources.cylera.com/new-evidence-linking-kwampirs-malware-to-shamoon-apts; classtype:trojan-
activity; sid:2035445; rev:1; metadata:attack_target Client_Endpoint, created_at 2022_03_14, deployment Perimeter,
performance_impact Low, signature_severity Informational, updated_at 2022_03_14;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (HTTP-Test-
Program)"; flow:to_server,established; content:"User-Agent|3a 20|User-Agent|3a 20|HTTP-Test-Program|0d 0a|";
http_header; reference:md5,6e69e15ae55aee85ace66bb99e6ba885; classtype:bad-unknown; sid:2035452; rev:1;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at
2022_03_14, deployment Perimeter, signature_severity Minor, updated_at 2022_03_14;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Malicious User-Agent
(CobaltStrike)"; flow:to_server,established; content:"User-Agent|3a 20|Mozilla/5.0_Frsg_stredf_o21_crown_type";
fast_pattern; http_header; reference:md5,b8b7a10dcc0dad157191620b5d4e5312; classtype:trojan-activity; sid:2035537;
rev:1; metadata:attack_target Client_Endpoint, created_at 2022_03_18, deployment Perimeter, malware_family
Cobalt_Strike, signature_severity Major, updated_at 2022_03_18, reviewed_at 2024_05_07, mitre_tactic_id TA0011,
mitre_tactic_name Command_And_Control, mitre_technique_id T1001, mitre_technique_name Data_Obfuscation;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Malicious User-Agent
(FastInvoice)"; flow:established,to_server; content:"User-Agent|3a 20|FastInvoice|0d 0a|"; http_header;
fast_pattern; reference:md5,42218b0ce7fc47f80aa239d4f9e000a1; classtype:bad-unknown; sid:2035932; rev:2;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at
2022_04_13, deployment Perimeter, signature_severity Minor, updated_at 2022_04_13;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed DPRK Related APT User-Agent
(dafom)"; flow:established,to_server; content:"dafom"; http_header; fast_pattern;
reference:url,www.cisa.gov/uscert/ncas/current-activity/2022/04/18/north-korean-state-sponsored-apt-targets-
blockchain-companies; classtype:bad-unknown; sid:2036260; rev:1; metadata:attack_target Client_Endpoint,
created_at 2022_04_19, deployment Perimeter, deployment SSLDecrypt, signature_severity Informational, updated_at
2022_04_19;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS AnyDesk Remote Desktop Software User-
Agent"; flow:established,to_server; content:"User-Agent|3a 20|AnyDesk"; http_header; fast_pattern;
reference:md5,1501639af59b0ff39d41577af30367cf; classtype:policy-violation; sid:2027762; rev:4;
metadata:attack_target Client_Endpoint, created_at 2019_07_26, deployment Perimeter, performance_impact Low,
```

```
signature_severity Minor, updated_at 2022_05_03;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent Mozilla/3.0";
flow:established,to_server; content:"User-Agent|3A| Mozilla/3.0|0d 0a|"; http_header; fast_pattern:11,14;
classtype:bad-unknown; sid:2012619; rev:6; metadata:affected_product Any, attack_target Client_Endpoint,
created_at 2011_04_01, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2022_06_27;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (adlib)";
flow:established,to_server; content:"User-Agent|3A 20|adlib/"; http_header;
reference:url,blog.trendmicro.com/connections-between-droiddreamlight-and-droidkungfu/; classtype:bad-unknown;
sid:2013967; rev:3; metadata:affected_product Any, attack_target Client_Endpoint, created_at 2011_11_24,
deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2022_06_27;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Windows
Explorer)"; flow:established,to_server; content:"User-Agent|3a 20|Windows Explorer|0d 0a|"; http_header; nocase;
fast_pattern; reference:url,twitter.com/reecdeep/status/1541735626915069954;
reference:md5,a750e7ca3c96e229159290610f050f44; classtype:trojan-activity; sid:2037137; rev:1;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at
2022_06_28, deployment Perimeter, signature_severity Informational, updated_at 2022_06_28;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS DanaBot Specific UA Observed";
flow:to_server,established; content:"User-Agent|3a 20|Mozilla/777.0"; fast_pattern:5,20; http_header;
classtype:trojan-activity; sid:2037737; rev:1; metadata:created_at 2022_07_11, signature_severity Major,
updated_at 2022_07_11;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (kath)";
flow:established,to_server; content:"User-Agent|3a 20|User-Agent|3a 20|kath|0d 0a|"; fast_pattern; http_header;
reference:md5,2ed86e80ea9b4b95b3e52ed77ea6c401; reference:url,cloudsek.com/yourcyanide-an-investigation-into-the-
frankenstein-ransomware-that-sends-malware-laced-love-letters/; classtype:bad-unknown; sid:2037747; rev:1;
metadata:attack_target Client_Endpoint, created_at 2022_07_12, deployment Perimeter, deployment SSLDecrypt,
signature_severity Informational, updated_at 2022_07_12;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (56)";
flow:to_server,established; content:"User-Agent|3a 20|56|0d 0a|"; fast_pattern; http_header;
reference:md5,c9ee1d6a90be7524b01814f48b39b232; classtype:trojan-activity; sid:2037828; rev:1;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at
2022_07_26, deployment Perimeter, signature_severity Major, updated_at 2022_07_26;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS ErbiumStealer UA Observed";
flow:to_server,established; content:"User-Agent|3a 20|Erbium-UA-"; fast_pattern; http_header;
reference:url,twitter.com/3xp0rtblog/status/1556256431904546816; classtype:trojan-activity; sid:2038482; rev:1;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at
2022_08_09, deployment Perimeter, malware_family Erbium, signature_severity Major, updated_at 2022_08_09,
reviewed_at 2024_05_08;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Hello World)";
flow:established,to_server; content:"User-Agent|3a 20|Hello World|0d 0a|"; http_header; nocase; fast_pattern;
classtype:trojan-activity; sid:2038507; rev:1; metadata:attack_target Client_Endpoint, created_at 2022_08_12,
deployment Perimeter, deployment SSLDecrypt, signature_severity Informational, updated_at 2022_08_12;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (xfilesreborn)";
flow:to_server,established; content:"User-Agent|3a 20|xfilesreborn|0d 0a|"; fast_pattern:4,20; http_header;
reference:md5,ba542a8d1d21e2016ade340fdc08d1a4; classtype:trojan-activity; sid:2038731; rev:1;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at
2022_09_02, deployment Perimeter, signature_severity Major, tag User_Agent, updated_at 2022_09_02, reviewed_at
2024_05_08;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Discord Bot User-Agent Observed
(DiscordBot)"; flow:established,to_server; content:"User-Agent|3a 20|DiscordBot"; http_header; fast_pattern;
reference:url,github.com/RogueException/Discord.Net; classtype:misc-activity; sid:2039124; rev:1;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at
```

2022_10_07, deployment Perimeter, deployment SSLDecrypt, signature_severity Informational, updated_at 2022_10_07;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (RestoroMainExe)"; flow:to_server,established; content:"User-Agent|3a 20|RestoroMainExe"; fast_pattern:6,20; http_header; threshold: type limit, count 1, seconds 600, track by_src; reference:md5,39fef85fe114d96dde745b8ce0659b2e; classtype:trojan-activity; sid:2038702; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2022_08_31, deployment Perimeter, signature_severity Major, updated_at 2022_10_10, reviewed_at 2024_05_08;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Windows 8)"; flow:to_server,established; content:"User-Agent|3a 20|Windows 8"; http_header; threshold:type limit, count 1, seconds 600, track by_src; classtype:bad-unknown; sid:2026520; rev:3; metadata:affected_product Web_Browsers, attack_target Client_Endpoint, created_at 2018_10_18, deployment Perimeter, signature_severity Minor, updated_at 2022_10_10;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (RT/1.0)"; flow:established,to_server; content:"User-Agent|3a 20|RT/1.0"; http_header; reference:md5,4c22c20fd816c11a3670100a40ac9dc0; classtype:trojan-activity; sid:2039422; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2022_10_17, deployment Perimeter, performance_impact Low, confidence High, signature_severity Informational, updated_at 2023_02_28, reviewed_at 2024_09_19;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Uclient User-Agent"; flow:established,to_server; content:"User-Agent|3a 20|UClient|20 28|"; fast_pattern; http_header; classtype:bad-unknown; sid:2039445; rev:1; metadata:attack_target Client_Endpoint, created_at 2022_10_19, deployment Perimeter, signature_severity Informational, updated_at 2022_10_19;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Malicious VBS Related UA"; flow:established,to_server; content:"User-Agent|3a 20|Mozilla/5.0 (Windows NT 10.0|3b 20|Win64|3b 20|x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36/"; fast_pattern:95,20; http_header; pcre:"/\x20Safari\/537.36\/[A-Za-z0-9]{17}\r\n/H"; reference:md5,2a90a42a4f379fb4a28bb32a96f8fc0f; classtype:trojan-activity; sid:2039832; rev:1; metadata:attack_target Client_Endpoint, created_at 2022_11_23, deployment Perimeter, signature_severity Major, updated_at 2022_11_23;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Microsoft Office Existence Discovery User-Agent"; flow:established,to_server; content:"User-Agent|3a 20|Microsoft Office Existence Discovery|0d 0a|"; http_header; fast_pattern:30,20; threshold:type both, track by_src, count 1, seconds 600; classtype:misc-activity; sid:2041131; rev:1; metadata:attack_target Client_Endpoint, created_at 2022_11_30, deployment Perimeter, signature_severity Informational, updated_at 2022_11_30;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed DonotGroup Related UA (Chrome Edge)"; flow:established,to_server; content:"User-Agent|3a 20|Chrome Edge 97.0.5|0d 0a|"; fast_pattern:12,20; http_header; reference:md5,79cff3bc3cbe51e1b3fecd131b949930; reference:md5,664d061c468079dcaa6486110879afc8; reference:url,twitter.com/StopMalvertisin/status/1624033048940642310; classtype:trojan-activity; sid:2044168; rev:1; metadata:attack_target Client_Endpoint, created_at 2023_02_10, deployment Perimeter, malware_family DonotGroup, signature_severity Major, updated_at 2023_02_10;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Donot Group UA (Mozilla FireFox)"; flow:established,to_server; content:"User-Agent|3a 20|Mozilla FireFox 61.00|0d 0a|"; fast_pattern:12,20; http_header; reference:md5,8f2829a963c3b6f247ac77e0bf992bf1; classtype:trojan-activity; sid:2044207; rev:1; metadata:attack_target Client_Endpoint, created_at 2023_02_15, deployment Perimeter, deployment SSLDecrypt, malware_family DonotGroup, signature_severity Major, updated_at 2023_02_15;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Bumblebee Loader User-Agent (bumblebee)"; flow:established,to_server; content:"User-Agent|3a 20|bumblebee|0d 0a|"; http_header; fast_pattern; reference:md5,555b77d23549e231c8d7f0b003cc5164; reference:md5,3f34d94803e9c8bc0a9cd09f507bc515; reference:url,www.cynet.com/orion-threat-alert-flight-of-the-bumblebee/; reference:url,blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/; classtype:trojan-activity; sid:2036237; rev:3; metadata:attack_target Client_Endpoint, created_at 2022_04_18, deployment Perimeter, deployment SSLDecrypt, malware_family Bumblebee_Loader, signature_severity Major, updated_at 2023_03_16;)

```
alert tcp any any -> $HOME_NET any (msg:"ET USER_AGENTS WinRM User Agent Detected - Possible Lateral Movement";
flow:established,to_server; content:"|0d 0a|User-Agent|3a 20|Microsoft|20|WinRM|20|Client|0d 0a|";
fast_pattern:14,20; reference:url,attack.mitre.org/techniques/T1028/; classtype:bad-unknown; sid:2026850; rev:3;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_and_Server, created_at
2019_01_23, deployment Internal, performance_impact Low, signature_severity Minor, tag WinRM, updated_at
2023_04_14, mitre_tactic_id TA0008, mitre_tactic_name Lateral_Movement, mitre_technique_id T1021,
mitre_technique_name Remote_Services;)

alert tcp $HOME_NET any -> any any (msg:"ET USER_AGENTS Win32/FakeAV InternetSecurityGuard User-Agent";
flow:established,to_server; content:"User-Agent|3a 20|"; content:"@internetsecurityguard|0d 0a|"; fast_pattern;
reference:md5,054139bbb3748d0b8d393ab438e3a050; classtype:trojan-activity; sid:2045158; rev:1; metadata:created_at
2023_04_24, confidence High, signature_severity Major, updated_at 2023_04_24;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (Zadanie)";
flow:established,to_server; content:"User-Agent|3a 20|Zadanie|0d 0a|"; http_header; nocase; fast_pattern;
reference:url,twitter.com/nahamike01/status/1664595922360344578; classtype:trojan-activity; sid:2046057; rev:1;
metadata:created_at 2023_06_02, signature_severity Major, updated_at 2023_06_02;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Kimsuky CnC Checkin User-Agent";
flow:established,to_server; content:"User-Agent|3a 20|Mozilla|2f|5|2e|0|20 28|Windows|20|NT|20|10|2e|x|3b
20|Win64|3b 20|x64|29 20|AppleWebKit|2f|537|2e|36|20 28|KHTML|2c 20|like|20|Gecko|29
20|Chremo|2f|87|2e|0|2e|4280|2e|141|20|Safari|2f|537|2e|36|20|Edgo|2f|87|2e|0|2e|664|2e|75|0d 0a|"; http_header;
fast_pattern:102,20; reference:url,zhuanlan.zhihu.com/p/567386930; classtype:trojan-activity; sid:2046893; rev:1;
metadata:attack_target Client_Endpoint, created_at 2023_07_25, deployment Perimeter, confidence High,
signature_severity Major, updated_at 2023_07_25;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Reconnaissance Related UA";
flow:established,to_server; content:"User-Agent|3a 20|Mozilla/5.0|20 28|Windows NT 6.1|3b 20|WOW64|3b
20|rv|3a|68.0|29 09 09 09 20 20 20 20|Gecko/20100101|20|Firefox/68.0|0d 0a|"; fast_pattern:44,20; http_header;
reference:url,www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a; classtype:misc-activity; sid:2047994;
rev:1; metadata:attack_target Client_Endpoint, created_at 2023_09_11, deployment Perimeter, performance_impact
Low, confidence Medium, signature_severity Informational, updated_at 2023_09_11, reviewed_at 2023_09_11;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Seetrol Client Remote Administration
Tool User-Agent"; flow:established,to_server; pcre:"/seetrol\x2e(?:com|(\x2eco)?kr)\x0d\x0a/H"; content:"User-
Agent|3a 20|SeetrolClient|0d 0a|"; http_header; fast_pattern:7,20; threshold:type limit,seconds 300,count 1,track
by_src; classtype:trojan-activity; sid:2049138; rev:1; metadata:affected_product
Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2023_11_09, deployment
Perimeter, deployment SSLDecrypt, confidence High, signature_severity Minor, updated_at 2023_11_09;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Observed Suspicious User-Agent
(inflammable)"; flow:established,to_server; content:"User-Agent|3a 20|inflammable|0d 0a|"; http_header;
fast_pattern:5,20; threshold:type limit,seconds 300,count 1,track by_src;
reference:md5,adcaa63353083b81150d99bca3fc8752; classtype:misc-activity; sid:2049171; rev:1;
metadata:attack_target Client_Endpoint, created_at 2023_11_14, deployment Perimeter, deployment SSLDecrypt,
confidence High, signature_severity Informational, updated_at 2023_11_14;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS WebHack Control Center User-Agent
Outbound (WHCC/)"; flow:established,to_server; content:"User-Agent|3a|"; nocase; content:"WHCC"; http_header;
fast_pattern; nocase; pcre:"/^User-Agent\:[^\n]+WHCC/Hmi";
reference:url,www.governmentsecurity.org/forum/index.php?showtopic=5112&pid=28561&mode=threaded&start=;
classtype:trojan-activity; sid:2003925; rev:8; metadata:created_at 2010_07_30, updated_at 2024_01_24;)

#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent Beginning with
digits - Likely spyware/trojan"; flow:established,to_server; content:"User-Agent|3a| "; http_header;
content:!"User-Agent|3a| Mozilla/"; http_header; pcre:"/\x0d\x0aUser-Agent\: \d+/H";
content:!"liveupdate.symanteclive update.com|0d 0a|"; http_header; classtype:trojan-activity; sid:2010697; rev:9;
metadata:affected_product Any, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter,
deprecation_reason Performance, performance_impact Significant, signature_severity Major, tag User_Agent,
updated_at 2024_02_27;)
```

```
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Microsoft Edge on Windows 10 SET";
flow:established,to_server; content:"User-Agent|3a 20|"; http_header; content:"Windows NT 10."; http_header;
distance:0; content:"Edge/12."; http_header; distance:0; fast_pattern; flowbits:set,ET_EDGE_UA; flowbits:noalert;
classtype:misc-activity; sid:2023197; rev:5; metadata:affected_product Microsoft_Edge_Browser, created_at
2016_09_13, deployment Perimeter, deprecation_reason Relevance, performance_impact Low, signature_severity
Informational, tag User_Agent, updated_at 2024_04_25;)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Go HTTP Client User-Agent";
flow:established,to_server; content:"User-Agent|3a 20|Go-http-client|0d 0a|"; nocase; http_header; fast_pattern;
classtype:misc-activity; sid:2024897; rev:3; metadata:attack_target Client_Endpoint, created_at 2017_10_23,
deployment Perimeter, confidence High, signature_severity Informational, updated_at 2024_06_13;)
```