```
reference:url,doc.emergingthreats.net/2003597; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Google; sid:2003597; rev:4;)

#Submitted by Michael Holstein, 2006-02-13. Reference from scheidell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Google Desktop User-Agent Detected"; flow:to_server,established; content:"User-Agent|3a| Mozilla/4.0 (compatible|3b|
Google Desktop)"; nocase; threshold: type limit, count 1, seconds 360, track by_src; classtype:policy-violation; reference:url,news.com.com/2100-1032_3-6038197.html;
reference:url,doc.emergingthreats.net/2002801; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Google; sid:2002801; rev:9;)

#Submitted 2006-02-28 by Mark Warren. For Google appliances that "should" only spider internal web sites (but sometimes go wild and spider the Internet)
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Google Search Appliance browsing the Internet"; flow:to_server,established; content:"GET "; depth:4; content:"User-
Agent|3A| gsa-crawler"; nocase; classtype:web-application-activity; reference:url,www.google.com/enterprise/gsa/index.html; reference:url,doc.emergingthreats.net/2002838;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Google; sid:2002838; rev:7;)

#By Matt Jonkman. Reviving this rule as it's been dropped from the snort.org rulesets.
#
#alert tcp $HOME_NET any -> 66.151.158.177 any (msg:"ET POLICY GotoMyPC Polling Client"; flow: established; threshold: type limit, track by_src, count 1, seconds 360; classtype: policy-
violation; reference:url,doc.emergingthreats.net/2000309; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_GotoMyPC; sid:2000309; rev:8;)

#This intends to be a more intelligent version of the old gotomypc rule, eventually to replace the old if it catches everything
#
alert tcp 66.151.158.177 8200 -> $HOME_NET any (msg:"ET POLICY GotoMyPC poll.gotomypc.com Server Response to Polling Client OK"; flow: established,from_server; content:"cnt=0"; nocase;
depth: 40; content:"eventid="; nocase; depth: 40; threshold: type limit, track by_src, count 1, seconds 360; classtype: policy-violation; reference:url,doc.emergingthreats.net/2002022;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_GotoMyPC; sid:2002022; rev:4;)

#Submitted 2006-08-30 by Robert Sharp
#
##alert tcp $HOME_NET any <> $EXTERNAL_NET $HTTP_PORTS (msg:"ET DELETED Gmail gtalk"; flow:established; pcre:"/\[\[\d{1,3}\,\[\\\"\w\\\"\,\\\".+@gmail.com.+\\\"\,\\\"/i";
classtype:policy-violation; reference:url,doc.emergingthreats.net/2003092; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Gtalk; sid:2003092; rev:3;)

#Submitted by Matt Jonkman
#hotmail has changed, obsoleting these
#to be deleted
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Hotmail Inbox Access"; flow: to_server,established; content:"hotmail.msn.com|0d 0a|"; uricontent:"/cgi-bin/HoTMaiL?
curmbox="; nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/2000035; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_HOTMAIL_Mail_Use; sid:2000035; rev:13;)

#Submitted by Matt Jonkman
#hotmail has changed, obsoleting these
#to be deleted
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Hotmail Message Access"; flow: to_server,established; content:"hotmail.msn.com|0d 0a|"; uricontent:"/cgi-
bin/getmsg?msg=MSG"; classtype: policy-violation; reference:url,doc.emergingthreats.net/2000036; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_HOTMAIL_Mail_Use; sid:2000036; rev:14;)

#Submitted by Matt Jonkman
#hotmail has changed, obsoleting these
#to be deleted
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Hotmail Compose Message Access"; flow: to_server,established; uricontent:"curmbox="; nocase;
content:"hotmail.msn.com|0d 0a|"; nocase; uricontent:"/cgi-bin/compose?/"; nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/2000037;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_HOTMAIL_Mail_Use; sid:2000037; rev:14;)

#Submitted by Matt Jonkman
#hotmail has changed, obsoleting these
#to be deleted
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Hotmail Compose Message Submit"; flow: to_server,established; content:"hotmail.msn.com|0d 0a|"; nocase;
uricontent:"/cgi-bin/premail/"; classtype: policy-violation; reference:url,doc.emergingthreats.net/2000038; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_HOTMAIL_Mail_Use; sid:2000038; rev:13;)

#Submitted by Matt Jonkman
#hotmail has changed, obsoleting these
#to be deleted
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Hotmail Compose Message Submit Data"; flow: to_server,established; content:"curmbox="; nocase; content:"login=";
nocase; content:"msghdrid"; nocase; content:"sigflag="; nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/2000039; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_HOTMAIL_Mail_Use; sid:2000039; rev:9;)

#by Rouke de Jong
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Hotmail Inbox Access"; flow:to_server,established; content:"GET "; depth:4; content:"mail.live.com";
uricontent:"/mail/InboxLight.aspx"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2008238; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_HOTMAIL_Mail_Use; sid:2008238; rev:2;)

#by Rouke de Jong
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Hotmail Message Access"; flow:to_server,established; content:"GET "; depth:4; content:"mail.live.com";
uricontent:"/mail/ReadMessageLight.aspx"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2008239; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_HOTMAIL_Mail_Use; sid:2008239; rev:2;)

#by Rouke de Jong
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Hotmail Compose Message Access"; flow:to_server,established; content:"GET "; depth:4; content:"mail.live.com";
nocase; uricontent:"/mail/EditMessageLight.aspx"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2008240; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_HOTMAIL_Mail_Use; sid:2008240; rev:2;)

#by Rouke de Jong
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET DELETED Hotmail Compose Message Submit"; flow:to_server,established; content:"POST "; depth:5; content:"mail.live.com";
nocase; uricontent:"SendMessageLight.aspx"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2008241; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_HOTMAIL_Mail_Use; sid:2008241; rev:2;)

#In full mode induvidual inbox, compose message etc rules cannot be
#aplied :
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Hotmail Access Full Mode"; flow:to_server,established; content:"GET "; depth:4; content:"mail.live.com";
uricontent:"/mail/ApplicationMain"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2008242; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_HOTMAIL_Mail_Use; sid:2008242; rev:2;)

#by Kevin Ross
#
alert tcp $HOME_NET 23 -> any any (msg:"ET POLICY Telnet to HP JetDirect Printer With No Password Set"; flow:to_client,established; content:"HP JetDirect"; content:"Password is not
set"; offset:40; depth:30; distance:2; classtype:misc-activity; reference:url,h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj05999#A3;
reference:url,doc.emergingthreats.net/2009535; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_HPJetDirect; sid:2009535; rev:2;)

#by Kevin Ross
#
alert tcp $HOME_NET 21 -> $EXTERNAL_NET any (msg:"ET POLICY External FTP Connection TO Local HP JetDirect Printer"; flow:to_client,established; content:"Hewlett-Packard FTP Print Server
Version"; content:"To print a file, use the command|3a| put <filename> [portx]"; offset:40; distance:80; depth:190; classtype:misc-activity;
reference:url,h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj06165; reference:url,doc.emergingthreats.net/2009536; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_HPJetDirect; sid:2009536; rev:3;)

#Submitted by Thomas Alex
#
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 8000 (msg:"ET MISC HP Web JetAdmin ExecuteFile admin access"; flow: to_server,established; content:"/plugins/framework/script/content.hts";
nocase; content:"ExecuteFile"; nocase; classtype: attempted-admin; reference:bugtraq,10224; reference:url,doc.emergingthreats.net/2001055; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_HP_Web_Jetadmin_Executefile_Access; sid:2001055; rev:6;)

#by Jaime Blasco
#
alert udp any 1985 -> 224.0.0.2 1985 (msg:"ET POLICY HSRP Active Router Changed"; content:"|00 04|"; depth:3; classtype:bad-unknown;
reference:url,packetlife.net/blog/2008/oct/27/hijacking-hsrp/; reference:url,doc.emergingthreats.net/2009243; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_HSRP_Change; sid:2009243; rev:2;)

#by chodemort
#use if you see fit, not safe for all networks
#
#alert tcp any $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY HTTP Redirect to IPv4 Address"; flow:established,from_server; content:"HTTP/1.1 302 Found"; nocase; depth:18;
content:"Location|3a| "; nocase; pcre:"/Location\: (http\:\/\/)?\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\//i"; classtype:misc-activity; reference:url,doc.emergingthreats.net/2011085;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_HTTP_Redirect; sid:2011085; rev:3;)

#Matt Jonkman
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET !$HTTP_PORTS (msg:"ET POLICY Inbound HTTP CONNECT Attempt on Off-Port"; flow:to_server,established; content:"CONNECT "; nocase; depth:8;
content:" HTTP/1."; nocase; within:1000; classtype:misc-activity; reference:url,doc.emergingthreats.net/2008284; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_HTTP_Tunneling_via_Proxy; sid:2008284; rev:3;)

#Submitted by Jason
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY HTTP CONNECT Tunnel Attempt Inbound"; flow: to_server,established; content:"CONNECT "; nocase; content:"|0d 0a|"; within:
1024; distance: 0; content:"HTTP/1."; nocase; within: 8; distance: -10; content:!"|3a|80"; within: 4; distance: -11; content:"CONNECT "; nocase; content:"|0d 0a|"; within: 1024;
distance: 0; content:"HTTP/1."; nocase; within: 8; distance: -10; content:!"|3a|443"; within: 5; distance: -12; classtype: misc-activity; reference:url,doc.emergingthreats.net/2000560;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_HTTP_Tunneling_via_Proxy; sid:2000560; rev:10;)

#Submitted by Jason
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET POLICY HTTP CONNECT Tunnel Attempt Outbound"; flow: to_server,established; content:"CONNECT "; nocase; content:"|0d 0a|"; within:
1024; distance: 0; content:"HTTP/1."; nocase; within: 8; distance: -10; content:!"|3a|80"; within: 4; distance: -11; content:"CONNECT "; nocase; content:"|0d 0a|"; within: 1024;
distance: 0; content:"HTTP/1."; nocase; within: 8; distance: -10; content:!"|3a|443"; within: 5; distance: -12; classtype: misc-activity; reference:url,doc.emergingthreats.net/2008330;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_HTTP_Tunneling_via_Proxy; sid:2008330; rev:11;)

#by Sandro Reis
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET POLICY Possible HTTP-TUNNEL to External Proxy for Anonymous Access"; flow:established,to_server; content:"GET
/login/FetchProtocolVersion2.htm"; depth:36; classtype:policy-violation; threshold:type limit, track by_src,count 5, seconds 30; reference:url,doc.emergingthreats.net/2008842;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_HTTP_Tunneling_via_Proxy; sid:2008842; rev:4;)

#by Sandro Reis
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET POLICY Possible HTTP-TUNNEL to External Proxy for Anonymous Access (server download)"; flow:established,to_server; content:"GET
login/fetchFreeServersVersion2.aspx"; depth:39; classtype:policy-violation; threshold:type limit, track by_src,count 5, seconds 30; reference:url,doc.emergingthreats.net/2008843;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_HTTP_Tunneling_via_Proxy; sid:2008843; rev:4;)

#
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 81:65535 (msg:"ET POLICY HTTP GET on unusual Port Possibly Hostile"; flowbits:isnotset,BS.HTTP.ok; flow:established,to_server; content:"GET ";
nocase; depth:4; classtype:policy-violation; reference:url,doc.emergingthreats.net/2006408; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_HTTP_on_Off_Ports; sid:2006408; rev:5;)

#idea from Blake Hartstein, use these only if you like. Not a definite indication of hostile activity
#alert tcp $HOME_NET any -> $EXTERNAL_NET 81:65535 (msg:"ET POLICY HTTP POST on unusual Port Possibly Hostile"; flowbits:isnotset,BS.HTTP.ok; flow:established,to_server; content:"POST
"; nocase; depth:5; classtype:policy-violation; reference:url,doc.emergingthreats.net/2006409; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_HTTP_on_Off_Ports; sid:2006409; rev:5;)

#by Dajackman
#
#alert tcp $HOME_NET any -> [64.34.106.33,64.94.18.67] 12975 (msg:"ET POLICY Outbound Hamachi VPN Connection Attempt"; flags:S,12; threshold:type limit, track by_src, count 1, seconds
120; classtype:policy-violation; reference:url,www.hamachi.cc; reference:url,doc.emergingthreats.net/2002729; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Hamachi_VPN; sid:2002729; rev:4;)

#by Jamian Mason of Deepnines.com
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Hi5.com Social Site Access"; flow:established,to_server; content:"Host|3a| www.hi5.com|0d 0a|"; threshold: type
both, track by_src, count 5, seconds 300; classtype:policy-violation; reference:url,doc.emergingthreats.net/2003455; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Hi5.com; sid:2003455; rev:5;)

#Dutch myspace style social networking site. Not a security threat, just a generally not permissable thing for the workplace
#by Cees Elzinga
#Both hyves.nl and hyves.net are used, so check for "hyves."
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Hyves Login Attempt"; flow:established,to_server; content:"|0d 0a|Host|3a| www.hyves."; content:"login_username";
classtype:policy-violation; reference:url,doc.emergingthreats.net/2007627; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Hyves; sid:2007627; rev:6;)

#Dutch myspace style social networking site. Not a security threat, just a generally not permissable thing for the workplace
#by Cees Elzinga
#Both hyves.nl and hyves.net are used, so check for "hyves."
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Hyves Inbox Access"; flow:established,to_server; content:"Host\: www.hyves."; uricontent:"/messages/inbox/";
classtype:policy-violation; reference:url,doc.emergingthreats.net/2007628; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Hyves; sid:2007628; rev:4;)

#Dutch myspace style social networking site. Not a security threat, just a generally not permissable thing for the workplace
#by Cees Elzinga
#Both hyves.nl and hyves.net are used, so check for "hyves."
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Hyves Message Access"; flow:established,to_server; content:"Host|3a| www.hyves.";
uricontent:"/messages/inbox/messages/"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2007629; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Hyves; sid:2007629; rev:5;)

#Dutch myspace style social networking site. Not a security threat, just a generally not permissable thing for the workplace
#by Cees Elzinga
#Both hyves.nl and hyves.net are used, so check for "hyves."
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Hyves Compose Message"; flow:established,to_server; content:"Host|3a| www.hyves."; uricontent:"index.php?l1=mg";
classtype:policy-violation; reference:url,doc.emergingthreats.net/2007630; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Hyves; sid:2007630; rev:5;)

#Dutch myspace style social networking site. Not a security threat, just a generally not permissable thing for the workplace
#by Cees Elzinga
#Both hyves.nl and hyves.net are used, so check for "hyves."
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Hyves Message Submit"; flow:established,to_server; content:"Host|3a| www.hyves."; uricontent:"/messages/";
content:"POST /messages/"; content:"postman_secret"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2007631; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Hyves; sid:2007631; rev:5;)

#by jack pepper
#disabled by default, but run it if you have your old IE under control
#
#alert tcp $HOME_NET any -> any $HTTP_PORTS (msg:"ET USER_AGENTS Internet Explorer 6 in use - Significant Security Risk"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
Mozilla/4.0 (compatible|3b| MSIE 6.0|3b|"; threshold: type limit, track by_src, seconds 180, count 1; classtype: policy-violation; reference:url,doc.emergingthreats.net/2010706;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IE6; sid:2010706; rev:6;)

#by Matt Jonkman, reference at http://piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Gadu-Gadu IM Login Server Request"; flow:established,to_server; uricontent:"/appsvc/appmsg"; nocase;
uricontent:".asp"; nocase; uricontent:"fmnumber="; uricontent:"&version="; uricontent:"&fmt="; content:"|0d 0a|Host\: appmsg.gadu-gadu."; classtype:policy-violation;
```

```
reference:url,piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html; reference:url,doc.emergingthreats.net/2008295; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_GaduGadu; sid:2008295; rev:4;)

#by Matt Jonkman, reference at http://piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html
#
alert tcp $EXTERNAL_NET 8074 -> $HOME_NET any (msg:"ET POLICY GaduGadu Chat Server Welcome Packet"; flow:established,from_server; dsize:12; content:"|01 00 00 00|"; depth:4;
flowbits:set,ET.gadu.welcome; classtype:policy-violation; reference:url,piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html;
reference:url,doc.emergingthreats.net/2008297; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_GaduGadu; sid:2008297; rev:4;)

#by Matt Jonkman, reference at http://piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 8074 (msg:"ET POLICY GaduGadu Chat Client Login Packet"; flowbits:isset,ET.gadu.welcome; flow:established,to_server; dsize:<50; content:"|15 00
00 00|"; depth:4; flowbits:set,ET.gadu.loginsent; classtype:policy-violation; reference:url,piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html;
reference:url,doc.emergingthreats.net/2008298; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_GaduGadu; sid:2008298; rev:3;)

#by Matt Jonkman, reference at http://piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html
#
alert tcp $EXTERNAL_NET 8074 -> $HOME_NET any (msg:"ET POLICY GaduGadu Chat Server Login OK Packet"; flowbits:isset,ET.gadu.loginsent; flow:established,from_server; dsize:8;
content:"|03 00 00 00 00 00 00 00|"; flowbits:set,ET.gadu.loggedin; classtype:policy-violation; reference:url,piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html;
reference:url,doc.emergingthreats.net/2008299; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_GaduGadu; sid:2008299; rev:3;)

#by Matt Jonkman, reference at http://piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html
#
alert tcp $EXTERNAL_NET 8074 -> $HOME_NET any (msg:"ET POLICY GaduGadu Chat Server Login Failed Packet"; flowbits:isset,ET.gadu.loginsent; flow:established,from_server; dsize:8;
content:"|09 00 00 00 00 00 00 00|"; classtype:policy-violation; reference:url,piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html;
reference:url,doc.emergingthreats.net/2008300; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_GaduGadu; sid:2008300; rev:3;)

#by Matt Jonkman, reference at http://piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html
#
alert tcp $EXTERNAL_NET 8074 -> $HOME_NET any (msg:"ET POLICY GaduGadu Chat Server Available Status Packet"; flowbits:isset,ET.gadu.loggedin; flow:established,to_server; content:"|02 00
00 00|"; depth:4; classtype:policy-violation; reference:url,piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html; reference:url,doc.emergingthreats.net/2008301;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_GaduGadu; sid:2008301; rev:3;)

#by Matt Jonkman, reference at http://piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 8074 (msg:"ET POLICY GaduGadu Chat Send Message"; flowbits:isset,ET.gadu.loggedin; flow:established,to_server; content:"|0b 00 00 00|"; depth:4;
classtype:policy-violation; reference:url,piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html; reference:url,doc.emergingthreats.net/2008302;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_GaduGadu; sid:2008302; rev:3;)

#by Matt Jonkman, reference at http://piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html
#
alert tcp $EXTERNAL_NET 8074 -> $HOME_NET any (msg:"ET POLICY GaduGadu Chat Receive Message"; flowbits:isset,ET.gadu.loggedin; flow:established,from_server; content:"|0a 00 00 00|";
depth:4; classtype:policy-violation; reference:url,piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html; reference:url,doc.emergingthreats.net/2008303;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_GaduGadu; sid:2008303; rev:3;)

#by Matt Jonkman, reference at http://piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 8074 (msg:"ET POLICY GaduGadu Chat Keepalive PING"; flowbits:isset,ET.gadu.loggedin; flow:established,to_server; content:"|08 00 00 00|";
depth:4; classtype:policy-violation; reference:url,piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html; reference:url,doc.emergingthreats.net/2008304;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_GaduGadu; sid:2008304; rev:3;)

#by Matt Jonkman, reference at http://piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html
#
alert tcp $EXTERNAL_NET 8074 -> $HOME_NET any (msg:"ET POLICY GaduGadu Chat Keepalive PONG"; flowbits:isset,ET.gadu.loggedin; flow:established,from_server; content:"|07 00 00 00|";
depth:4; classtype:policy-violation; reference:url,piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html; reference:url,doc.emergingthreats.net/2008305;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_GaduGadu; sid:2008305; rev:3;)

#by Matt Jonkman, reference at http://piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 8074 (msg:"ET POLICY GaduGadu Chat File Send Request"; flowbits:isset,ET.gadu.loggedin; flow:established,to_server; content:"|01 00 00 00|";
depth:4; classtype:policy-violation; reference:url,piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html; reference:url,doc.emergingthreats.net/2008306;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_GaduGadu; sid:2008306; rev:3;)

#by Matt Jonkman, reference at http://piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 8074 (msg:"ET POLICY GaduGadu Chat File Send Details"; flowbits:isset,ET.gadu.loggedin; flow:established,to_server; content:"|03 00 00 00|";
depth:4; classtype:policy-violation; reference:url,piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html; reference:url,doc.emergingthreats.net/2008307;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_GaduGadu; sid:2008307; rev:3;)

#by Matt Jonkman, reference at http://piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html
#
alert tcp $EXTERNAL_NET 8074 -> $HOME_NET any (msg:"ET POLICY GaduGadu Chat File Send Accept"; flowbits:isset,ET.gadu.loggedin; flow:established,from_server; content:"|06 00 00 00|";
depth:4; classtype:policy-violation; reference:url,piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html; reference:url,doc.emergingthreats.net/2008308;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_GaduGadu; sid:2008308; rev:3;)

#by Matt Jonkman, reference at http://piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html
#
alert tcp $EXTERNAL_NET 8074 -> $HOME_NET any (msg:"ET POLICY GaduGadu Chat File Send Begin"; flowbits:isset,ET.gadu.loggedin; flow:established,from_server; content:"|03 00 00 00|";
depth:4; classtype:policy-violation; reference:url,piotr.trzcionkowski.pl/default.asp?load=/programy/pppgg_protokol.html; reference:url,doc.emergingthreats.net/2008309;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_GaduGadu; sid:2008309; rev:3;)

#By Merphie from the forums
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 5190 (msg:"ET POLICY ICQ Status Invisible"; flow: from_client,established; content:"|2A02|"; depth: 2; content:"|001900130005|"; offset: 4;
depth: 6; classtype: policy-violation; reference:url,doc.emergingthreats.net/2001801; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_ICQ; sid:2001801;
rev:5;)

#By Merphie from the forums
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 5190 (msg:"ET POLICY ICQ Status Change (1)"; flow: from_client,established; content:"|2A02|"; depth: 2; content:"|000E00010011|"; offset: 4;
depth: 6; classtype: policy-violation; reference:url,doc.emergingthreats.net/2001802; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_ICQ; sid:2001802;
rev:6;)

#By Merphie from the forums
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 5190 (msg:"ET POLICY ICQ Status Change (2)"; flow: from_client,established; content:"|2A02|"; depth: 2; content:"|00120001001E|"; offset: 4;
depth: 6; classtype: policy-violation; reference:url,doc.emergingthreats.net/2001803; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_ICQ; sid:2001803;
rev:6;)

#By Merphie from the forums
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 5190 (msg:"ET POLICY ICQ Login"; flow: from_client,established; content:"|2A01|"; depth: 2; content:"|00010001|"; offset: 8; depth: 4;
classtype: policy-violation; reference:url,doc.emergingthreats.net/2001804; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_ICQ; sid:2001804; rev:5;)

#By Merphie from the forums
#
alert tcp $HOME_NET any <> $EXTERNAL_NET any (msg:"ET POLICY ICQ Message"; flow: established; content:"|2A02|"; depth: 2; content:"|000400060000|"; offset: 6; depth: 6; classtype:
policy-violation; reference:url,doc.emergingthreats.net/2001805; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_ICQ; sid:2001805; rev:5;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY ICP Email Send via HTTP - Often Trojan Install Reports"; flow:established,to_server;
uricontent:"/friendship/email_thank_you.php?"; nocase; uricontent:"folder_id="; nocase; uricontent:"&params_count="; nocase; uricontent:"&nick_name="; nocase; uricontent:"&user_email=";
nocase; uricontent:"&user_uin="; nocase; uricontent:"&friend_nickname="; nocase; uricontent:"&friend_contact="; nocase; classtype:policy-violation;
reference:url,doc.emergingthreats.net/2008351; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_ICQ; sid:2008351; rev:2;)

#by Mark Tombaugh
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 5222 (msg:"ET POLICY Google Talk (Jabber) Client Login"; flow:established,to_server; content:"gmail.com"; nocase; content:"jabber"; nocase;
```

```
distance:9; within:6; classtype:policy-violation; reference:url,talk.google.com; reference:url,www.xmpp.org; reference:url,doc.emergingthreats.net/2002327;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_Jabber; sid:2002327; rev:4;)

#by Mark Tombaugh
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 443 (msg:"ET POLICY Google Talk TLS Client Traffic"; flow:established,to_server; content:"gmail.com"; nocase; content:"jabber"; nocase;
distance:64; within:78; classtype:policy-violation; reference:url,talk.google.com; reference:url,www.xmpp.org; reference:url,doc.emergingthreats.net/2002330;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_Jabber; sid:2002330; rev:4;)

#by Brad Doctor
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET POLICY Google IM traffic Windows client user sign-on"; flow:to_server; content:"ms|3a|xml|3a|ns|3a|xmpp-s"; content:"X-GOOGLE-
TOKEN"; classtype:policy-violation; reference:url,www.google.com/talk; reference:url,doc.emergingthreats.net/2002332; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_Jabber; sid:2002332; rev:6;)

#by Brad Doctor
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET POLICY Google IM traffic friend invited"; flow:to_server; content:"><invitati"; content:"on xmlns=\"google"; classtype:policy-
violation; reference:url,www.google.com/talk; reference:url,doc.emergingthreats.net/2002333; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_Jabber;
sid:2002333; rev:6;)

#by Brad Doctor
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 5222 (msg:"ET POLICY Google IM traffic Jabber client sign-on"; flow:to_server; content:"gmail.com"; nocase; content:"jabber.org"; nocase;
content:"version="; classtype:policy-violation; reference:url,www.google.com/talk; reference:url,doc.emergingthreats.net/2002334; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_Jabber; sid:2002334; rev:5;)

#Submitted by Joel Esler
#
alert tcp $HOME_NET any <> $EXTERNAL_NET any (msg:"ET CHAT MSN file transfer request"; flow: established; content:"MSG "; depth: 4; content:"Content-Type|3A|"; nocase; distance: 0;
content:"text/x-msmsgsinvite"; nocase; distance: 0; content:"Application-Name|3A|"; content:"File Transfer"; nocase; distance: 0; classtype: policy-violation;
reference:url,doc.emergingthreats.net/2001241; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_MSN; sid:2001241; rev:5;)

#Submitted by Joel Esler
#
alert tcp $HOME_NET any <> $EXTERNAL_NET any (msg:"ET CHAT MSN file transfer accept"; flow: established; content:"MSG "; depth: 4; content:"Content-Type|3A|"; nocase; content:"text/x-
msmsgsinvite"; distance: 0; content:"Invitation-Command|3A|"; content:"ACCEPT"; distance: 1; classtype: policy-violation; reference:url,doc.emergingthreats.net/2001242;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_MSN; sid:2001242; rev:5;)

#Submitted by Joel Esler
#
alert tcp $HOME_NET any <> $EXTERNAL_NET any (msg:"ET CHAT MSN file transfer reject"; flow: established; content:"MSG "; depth: 4; content:"Content-Type|3A|"; nocase; content:"text/x-
msmsgsinvite"; distance: 0; content:"Invitation-Command|3A|"; content:"CANCEL"; distance: 0; content:"Cancel-Code|3A|"; nocase; content:"REJECT"; nocase; distance: 0; classtype: policy-
violation; reference:url,doc.emergingthreats.net/2001243; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_MSN; sid:2001243; rev:5;)

#Matt Jonkman, more msn
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CHAT MSN IM Poll via HTTP"; flow: established,to_server; uricontent:"/gateway/gateway.dll?Action=poll&SessionID="; nocase;
threshold: type limit, track by_src, count 10, seconds 3600; classtype: policy-violation; reference:url,doc.emergingthreats.net/2001682; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_MSN; sid:2001682; rev:8;)

#Submitted by Scott Melnick
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET CHAT MSN status change"; flow:established,to_server; content:"CHG "; depth:55; classtype:policy-violation;
reference:url,doc.emergingthreats.net/2002192; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_MSN; sid:2002192; rev:4;)

#Submitted by Scott Melnick
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET DELETED MSN Game Loading"; flow:established,to_server; content:"|6D 73 6E 67 61 6D 65 2E 61 73 70 78|"; depth:90;
classtype:policy-violation; reference:url,doc.emergingthreats.net/2002312; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_MSN; sid:2002312; rev:4;)

#by Sp0oker
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1863 (msg:"ET CHAT Possible MSN Messenger File Transfer"; flow:established,from_client; content:"x-msnmsgrp2p"; nocase; content:"appid|3a|";
nocase; pcre:"/appid\x3a\s+2/i"; classtype: policy-violation; reference:url,www.hypothetic.org/docs/msn/client/file_transfer.php; reference:url,doc.emergingthreats.net/2008289;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_MSN; sid:2008289; rev:5;)

#bu Jaime Blasco
#
alert tcp $HOME_NET any <> $EXTERNAL_NET any (msg:"ET POLICY General MSN Chat Activity"; flow: established; content:"|0d 0a|Content-Type|3A|"; content:"application/x-msn-messenger";
distance:0; classtype:policy-violation; reference:url,www.hypothetic.org/docs/msn/general/http_examples.php; reference:url,doc.emergingthreats.net/2009375;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_MSN; sid:2009375; rev:2;)

#bu Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET CHAT MSN User-Agent Activity"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| MSMSGS"; nocase; classtype:policy-
violation; reference:url,www.hypothetic.org/docs/msn/general/http_examples.php; reference:url,doc.emergingthreats.net/2009376; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_MSN; sid:2009376; rev:3;)

#Submitted by Joel Esler
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET CHAT Yahoo IM successful logon"; flow: from_server,established; content:"YMSG"; nocase; depth: 4; content:"|00 01|"; offset: 10;
depth: 2; classtype: policy-violation; reference:url,doc.emergingthreats.net/2001253; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_Yahoo; sid:2001253;
rev:5;)

#Submitted by Joel Esler
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET CHAT Yahoo IM voicechat"; flow: from_server,established; content:"YMSG"; nocase; depth: 4; content:"|00|J"; offset: 10; depth: 2;
classtype: policy-violation; reference:url,doc.emergingthreats.net/2001254; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_Yahoo; sid:2001254; rev:5;)

#Commenting out, duplicated in Snort.org set
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET CHAT Yahoo IM ping"; flow: to_server,established; content:"YMSG"; nocase; depth: 4; content:"|00 12|"; offset: 10; depth: 2;
classtype: policy-violation; reference:url,doc.emergingthreats.net/2001255; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_Yahoo; sid:2001255; rev:6;)

#Commenting out, duplicated in Snort.org set
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET CHAT Yahoo IM conference invitation"; flow: from_server,established; content:"YMSG"; nocase; depth: 4; content:"|00 18|"; offset:
10; depth: 2; classtype: policy-violation; reference:url,doc.emergingthreats.net/2001256; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_Yahoo;
sid:2001256; rev:5;)

#Commenting out, duplicated in Snort.org set
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET CHAT Yahoo IM conference logon success"; flow: from_server,established; content:"YMSG"; nocase; depth: 4; content:"|00 19|";
offset: 10; depth: 2; classtype: policy-violation; reference:url,doc.emergingthreats.net/2001257; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_Yahoo;
sid:2001257; rev:5;)

#Commenting out, duplicated in Snort.org set
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET CHAT Yahoo IM conference message"; flow: to_server,established; content:"YMSG"; nocase; depth: 4; content:"|00 1D|"; offset: 10;
depth: 2; classtype: policy-violation; reference:url,doc.emergingthreats.net/2001258; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_Yahoo; sid:2001258;
rev:5;)

#Commenting out, duplicated in Snort.org set
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET CHAT Yahoo IM Unavailable Status"; flow: to_server,established; content:"|59 47 00 0b 00 00 00 00 00 12 00 00 00 00|"; depth: 55;
classtype: policy-violation; reference:url,doc.emergingthreats.net/2001427; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_Yahoo; sid:2001427; rev:5;)
```

```
#Commenting out, duplicated in Snort.org set
#
alert tcp $HOME_NET any <> $EXTERNAL_NET any (msg:"ET CHAT Yahoo IM file transfer request"; flow: established; content:"YMSG"; nocase; depth: 4; content:"|00|M"; offset: 10; depth: 2;
classtype: policy-violation; reference:url,doc.emergingthreats.net/2001259; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_Yahoo; sid:2001259; rev:6;)

#Commenting out, duplicated in Snort.org set
#
#alert tcp $HOME_NET any <> $EXTERNAL_NET any (msg:"ET CHAT Yahoo IM message"; flow: established; content:"YMSG"; depth: 4; classtype: policy-violation;
reference:url,doc.emergingthreats.net/2001260; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_Yahoo; sid:2001260; rev:6;)

#Commenting out, duplicated in Snort.org set
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET CHAT Yahoo IM successful chat join"; flow: from_server,established; content:"YMSG"; nocase; depth: 4; content:"|00 98|"; offset:
10; depth: 2; classtype: policy-violation; reference:url,doc.emergingthreats.net/2001261; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_Yahoo;
sid:2001261; rev:5;)

#Commenting out, duplicated in Snort.org set
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET CHAT Yahoo IM conference offer invitation"; flow: to_server,established; content:"YMSG"; nocase; depth: 4; content:"|00|P"; offset:
10; depth: 2; classtype: policy-violation; reference:url,doc.emergingthreats.net/2001262; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_Yahoo;
sid:2001262; rev:5;)

#Commenting out, duplicated in Snort.org set
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET CHAT Yahoo IM conference request"; flow: to_server,established; content:"<R"; depth: 2; pcre:"/^\x3c(REQIMG|RVWCFG)\x3e/ism";
classtype: policy-violation; reference:url,doc.emergingthreats.net/2001263; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_Yahoo; sid:2001263; rev:5;)

#Commenting out, duplicated in Snort.org set
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET CHAT Yahoo IM conference watch"; flow: from_server,established; content:"|0D 00 05 00|"; depth: 4; classtype: policy-violation;
reference:url,doc.emergingthreats.net/2001264; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_Yahoo; sid:2001264; rev:5;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CHAT Yahoo IM Client Install"; flow: to_server,established; uricontent:"/ycontent/stats.php?version="; nocase;
uricontent:"EVENT=InstallBegin"; nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/2002659; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_Yahoo; sid:2002659; rev:4;)

#by Chris Newton
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET 5050 (msg:"ET DELETED Yahoo Chat Signin Inside Webmail"; flow:established,to_server; content:"content-length|3a|"; nocase; depth:15; content:"
<Ymsg Command=|22|550|22|"; nocase; classtype:policy-violation; reference:url,yahoo.com; reference:url,doc.emergingthreats.net/2007066; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_Yahoo; sid:2007066; rev:4;)

#by Chris Newton
#
#alert tcp $EXTERNAL_NET 5050 -> $HOME_NET any (msg:"ET DELETED Yahoo Chat Signin Success Inside Webmail"; flow:established,to_server; content:"content-length|3a|"; nocase; depth:15;
content:"<Ymsg Command=|22|85|22|"; nocase; classtype:policy-violation; reference:url,yahoo.com; reference:url,doc.emergingthreats.net/2007067;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_Yahoo; sid:2007067; rev:4;)

#by Chris Newton
#
##alert tcp $EXTERNAL_NET 5050 <> $HOME_NET any (msg:"ET DELETED Yahoo Chat Activity Inside Webmail"; flow:established,to_server; content:"content-length|3a|"; nocase; depth:15;
content:"<Ymsg Command=|22|"; nocase; classtype:policy-violation; reference:url,yahoo.com; reference:url,doc.emergingthreats.net/2007068; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_Yahoo; sid:2007068; rev:4;)

#by Chris Newton
#
##alert tcp $EXTERNAL_NET 5050 <> $HOME_NET any (msg:"ET DELETED Yahoo Chat Activity Inside Webmail (2)"; flow:established,to_server; content:"<Ymsg Command=|22|"; depth:15; nocase;
classtype:policy-violation; reference:url,yahoo.com; reference:url,doc.emergingthreats.net/2007069; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IM_Yahoo;
sid:2007069; rev:3;)

#by matt jonkman
#these services aren't bad inherently, but are often used by trojans to get their external IP
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Internal Host Retrieving External IP via whatismyip.com Automation Page - Possible Infection";
flow:established,to_server; uricontent:"/automation/n09230945.asp"; classtype:attempted-recon; reference:url,doc.emergingthreats.net/2008985; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_IP_Check; sid:2008985; rev:2;)

#by matt jonkman
#these services aren't bad inherently, but are often used by trojans to get their external IP
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Internal Host Retrieving External IP via whatismyip.com - Possible Infection"; flow:established,to_server;
content:"GET "; depth:4; content:"|0d 0a|Host\: "; content:".whatismyip."; within:15; classtype:attempted-recon; reference:url,doc.emergingthreats.net/2008986;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IP_Check; sid:2008986; rev:2;)

#by matt jonkman
#these services aren't bad inherently, but are often used by trojans to get their external IP
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Internal Host Retrieving External IP via showip.net - Possible Infection"; flow:established,to_server; content:"GET
"; depth:4; content:"|0d 0a|Host\: "; content:".showip."; within:15; classtype:attempted-recon; reference:url,doc.emergingthreats.net/2008987; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_IP_Check; sid:2008987; rev:2;)

#by matt jonkman
#these services aren't bad inherently, but are often used by trojans to get their external IP
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Internal Host Retrieving External IP via cmyip.com - Possible Infection"; flow:established,to_server; content:"GET
"; depth:4; content:"|0d 0a|Host|3a| "; content:".cmyip."; within:12; classtype:attempted-recon; reference:url,doc.emergingthreats.net/2008988;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IP_Check; sid:2008988; rev:3;)

#by matt jonkman
#these services aren't bad inherently, but are often used by trojans to get their external IP
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Internal Host Retrieving External IP via showmyip.com - Possible Infection"; flow:established,to_server;
content:"GET "; depth:4; content:"|0d 0a|Host|3a| "; content:".showmyip."; within:15; classtype:attempted-recon; reference:url,doc.emergingthreats.net/2008989;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IP_Check; sid:2008989; rev:3;)

#by matt jonkman
#these services aren't bad inherently, but are often used by trojans to get their external IP
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Internal Host Retrieving External IP via ipchicken.com - Possible Infection"; flow:established,to_server;
content:"GET "; depth:4; content:"|0d 0a|Host|3a| "; content:".ipchicken.com"; within:25; classtype:attempted-recon; reference:url,doc.emergingthreats.net/2009020;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IP_Check; sid:2009020; rev:3;)

#Submitted by Vernon Stark
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY IRC authorization message"; flow: established; content:"NOTICE AUTH"; content:"Looking up your hostname..."; nocase;
classtype: misc-activity; reference:url,doc.emergingthreats.net/2000355; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IRC; sid:2000355; rev:5;)

#Submitted by Vernon Stark
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY IRC connection"; flow: established; content:"Welcome to the "; content:"IRC Network"; nocase; classtype: misc-activity;
reference:url,doc.emergingthreats.net/2000356; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IRC; sid:2000356; rev:5;)

#by Matt Jonkman
#
#alert ip any any -> any any (msg:"ET POLICY EIN in the clear (US-IRS Employer ID Number)"; pcre:"/ \d\d-\d{7} /"; classtype:policy-violation;
reference:url,policy.ssa.gov/poms.nsf/lnx/0101001004; reference:url,policy.ssa.gov/poms.nsf/lnx/0101001001?opendocument; reference:url,doc.emergingthreats.net/2002658;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_IRS_Related; sid:2002658; rev:4;)
```

```
#by Cam Beasley. Experimental, please report your experiences
#
##alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET DELETED Possible Image Spam Inbound (simple rule)"; flow:established,to_server; content:"Content-Transfer-Encoding|3A|";
content:"AMAgAOAgAABAACBAAEBAAGBAAIBAAKBAAMBAAOBAAABgACBgAEBgAGBgAIBgAKBgAMBgAOBg"; depth:575; content:"AACAACCAAECAAGCAAICAAKCAAMCAAOCAAACgACCgAECgAGCgAICgAKCgAMCgAOCgAADAACDA";
content:"AEDAAGDAAIDAAKDAAMDAAODAAADgACDgAEDgAGDgAIDgAKDgAMDgAODgAAAAQCAAQEAAQGAA"; classtype:misc-activity; reference:url,doc.emergingthreats.net/2003096;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_ImageSpam; sid:2003096; rev:4;)

#by Cam Beasley. Experimental, please report your experiences
#
##alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET DELETED Possible Image Spam Inbound (complex rule)"; flow:established,to_server; content:"Content-Transfer-Encoding|3A|";
content:"AMAgAOAgAABAACBAAEBAAGBAAIBAAKBAAMBAAOBAAABgACBgAEBgAGBgAIBgAKBgAMBgAOBg"; depth:575; content:"AACAACCAAECAAGCAAICAAKCAAMCAAOCAAACgACCgAECgAGCgAICgAKCgAMCgAOCgAADAACDA";
content:"AEDAAGDAAIDAAKDAAMDAAODAAADgACDgAEDgAGDgAIDgAKDgAMDgAODgAAAAQCAAQEAAQGAA"; content:"QIAAQKAAQMAAQOAAQAAgQCAgQEAgQGAgQIAgQKAgQMAgQOAgQABAQCBAQEBAQGBAQIBAQKBA";
content:"QMBAQOBAQABgQCBgQEBgQGBgQIBgQKBgQMBgQOBgQACAQCCAQECAQGCAQICAQKCAQMCAQOCA"; content:"QACgQCCgQECgQGCgQICgQKCgQMCgQOCgQADAQCDAQEDAQGDAQIDAQKDAQMDAQODAQADgQCDg";
content:"QEDgQGDgQIDgQKDgQMDgQODgQAAAgCAAgEAAgGAAgIAAgKAAgMAAgOAAgAAggCAggEAggGAg"; content:"gIAggKAggMAggOAggABAgCBAgEBAgGBAgIBAgKBAgMBAgOBAgABggCBggEBggGBggIBggKBg";
content:"gMBggOBggACAgCCAgECAgGCAgICAgKCAgMCAgOCAgACggCCggECggGCggICggKCggMCggOCg"; content:"gADAgCDAgEDAgGDAgIDAgKDAgMDAgODAgADggCDggEDggGDggIDggKDggMDggODggAAAwCAA";
content:"wEAAwGAAwIAAwKAAwMAAwOAAwAAgwCAgwEAgwGAgwIAgwKAgwMAgwOAgwABAwCBAwEBAwGBA"; content:"wIBAwKBAwMBAwOBAwABgwCBgwEBgwGBgwIBgwKBgwMBgwOBgwACAwCCAwECAwGCAwICAwKCA";
content:"wMCAwOCAwACgwCCgwECgwGCgwICgwKCgwMCgwOCgwADAwCDAwEDAwGDAwIDAwKDAwP/78KCg"; classtype:misc-activity; reference:url,doc.emergingthreats.net/2003097;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_ImageSpam; sid:2003097; rev:4;)

#Another from Cam Beasley
#
##alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET DELETED Possible Image Spam Inbound (3)"; flow:established,to_server; content:"Content-Transfer-Encoding|3A|"; content:"R0lGODlh";
depth:575; content:"AOAgAABAACBAAEBAAGBAAIBAAKBAAMBAAOBAAABgACBgAEBgAGBgAIBgAKBgAMBgAOBgAACAACCA";
content:"AECAAGCAAICAAKCAAMCAAOCAAACgACCgAECgAGCgAICgAKCgAMCgAOCgAADAACDAAEDAAGDAAIDA"; classtype:misc-activity; reference:url,doc.emergingthreats.net/2003120;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_ImageSpam; sid:2003120; rev:4;)

#from Russ Mcree
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY iTunes User Agent"; flow: established,to_server; content:"|0d 0a|User-Agent|3a| iTunes"; nocase; classtype:policy-
violation; threshold: type limit, count 1, seconds 360, track by_src; reference:url,hcsoftware.sourceforge.net/jason-rohrer/itms4all/; reference:url,doc.emergingthreats.net/2002878;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Itunes; sid:2002878; rev:7;)

#by kevin ross
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY Possible Multiple Levels of Javascript Encoding & Compression Filters in PDF, Possibly Hostile PDF";
flow:established,to_server; content:"PDF-"; nocase; depth:300; content:"/Filter"; nocase; distance:0; content:"Decode"; nocase; within:30; content:"Decode"; nocase; within:30;
content:"Decode"; nocase; within:30; content:"Decode"; nocase; within:30; content:"Decode"; nocase; within:30; content:"Decode"; nocase; within:30; classtype:misc-activity;
reference:url,www.symantec.com/connect/blogs/journey-center-pdf-stream; reference:url,doc.emergingthreats.net/2011008; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Java; sid:2011008; rev:2;)

#by mex
#
#alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"ET POLICY JBOSS/JMX port 80 access from outside"; flow:established,to_server; content:"GET"; nocase; depth:3; uricontent:"/jmx-
console"; nocase; classtype:web-application-attack; threshold:type limit, track by_src, count 1, seconds 60; reference:url,www.notsosecure.com/folder2/2009/10/27/hacking-jboss-with-jmx-
console/; reference:url,www.nruns.com/_downloads/Whitepaper-Hacking-jBoss-using-a-Browser.pdf; reference:url,doc.emergingthreats.net/2010377; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Jboss; sid:2010377; rev:3;)

#by mex
#
#alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 8080 (msg:"ET POLICY JBOSS/JMX port 8080 access from outside"; flow:established,to_server; content: "GET"; nocase; depth:3;
uricontent:"/jmx-console"; nocase; classtype:web-application-attack; threshold:type limit, track by_src, count 1, seconds 60;
reference:url,www.notsosecure.com/folder2/2009/10/27/hacking-jboss-with-jmx-console/; reference:url,www.nruns.com/_downloads/Whitepaper-Hacking-jBoss-using-a-Browser.pdf;
reference:url,doc.emergingthreats.net/2010378; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Jboss; sid:2010378; rev:3;)

#Submitted by Jonathan Miner
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET DELETED KitCo Kcast Ticker (agtray)"; flow: to_server,established; uricontent:"/pr/agtray.txt"; nocase; classtype:
policy-violation; reference:url,doc.emergingthreats.net/2000569; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Kitco_Ticker; sid:2000569; rev:6;)

#Submitted by Jonathan Miner
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET DELETED KitCo Kcast Ticker (autray)"; flow: to_server,established; uricontent:"/pr/autray.txt"; nocase; classtype:
policy-violation; reference:url,doc.emergingthreats.net/2000570; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Kitco_Ticker; sid:2000570; rev:6;)

#by William Metcalf
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Logmein.com Host List Download"; flow:established,to_server; content:"GET "; depth:4;
uricontent:"/myrahost/list.aspx?"; nocase; content:!"|0d 0a|Host|3a| "; classtype:policy-violation; reference:url,doc.emergingthreats.net/2007765;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Logmein.com; sid:2007765; rev:4;)

#by William Metcalf
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Logmein.com Update Activity"; flow:to_server,established; content:"GET "; depth:4;
uricontent:"/update.logmein.com/"; nocase; content:!"|0d 0a|Host|3a| "; classtype:policy-violation; reference:url,doc.emergingthreats.net/2007766;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Logmein.com; sid:2007766; rev:4;)

#by William Bell
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET POLICY MP3 File Transfer Outbound"; flow:established; content:"ID3|03|"; content:"TIT2"; distance:6; within:10; classtype:policy-
violation; reference:url,filext.com/detaillist.php?extdetail=mp3&Search=Search; reference:url,doc.emergingthreats.net/2002722; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_MP3_Files; sid:2002722; rev:4;)

#by William Bell
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY MP3 File Transfer Inbound"; flow: established; content:"ID3|03|"; content:"TIT2"; distance:6; within:10; classtype:policy-
violation; reference:url,filext.com/detaillist.php?extdetail=mp3&Search=Search; reference:url,doc.emergingthreats.net/2002723; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_MP3_Files; sid:2002723; rev:4;)

#by Jeff Kell
#Microsoft teredo tunnel
#
alert udp $HOME_NET any -> $EXTERNAL_NET 3544 (msg:"ET POLICY Microsoft TEREDO IPv6 tunneling"; content:"|FE 80 00 00 00 00 00 00 80 00|TEREDO"; offset:21; depth:16; classtype:misc-
activity; reference:url,doc.emergingthreats.net/2003155; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_MS_Teredo_Tunnel; sid:2003155; rev:4;)

#by Stephen Nesman at Monster.com
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET DELETED Majestic-12 Spider Bot User-Agent (MJ12bot)"; flow:to_server,established; content:"|0d 0a|User-Agent\: MJ12bot|0d
0a|"; classtype:trojan-activity; reference:url,www.majestic12.co.uk/; reference:url,doc.emergingthreats.net/2003409; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Majestic-12; sid:2003409; rev:4;)

#by cunningpike
#
##alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET DELETED Majestic-12 Spider Bot User-Agent Inbound (MJ12bot)"; flow:to_server,established; content:"|0d 0a|User-Agent\:
MJ12bot"; classtype:trojan-activity; reference:url,www.majestic12.co.uk/; reference:url,doc.emergingthreats.net/2007762; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Majestic-12; sid:2007762; rev:4;)

#Matt Jonkman
#This will let you know when McAffee is updating sigs. Not a security threat, but could be of interest to folks using mcafee to track updates
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY McAfee Update User Agent (McAfee AutoUpdate)"; flow:to_server,established; content:"User-Agent|3a| "; nocase;
content:"McAfee AutoUpdate"; within:50; pcre:"/User-Agent\:[^\n]+McAfee AutoUpdate/i"; classtype:not-suspicious; reference:url,doc.emergingthreats.net/2003381;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_McAffee; sid:2003381; rev:5;)

#by Will Metcalf
#Rapidshare is a video sharing service, uses VERY ppor auth, and can be used for non-work appropriate material.
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET DELETED Metacafe.com family filter off"; flow:established,to_server; content:"POST "; depth:5; content:"Host|3a|
```

www.metacafe.com"; content:"submit=Continue+-+I%27m+over+18"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2006367; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Metacafe; sid:2006367; rev:5;)

#by Will Metcalf
#Rapidshare is a video sharing service, uses VERY ppor auth, and can be used for non-work appropriate material.
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET DELETED Rapidshare download unauthd image post"; flow:to_server,established; content:"POST "; depth: 5; uricontent:"/files/"; nocase; content:"Host|3a|"; nocase; content:"rapidshare.com"; nocase; within: 40; content:"&accesscode="; nocase; content:"&actionstring=Download"; nocase; within:50; classtype:policy-violation; reference:url,en.wikipedia.org/wiki/RapidShare; reference:url,doc.emergingthreats.net/2006368; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Metacafe; sid:2006368; rev:5;)

#by Will Metcalf
#Rapidshare is a video sharing service, uses VERY poor auth, and can be used for non-work appropriate material.
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Rapidshare auth cookie download"; flow:to_server,established; content:"GET "; depth: 4; uricontent:"/files/"; content:"Host|3a|"; nocase; content:"rapidshare.com"; nocase; within:40; content:"Cookie|3a| user="; nocase; classtype:policy-violation; reference:url,en.wikipedia.org/wiki/RapidShare; reference:url,doc.emergingthreats.net/2006369; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Metacafe; sid:2006369; rev:5;)

#by Jamian Mason of Deepnines.com
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Metacafe.com Social Site Access"; flow:established,to_server; content:"Host|3a| www.metacafe.com"; threshold: type both, track by_src, count 5, seconds 300; classtype:policy-violation; reference:url,doc.emergingthreats.net/2003457; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Metacafe.com; sid:2003457; rev:4;)

#by Kevin Ross and others
#
alert tcp $EXTERNAL_NET 443 -> $HOME_NET any (msg:"ET POLICY Metasploit Framework Update"; flow:from_server,established; content:"http|3A|//certificates.godaddy.com/repository"; content: "metasploit.com"; distance:0; classtype:misc-activity; reference:url,www.metasploit.com/framework/; reference:url,www.ethicalhacker.net/content/view/29/24/; reference:url,doc.emergingthreats.net/2008418; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Metasploit; sid:2008418; rev:4;)

#by Kevin Ross
#
##alert tcp $HOME_NET any -> 76.74.9.18 $HTTP_PORTS (msg:"ET DELETED Milw0rm Exploit Archive Download"; content:"GET /sploits/milw0rm.tar.bz2"; depth:60; flow:to_server,established; classtype:misc-activity; reference:url,www.milw0rm.com; reference:url,doc.emergingthreats.net/2008524; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Metasploit; sid:2008524; rev:2;)

#by Kevin Ross
#
##alert tcp $HOME_NET any -> 76.74.9.19 $HTTP_PORTS (msg:"ET DELETED Packetstormsecurity Exploits Of The Month Download"; content:"GET /"; uricontent:"-exploits.tgz"; depth:70; flow:to_server,established; classtype:misc-activity; reference:url,www.packetstormsecurity.org; reference:url,doc.emergingthreats.net/2008525; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Metasploit; sid:2008525; rev:2;)

#by wolvee
#
##alert tcp $HOME_NET any -> 76.74.9.18 $HTTP_PORTS (msg:"ET DELETED Milw0rm Exploit Launch Attempt"; flow:to_server,established; content:"GET "; depth:4; uricontent:"/exploit.php?id="; nocase; classtype:misc-activity; reference:url,www.milw0rm.com; reference:url,doc.emergingthreats.net/2009586; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Milw0rm.com; sid:2009586; rev:3;)

#Submitted by Joseph Gama
#
##alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY Mozilla XPI install files download"; flow: from_server,established; content:"content-type|3a| application/x-xpinstall"; nocase; classtype: bad-unknown; reference:url,doc.emergingthreats.net/2001114; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Mozilla_XPI_Install; sid:2001114; rev:8;)

#by dajackman, updated by Mike Wall at BLCPro, LLC
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Myspace Login Attempt"; flow:established,to_server; content:"secure.myspace.com"; uricontent:"/index.cfm?fuseaction=login"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002872; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Myspace; sid:2002872; rev:5;)

#by Matt Jonkman
#These sigs aren't signs of hostile activity, just something of interest in some places
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY Nagios HTTP Monitoring Connection"; flow:established,to_server; content:"User-Agent|3a| check_http/"; nocase; content:"(nagios-plugins "; nocase; within:30; classtype:not-suspicious; reference:url,doc.emergingthreats.net/2006779; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Nagios; sid:2006779; rev:5;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET 443 -> $HOME_NET any (msg:"ET POLICY Nessus Vulnerability Scanner Plugins Update"; flow:to_client,established; content:"plugins.nessus.org"; content:"https|3a|//www.thawte.com/repository/index.html"; offset:432; depth:88; distance:10; classtype:misc-activity; reference:url,www.nessus.org/nessus/; reference:url,www.nessus.org/plugins/; reference:url,doc.emergingthreats.net/2009706; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Nessus; sid:2009706; rev:4;)

#by Will Metcalf, Netflix on demand UA
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Netflix On-demand User-Agent"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| WmpHostInternetConnection"; nocase; classtype:policy-violation; reference:url,doc.emergingthreats.net/2007638; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Netflix; sid:2007638; rev:5;)

#Submitted by Lance Boon
#
alert udp any any -> any any (msg:"ET POLICY Netop Remote Control Usage"; content:"|554b303037363053374730|"; classtype: policy-violation; reference:url,www.netop.com; reference:url,doc.emergingthreats.net/2001597; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Netop_Remote_Control; sid:2001597; rev:5;)

#by Jamian Mason of Deepnines.com
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET DELETED Netvacy.com Anonymizing Proxy Access"; flow:established,to_server; content:"Host|3a| www.netvacy.com"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2003453; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Netvacy.com; sid:2003453; rev:4;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Netviewer.com Remote Control Proxy Test"; flow:established,to_server; content:"POST /nvserver HTTP"; depth:19; content:"|0d 0a 0d 0a|cmd="; content:"&params="; distance:0; content:"Netviewer Proxy Test"; distance:0; classtype:policy-violation; reference:url,doc.emergingthreats.net/2008472; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Netviewer.com; sid:2008472; rev:3;)

#by James Pledger
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Newzbin Usenet Reader License Check"; flow:established,to_server; uricontent:"/internal/internal_loader.v2.php?"; uricontent:"prodID=nl&licID="; uricontent:"&prodVer="; content:"|0d 0a|Host|3A| www.newsleecher.com"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2009095; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Newzbin; sid:2009095; rev:2;)

#by matt jonkman
#nginx is an open http server. It's quite good, but seems an extremely high number of it's
#installs are malicious. Storm, rbn, etc. Use this rule if you are interested
#disabling by default, falses a lot but may be of interest to some folks
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY Nginx Server in use - Often Hostile Traffic"; flow:established,from_server; content:"|0d 0a|Server|3a| nginx"; nocase; threshold:type limit, seconds 60, count 3, track by_src; classtype:bad-unknown; reference:url,doc.emergingthreats.net/2008054; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Nginx; sid:2008054; rev:4;)

#by matt jonkman
#nginx is an open http server. It's quite good, but seems an extremely high number of it's
#installs are malicious. Storm, rbn, etc. Use this rule if you are interested
#disabling by default, falses a lot but may be of interest to some folks
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY Nginx Server with no version string - Often Hostile Traffic"; flow:established,from_server; content:"|0d 0a|Server|3a| nginx|0d 0a|"; nocase; threshold:type limit, seconds 60, count 3, track by_src; classtype:bad-unknown; reference:url,doc.emergingthreats.net/2008064; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Nginx; sid:2008064; rev:3;)

```
#by matt jonkman
#nginx is an open http server. It's quite good, but seems an extremely high number of it's
#installs are malicious. Storm, rbn, etc. Use this rule if you are interested
#disabling by default, falses a lot but may be of interest to some folks
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY Nginx Server with modified version string - Often Hostile Traffic"; flow:established,from_server; content:"HTTP/1.";
depth:7; content:"|0d 0a|Server|3a| nginx/"; nocase; pcre:"/Server\: nginx/[a-zA-Z]/i"; threshold:type limit, seconds 60, count 3, track by_src; classtype:bad-unknown;
reference:url,doc.emergingthreats.net/2008065; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Nginx; sid:2008065; rev:3;)

#New way to do ssh. First to detect legit ssh sessions on normal ports. Enable these ONLY if you need to know about
#normal ssh sessions
#Written by Erik Fichtner, adapted some
#
#alert tcp any $SSH_PORTS -> any any (msg:"ET POLICY SSH Server Banner Detected on Expected Port"; flowbits:noalert; flow: from_server,established; content:"SSH-"; offset: 0; depth: 4;
byte_test:1,>,48,0,relative; byte_test:1,<,51,0,relative; byte_test:1,=,46,1,relative; flowbits: set,is_ssh_server_banner; classtype:misc-activity;
reference:url,doc.emergingthreats.net/2001973; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Non-Standard_SSH_Port; sid:2001973; rev:7;)

#New way to do ssh. First to detect legit ssh sessions on normal ports. Enable these ONLY if you need to know about
#normal ssh sessions
#Written by Erik Fichtner, adapted some
#
#alert tcp any any -> any $SSH_PORTS (msg:"ET POLICY SSH Client Banner Detected on Expected Port"; flowbits:isset,is_ssh_server_banner; flowbits:noalert; flow: from_client,established;
content:"SSH-"; offset: 0; depth: 4; byte_test:1,>,48,0,relative; byte_test:1,<,51,0,relative; byte_test:1,=,46,1,relative; flowbits: set,is_ssh_client_banner; classtype:misc-activity;
reference:url,doc.emergingthreats.net/2001974; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Non-Standard_SSH_Port; sid:2001974; rev:7;)

#New way to do ssh. First to detect legit ssh sessions on normal ports. Enable these ONLY if you need to know about
#normal ssh sessions
#Written by Erik Fichtner, adapted some
#
#alert tcp any any -> any $SSH_PORTS (msg:"ET POLICY SSHv2 Server KEX Detected on Expected Port"; flowbits:isset,is_ssh_client_banner; flowbits:noalert; flow: from_server,established;
byte_test:1,=,20,5; flowbits: set,is_ssh_server_kex; classtype:misc-activity; reference:url,doc.emergingthreats.net/2001975; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Non-Standard_SSH_Port; sid:2001975; rev:7;)

#New way to do ssh. First to detect legit ssh sessions on normal ports. Enable these ONLY if you need to know about
#normal ssh sessions
#Written by Erik Fichtner, adapted some
#
#alert tcp any any -> any $SSH_PORTS (msg:"ET POLICY SSHv2 Client KEX Detected on Expected Port"; flowbits:isset,is_ssh_server_kex; flowbits:noalert; flow: from_client,established;
byte_test:1,=,20,5; flowbits: set,is_ssh_client_kex; classtype:misc-activity; reference:url,doc.emergingthreats.net/2001976; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Non-Standard_SSH_Port; sid:2001976; rev:8;)

#New way to do ssh. First to detect legit ssh sessions on normal ports. Enable these ONLY if you need to know about
#normal ssh sessions
#Written by Erik Fichtner, adapted some
#
#alert tcp any any -> any $SSH_PORTS (msg:"ET POLICY SSHv2 Client New Keys detected on Expected Port"; flowbits:noalert; flowbits:isset,is_ssh_client_kex; flow: from_client,established;
byte_test:1,=,21,5; flowbits: set,is_proto_ssh; classtype:misc-activity; reference:url,doc.emergingthreats.net/2001977; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Non-Standard_SSH_Port; sid:2001977; rev:8;)

#New way to do ssh. First to detect legit ssh sessions on normal ports. Enable these ONLY if you need to know about
#normal ssh sessions
#Written by Erik Fichtner, adapted some
#
#alert tcp any any <> any $SSH_PORTS (msg:"ET POLICY SSH session in progress on Expected Port"; flowbits: isset,is_proto_ssh; threshold: type both, track by_src, count 2, seconds 300;
classtype:misc-activity; reference:url,doc.emergingthreats.net/2001978; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Non-Standard_SSH_Port; sid:2001978;
rev:6;)

#And now to detect Non-standard port usage
#
#alert tcp any !$SSH_PORTS -> any any (msg:"ET POLICY SSH Server Banner Detected on Unusual Port"; flowbits:noalert; flow: from_server,established; content:"SSH-"; offset: 0; depth: 4;
byte_test:1,>,48,0,relative; byte_test:1,<,51,0,relative; byte_test:1,=,46,1,relative; flowbits: set,is_ssh_server_banner; classtype:misc-activity;
reference:url,doc.emergingthreats.net/2001979; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Non-Standard_SSH_Port; sid:2001979; rev:7;)

#And now to detect Non-standard port usage
#
#alert tcp any any -> any !$SSH_PORTS (msg:"ET POLICY SSH Client Banner Detected on Unusual Port"; flowbits:isset,is_ssh_server_banner; flow: from_client,established; content:"SSH-";
offset: 0; depth: 4; byte_test:1,>,48,0,relative; byte_test:1,<,51,0,relative; byte_test:1,=,46,1,relative; flowbits: set,is_ssh_client_banner; classtype:misc-activity;
reference:url,doc.emergingthreats.net/2001980; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Non-Standard_SSH_Port; sid:2001980; rev:9;)

#And now to detect Non-standard port usage
#
#alert tcp any !$SSH_PORTS -> any any (msg:"ET POLICY SSHv2 Server KEX Detected on Unusual Port"; flowbits:isset,is_ssh_client_banner; flowbits:noalert; flow: from_server,established;
byte_test:1,=,20,5; flowbits: set,is_ssh_server_kex; classtype:misc-activity; reference:url,doc.emergingthreats.net/2001981; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Non-Standard_SSH_Port; sid:2001981; rev:7;)

#And now to detect Non-standard port usage
#
#alert tcp any any -> any !$SSH_PORTS (msg:"ET POLICY SSHv2 Client KEX Detected on Unusual Port"; flowbits:noalert; flowbits:isset,is_ssh_server_kex; flow: from_client,established;
byte_test:1,=,20,5; flowbits: set,is_ssh_client_kex; classtype:misc-activity; reference:url,doc.emergingthreats.net/2001982; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Non-Standard_SSH_Port; sid:2001982; rev:8;)

#And now to detect Non-standard port usage
#
#alert tcp any any -> any !$SSH_PORTS (msg:"ET POLICY SSHv2 Client New Keys Detected on Unusual Port"; flowbits:isset,is_ssh_client_kex; flowbits:noalert; flow: from_client,established;
byte_test:1,=,21,5; flowbits: set,is_proto_ssh; classtype:misc-activity; reference:url,doc.emergingthreats.net/2001983; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Non-Standard_SSH_Port; sid:2001983; rev:8;)

#And now to detect Non-standard port usage
#
#alert tcp any !$SSH_PORTS -> any !$SSH_PORTS (msg:"ET POLICY SSH session in progress on Unusual Port"; flowbits: isset,is_proto_ssh; threshold: type both, track by_src, count 2,
seconds 300; classtype:misc-activity; reference:url,doc.emergingthreats.net/2001984; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Non-Standard_SSH_Port;
sid:2001984; rev:7;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET POLICY External Unencrypted Connection to Ossec WUI"; flow:established,to_server; uricontent:"/ossec/";
uricontent:"js/calendar-setup.js"; classtype:misc-activity; reference:url,www.ossec.net; reference:url,doc.emergingthreats.net/2008569; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_OSSEC; sid:2008569; rev:2;)

#by evilghost
#
#alert tcp $HOME_NET $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET POLICY Exchange 2003 OWA plain-text E-Mail message access, not SSL"; flow:established,from_server; content:"var g_szURL =
\"http|3a|//"; content:"var g_szFolder = \"";  content:"varg_szVirtualRoot = \"http\://"; content:"Microsoft Corporation."; classtype:web-application-activity;
reference:url,support.microsoft.com/kb/321832; reference:url,doc.emergingthreats.net/2010030; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_OWA;
sid:2010030; rev:4;)

#by Christopher Campesi
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 16680 (msg:"ET POLICY OperaUnite URL Registration"; flow:to_server,established; content:"REGISTER"; offset:0; depth:8; content:"operaunite.com";
within:109; classtype:policy-violation; reference:url,unite.opera.com; reference:url,doc.emergingthreats.net/2009895; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_OperaUnite; sid:2009895; rev:3;)

#by Jamian Mason of Deepnines.com
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Orkut.com Social Site Access"; flow:established,to_server; content:"Host|3a| www.orkut.com"; threshold: type both,
track by_src, count 5, seconds 300; classtype:policy-violation; reference:url,doc.emergingthreats.net/2003458; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Orkut.com; sid:2003458; rev:4;)
```

```
#Submitted by Scott Melnick
#
##alert tcp $HOME_NET any -> any !$HTTP_PORTS (msg:"ET DELETED PCMesh Anonymous Proxy client connect"; flow: from_client,established; content:"http|3a|//www.pcmesh.com|3a|80/ip-
check.cgi"; depth:37; offset:4; classtype: policy-violation; reference:url,doc.emergingthreats.net/2003040; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_PCMesh; sid:2003040; rev:4;)

#Only enable if you do not use and internal Proxy server with your
#clients or change your HTTP_PORTS to match your Proxy server port
#
##alert tcp $HOME_NET any -> any !$HTTP_PORTS (msg:"ET DELETED Anonymous Proxy Traffic from Inside"; flow: from_client,established; flags: *AP,12; content:"GET http|3a|//"; depth:11;
offset:0; content:"HTTP/1.0"; within:50; offset:11; classtype: policy-violation; reference:url,doc.emergingthreats.net/2003069; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_PCMesh; sid:2003069; rev:3;)

#by kevin ross
#Disabled by default as they may be high load
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET DELETED Hex Obfuscated arguments.callee Javascript Method in PDF - Possibly Hostile PDF"; flow:established,to_client;
content:"PDF-"; nocase; depth:300; content:"|61|"; distance:0; content:"|72|"; distance:1; within:2; content:"|67|"; distance:1; within:2; content:"|75|"; distance:1; within:2;
content:"|6d|"; distance:1; within:2; content:"|65|"; distance:1; within:2; content:"|6e|"; distance:1; within:2; content:"|74|"; distance:1; within:2; content:"|73|"; distance:1;
within:2; content:"|2e|"; distance:1; within:2; content:"|63|"; distance:1; within:2; content:"|61|"; distance:1; within:2; content:"|6c|"; distance:1; within:2; content:"|6c|";
distance:1; within:2; content:"|65|"; distance:1; within:2; content:"|65|"; distance:1; within:2; classtype:misc-activity; reference:url,doc.emergingthreats.net/2010879;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_PDF; sid:2010879; rev:2;)

#by kevin ross
#Disabled by default as they may be high load
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET DELETED Possible Hex Obfuscation of Javascript Declaration Within PDF File - Likely Hostile"; flow:established,to_client;
content:"PDF-"; nocase; depth:300; content:"|2f|"; distance:0; content:"|4a|"; distance:1; within:2; content:"|61|"; distance:1; within:2; content:"|76|"; distance:1; within:2;
content:"|61|"; distance:1; within:2; content:"|73|"; distance:1; within:2; content:"|63|"; distance:1; within:2; content:"|72|"; distance:1; within:2; content:"|69|"; content:"|70|";
distance:1; within:2; content:"|74|"; distance:1; within:2; classtype:misc-activity; reference:url,doc.emergingthreats.net/2010880; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_PDF; sid:2010880; rev:2;)

#by kevin ross
#Disabled by default as they may be high load
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY .pdf File Containing Javascript"; flow:established,to_client; content:"PDF-"; nocase; depth:300;
content:"/Javascript"; nocase; distance:0; classtype:misc-activity; reference:url,doc.emergingthreats.net/2010882; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_PDF; sid:2010882; rev:2;)

#by kevin ross
#Disabled by default as they may be high load
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY PDF File Containing arguments.callee in Cleartext - Likely Hostile"; flow:established,to_client; content:"PDF-";
nocase; depth:300; content:"arguments.callee"; nocase; distance:0; classtype:misc-activity; reference:url,isc.sans.org/diary.html?storyid=1519; reference:url,isc.sans.org/diary.html?
storyid=7906; reference:url,doc.emergingthreats.net/2010883; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_PDF; sid:2010883; rev:3;)

#disabled as it may be high load
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET DELETED .pdf File Possibly Containing Basic Hex Obfuscation"; flow:established,from_server; content:"PDF-"; nocase;
depth:300; pcre:"/PDF-.+[0-9,A-F][0-9,A-F].[0-9,A-F][0-9,A-F].[0-9,A-F][0-9,A-F].[0-9,A-F][0-9,A-F].[0-9,A-F][0-9,A-F].[0-9,A-F][0-9,A-F].[0-9,A-F][0-9,A-F]/si"; classtype:misc-activity;
reference:url,isc.sans.org/diary.html?storyid=7903; reference:url,isc.sans.org/diary.html?storyid=7906; reference:url,doc.emergingthreats.net/2010884;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_PDF; sid:2010884; rev:3;)

#by Will Metcalf. These will detect a php proxy/anonymizer/content control evasion site in use
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET DELETED PHP Anonymizing/Evasion Proxy In Use"; flow: to_server,established; content:"GET "; depth: 4;
uricontent:"/index.php?q="; nocase; pcre:"/index\.php\?q=(uggc|jjj|http|www|aHR0c|d3d3)/Ui"; classtype:policy-violation; reference:url,sourceforge.net/projects/php-proxy/;
reference:url,doc.emergingthreats.net/2006410; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_PHP_Proxy; sid:2006410; rev:5;)

#by Jaime Blasco
#Needs tweaking ... aight, tweaked... needs testing now :)
#
alert tcp $HOME_NET 1723 -> $EXTERNAL_NET any (msg:"ET POLICY PPTP Requester is not authorized to establish a command channel"; flow:to_server,established,no_stream; content:"|00 01|";
offset:2; depth:4; content:"|00 02|"; offset:8; depth:10; content:"|04|"; offset:12; depth:13; classtype:attempted-admin; reference:url,tools.ietf.org/html/rfc2637;
reference:url,doc.emergingthreats.net/2009387; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_PPTP; sid:2009387; rev:3;)

#by jack pepper
#
#alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET POLICY Login Credentials Possibly Passed in URI"; flow:established,to_server; uricontent:"username="; nocase;
uricontent:"password="; nocase; classtype:policy-violation; reference:url,doc.emergingthreats.net/2009001; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Pass_in_uri; sid:2009001; rev:3;)

#disabled by default for possiblity of false positives. Use only if needed
#
#alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET POLICY Login Credentials Possibly Passed in POST Data"; flow:established,to_server; content:"POST "; depth:5;
content:"|0d 0a 0d 0a|"; content:"username="; distance:0; nocase; content:"password="; nocase; classtype:policy-violation; reference:url,doc.emergingthreats.net/2009004;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Pass_in_uri; sid:2009004; rev:4;)

#by Jonathan Scheidell
#Pingdom.com is an otherwise legitimate org that does free distributed ping monitoring
#This sig will let you know if you're being monitored.
#
#alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET POLICY Pingdom.com Monitoring detected"; flow:to_server,established; content:"User-Agent|3a| Pingdom"; nocase;
classtype:attempted-recon; reference:url,royal.pingdom.com/?p=46; reference:url,doc.emergingthreats.net/2003214; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Pingdom_Monitoring; sid:2003214; rev:5;)

#This will tell you if a local host is signed up as a pingdom monitoring node
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Pingdom.com Monitoring Node Active"; flow: to_server,established; content: "User-Agent|3a| Pingdom"; nocase;
classtype:attempted-recon; reference:url,royal.pingdom.com/?p=46; reference:url,doc.emergingthreats.net/2003215; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Pingdom_Monitoring; sid:2003215; rev:5;)

#Added by Frank Knobbe
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET DELETED Prospero Chat Session in Progress"; flow: established,to_server; content:"PCHAT2 "; offset: 0; depth: 7; content:"v='";
nocase; offset: 8; depth: 400; content:"jv='"; nocase; offset: 8; depth: 400; content:"u='"; nocase; offset: 8; depth: 400; classtype: policy-violation;
reference:url,www.prospero.com/technology.htm; reference:url,doc.emergingthreats.net/2001989; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Prospero_Chat;
sid:2001989; rev:5;)

#From Adam Hogan
#
#alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET POLICY Proxy GET Request"; flow: to_server,established; content:"GET http|3a|//"; nocase; depth: 11; classtype: bad-
unknown; reference:url,doc.emergingthreats.net/2001669; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Proxy; sid:2001669; rev:8;)

#From Adam Hogan
#
#alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET POLICY Proxy HEAD Request"; flow: to_server,established; content:"HEAD http|3a|//"; nocase; depth: 12; classtype: bad-
unknown; reference:url,doc.emergingthreats.net/2001670; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Proxy; sid:2001670; rev:9;)

#From Adam Hogan
#
#alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET POLICY Proxy POST Request"; flow: to_server,established; content:"POST http|3a|//"; nocase; depth: 12; classtype: bad-
unknown; reference:url,doc.emergingthreats.net/2001674; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Proxy; sid:2001674; rev:8;)

#From Adam Hogan
#
#alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET POLICY Proxy CONNECT Request"; flow: to_server,established; content:"CONNECT "; nocase; depth: 8; classtype: bad-
unknown; reference:url,doc.emergingthreats.net/2001675; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Proxy; sid:2001675; rev:7;)
```

```
#by Markus Manzke
#HTTP-TRACE Request
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET POLICY Proxy TRACE Request - inbound"; flow: to_server,established; content:"TRACE "; nocase; depth: 6; classtype: bad-
unknown; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Proxy; reference:url,doc.emergingthreats.net/2010766; sid:2010766; rev:9;)

#by Markus Manzke
#HTTP-TRACE Request
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY TRACE Request - outbound"; flow: to_server,established; content:"TRACE "; nocase; depth: 6; classtype: bad-unknown;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Proxy; reference:url,doc.emergingthreats.net/2010767; sid:2010767; rev:9;)

#BY Sandro Reis.
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Possible ProxyShell Anonymous Access Connection"; flow:established,to_server; uricontent:"/services/get_proxies/";
classtype:policy-violation; reference:url,doc.emergingthreats.net/2010969; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/sigs/POLICY/POLICY_ProxyShell; sid:2010969;
rev:2;)

#by waldo kitty
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Possible ProxyShell Hide IP Installation file download"; flow:established,to_server; content:"GET "; nocase;
depth:4; uricontent:"/proxyshell_hide_ip_setup.exe"; nocase; classtype:policy-violation; reference:url,www.browserdefender.com/file/484661/site/putas18.info/;
reference:url,doc.emergingthreats.net/2010792; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_ProxyShell; sid:2010972; rev:3;)

#Seeing some bots and proxy evasion apps use these proxy judges to find their way out
#by Scotty Melnick
#
alert tcp any any -> any $HTTP_PORTS (msg:"ET POLICY Proxy Judge Discovery/Evasion (prxjdg.cgi)"; flow: established,to_server; uricontent:"/prxjdg.cgi"; nocase; classtype:policy-
violation; reference:url,doc.emergingthreats.net/2003047; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Proxy_Judge; sid:2003047; rev:3;)

#Seeing some bots and proxy evasion apps use these proxy judges to find their way out
#by Scotty Melnick
#
alert tcp any any -> any $HTTP_PORTS (msg:"ET POLICY Proxy Judge Discovery/Evasion (proxyjudge.cgi)"; flow: established,to_server; uricontent:"/proxyjudge.cgi"; nocase;
classtype:policy-violation; reference:url,doc.emergingthreats.net/2003048; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Proxy_Judge; sid:2003048; rev:3;)

#by Jeremy at sudosecure
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Set flow on rar file get"; flow:established,to_server; content:"GET "; depth:4; uricontent:".rar"; content:".rar
HTTP/1."; flowbits:set,ET.rar_seen; flowbits:noalert; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008781; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_RAR_Files; sid:2008781; rev:3;)

#by Jeremy at sudosecure
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY Possible Trojan File Download bad rar file header (not a valid rar file)"; flow:established,from_server;
content:"Content-Type|3a| application|2f|octet-stream"; content:"|0d 0a 0d 0a 52 61 72 21|"; distance:0; content:!"|1A 07|"; within:2; classtype:trojan-activity; reference:url,www.win-
rar.com/index.php?id=24&kb=1&kb_article_id=162; reference:url,doc.emergingthreats.net/2008782; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_RAR_Files;
sid:2008782; rev:2;)

#by Jeremy at sudosecure
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY Possible Trojan File Download - Rar Requested but not received"; flow:established,from_server;
flowbits:isset,ET.rar_seen; flowbits:unset,ET.rar_seen; content:"200 OK"; content:"Content-Type|3a| application|2f|octet-stream"; content:!"|0d 0a 0d 0a 52 61 72 21 1A 07|";
classtype:trojan-activity; reference:url, www.win-rar.com/index.php?id=24&kb=1&kb_article_id=162; reference:url,doc.emergingthreats.net/2008783;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_RAR_Files; sid:2008783; rev:3;)

#Submitted by James Ashton
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 3389 (msg:"ET POLICY RDP connection request"; flow: to_server,established; content:"|03|"; offset: 0; depth: 1; content:"|E0|"; offset: 5;
depth: 1; classtype: misc-activity; reference:url,doc.emergingthreats.net/2001329; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_RDP_Connections;
sid:2001329; rev:8;)

#Submitted by James Ashton
#
alert tcp $HOME_NET 3389 -> $EXTERNAL_NET any (msg:"ET POLICY RDP connection confirm"; flow: from_server,established; content:"|03|"; offset: 0; depth: 1; content:"|D0|"; offset: 5;
depth: 1; classtype: misc-activity; reference:url,doc.emergingthreats.net/2001330; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_RDP_Connections;
sid:2001330; rev:8;)

#Submitted by James Ashton
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 3389 (msg:"ET POLICY RDP disconnect request"; flow: to_server,established; content:"|03|"; offset: 0; depth: 1; content:"|80|"; offset: 5;
depth: 1; classtype: misc-activity; reference:url,doc.emergingthreats.net/2001331; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_RDP_Connections;
sid:2001331; rev:8;)

#By Scott Melnick
#Users can connect to remote machines by port forwarding 3389 through personal routers.
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET !3389 (msg:"ET POLICY Remote Desktop Connection via non RDP Port"; flow:established,to_server; content:"|03|"; offset: 0; depth: 1;
content:"|E0|"; offset: 5; depth: 1; content:"Cookie|3a|"; offset: 11; depth: 7; classtype: policy-violation; reference:url,doc.emergingthreats.net/2007571;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_RDP_Connections; sid:2007571; rev:5;)

#Matt Jonkman
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 1024:65535 (msg:"ET POLICY Radmin Remote Control Session Setup Initiate"; flow:established,to_server; content:"|01 00 00 00 01 00 00 00 08 08|";
flowbits:set,BE.Radmin.Challenge; classtype:not-suspicious; reference:url,www.radmin.com; reference:url,doc.emergingthreats.net/2003479; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Radmin; sid:2003479; rev:4;)

#Matt Jonkman
#
alert tcp $HOME_NET 1024:65535 -> $EXTERNAL_NET any (msg:"ET POLICY Radmin Remote Control Session Setup Response"; flowbits:isset,BE.Radmin.Challenge; flow:established,from_server;
dsize:<50; content:"|01 00 00 00 25 00 00 02 12 08 02 00 00 0a 00 00 00 00 00 00|"; flowbits:noalert; classtype:not-suspicious; reference:url,www.radmin.com;
reference:url,doc.emergingthreats.net/2003480; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Radmin; sid:2003480; rev:4;)

#Matt Jonkman
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 1024:65535 (msg:"ET POLICY Radmin Remote Control Session Authentication Initiate"; flow:established,to_server; dsize:<20; content:"|01 00 00 00
05 00 00 02 27 27 02 00 00 00|"; flowbits:set,BE.Radmin.Auth.Challenge; classtype:not-suspicious; reference:url,www.radmin.com; reference:url,doc.emergingthreats.net/2003481;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Radmin; sid:2003481; rev:4;)

#Matt Jonkman
#
alert tcp $HOME_NET 1024:65535 -> $EXTERNAL_NET any (msg:"ET POLICY Radmin Remote Control Session Authentication Response"; flowbits:isset,BE.Radmin.Auth.Challenge;
flow:established,from_server; dsize:<20; content:"|01 00 00 00 05 00 00 00 27 27 00 00 00 00|"; flowbits:noalert; classtype:not-suspicious; reference:url,www.radmin.com;
reference:url,doc.emergingthreats.net/2003482; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Radmin; sid:2003482; rev:4;)

#Matt jonkman
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET DELETED Real.com Game Arcade Install (User agent)"; flow: established,to_server; content:"User-Agent\:"; nocase;
pcre:"/User-Agent\:[^\n]+ARCADE_BUNDLE_DOWNLOADER/i"; classtype: policy-violation; reference:url,doc.emergingthreats.net/2003045; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Real.com_Game_Installs; sid:2003045; rev:4;)

#Matt jonkman
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET DELETED Real.com Game Arcade Install"; flow: established,to_server; content:"/gameconsole/bundlescripts/"; classtype:
policy-violation; reference:url,doc.emergingthreats.net/2003046; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Real.com_Game_Installs; sid:2003046; rev:3;)

#part of the state machine sigs in EXPLOIT/RealVNC
```

```
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET POLICY VNC Authentication Successful"; flowbits:isset,BSvnc.auth.agreed; flow:established; dsize:4; content:"|00 00 00 00|";
depth:4; flowbits:unset,BSvnc.auth.agreed; flowbits:unset,BSis.vnc.setup; classtype:not-suspicious; reference:url,www.cl.cam.ac.uk/Research/DTG/attarchive/vnc/rfbproto.pdf;
reference:url,doc.emergingthreats.net/bin/view/Main/2002922; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_RealVNC; sid:2002922; rev:5;)

#part of the state machine sigs in EXPLOIT/RealVNC
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET POLICY VNC Authentication Failure"; flowbits:isset,BSvnc.auth.agreed; flow:established; dsize:<50; content:"|00 00 00 01|";
depth:4; classtype:attempted-admin; reference:url,www.cl.cam.ac.uk/Research/DTG/attarchive/vnc/rfbproto.pdf; reference:url,doc.emergingthreats.net/bin/view/Main/2002920;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_RealVNC; sid:2002920; rev:5;)

#by marcus at unsober
#ref: 0d805713a6f969a3675d5776c7b2c4df
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY RemoteSpy.com Upload Detect"; flow:established,to_server; content:"POST "; depth:5; uricontent:"upload.php";
content:"|0d 0a|Host|3a| www.remotespy.com|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008406; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Remotespy.com; sid:2008406; rev:6;)

#Matt Jonkman, modified by jholguin (tb-security)
#This is a commercial product, but we see it very often used in malware. Send this email on install
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET POLICY SC-KeyLog Keylogger Installed - Sending Initial Email Report"; flow:established,to_server; content:"Installation of SC-KeyLog
on host "; nocase; content:"<p>You will receive a log report every "; nocase; classtype:trojan-activity; reference:url,www.soft-central.net/keylog.php;
reference:url,doc.emergingthreats.net/2002979; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_SC-KeyLog; sid:2002979; rev:4;)

#by jholguin (tb-security), re d5d466779b27cfc8e68c73145c5f3b36
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET POLICY SC-KeyLog Keylogger Installed - Sending Log Email Report"; flow:established,to_server; content:"SC-KeyLog log report";
nocase; content:"See attached file"; nocase; content:".log"; nocase; classtype:trojan-activity; reference:url,www.soft-central.net/keylog.php;
reference:url,doc.emergingthreats.net/2008348; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_SC-KeyLog; sid:2008348; rev:2;)

#by matt Jonkman
#TLS/SSL State Machine for 8081 and up
#if you have sessions that do NOT trip this please let me know.
#I only know this will work for sslv2, sslv3, and most TLS.
#Adding these sigs to prevent known ssl ports from being included. You may need to duplicate some of these
#to exclude known ssl traffic in your environment.
#You can also avoid falses by suppressing sigs 2003002-5 for the hosts that you expect unusual port SSL to/from
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 443 (msg:"ET POLICY Known SSL traffic on port 443 being excluded from SSL Alerts"; flow:established,to_server; flowbits:noalert;
flowbits:set,BS.SSL.Known.Port; classtype:not-suspicious; reference:url,doc.emergingthreats.net/2003026; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003026; rev:5;)

#by matt Jonkman
#TLS/SSL State Machine for 8081 and up
#if you have sessions that do NOT trip this please let me know.
#I only know this will work for sslv2, sslv3, and most TLS.
#Adding these sigs to prevent known ssl ports from being included. You may need to duplicate some of these
#to exclude known ssl traffic in your environment.
#You can also avoid falses by suppressing sigs 2003002-5 for the hosts that you expect unusual port SSL to/from
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 9001 (msg:"ET POLICY Known SSL traffic on port 9001 (aol) being excluded from SSL Alerts"; flow:established,to_server; flowbits:noalert;
flowbits:set,BS.SSL.Known.Port; classtype:not-suspicious; reference:url,doc.emergingthreats.net/2004598; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2004598; rev:4;)

#by matt Jonkman
#TLS/SSL State Machine for 8081 and up
#if you have sessions that do NOT trip this please let me know.
#I only know this will work for sslv2, sslv3, and most TLS.
#Adding these sigs to prevent known ssl ports from being included. You may need to duplicate some of these
#to exclude known ssl traffic in your environment.
#You can also avoid falses by suppressing sigs 2003002-5 for the hosts that you expect unusual port SSL to/from
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 8000 (msg:"ET POLICY Known SSL traffic on port 8000 being excluded from SSL Alerts"; flow:established,to_server; flowbits:noalert;
flowbits:set,BS.SSL.Known.Port; classtype:not-suspicious; reference:url,doc.emergingthreats.net/2003027; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003027; rev:5;)

#by matt Jonkman
#TLS/SSL State Machine for 8081 and up
#if you have sessions that do NOT trip this please let me know.
#I only know this will work for sslv2, sslv3, and most TLS.
#Adding these sigs to prevent known ssl ports from being included. You may need to duplicate some of these
#to exclude known ssl traffic in your environment.
#You can also avoid falses by suppressing sigs 2003002-5 for the hosts that you expect unusual port SSL to/from
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 8080 (msg:"ET POLICY Known SSL traffic on port 8080 being excluded from SSL Alerts"; flow:established,to_server; flowbits:noalert;
flowbits:set,BS.SSL.Known.Port; classtype:not-suspicious; reference:url,doc.emergingthreats.net/2003028; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003028; rev:5;)

#by matt Jonkman
#TLS/SSL State Machine for 8081 and up
#if you have sessions that do NOT trip this please let me know.
#I only know this will work for sslv2, sslv3, and most TLS.
#Adding these sigs to prevent known ssl ports from being included. You may need to duplicate some of these
#to exclude known ssl traffic in your environment.
#You can also avoid falses by suppressing sigs 2003002-5 for the hosts that you expect unusual port SSL to/from
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 8200 (msg:"ET POLICY Known SSL traffic on port 8200 being excluded from SSL Alerts"; flow:established,to_server; flowbits:noalert;
flowbits:set,BS.SSL.Known.Port; classtype:not-suspicious; reference:url,doc.emergingthreats.net/2003029; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003029; rev:5;)

#by matt Jonkman
#TLS/SSL State Machine for 8081 and up
#if you have sessions that do NOT trip this please let me know.
#I only know this will work for sslv2, sslv3, and most TLS.
#Adding these sigs to prevent known ssl ports from being included. You may need to duplicate some of these
#to exclude known ssl traffic in your environment.
#You can also avoid falses by suppressing sigs 2003002-5 for the hosts that you expect unusual port SSL to/from
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 8443 (msg:"ET POLICY Known SSL traffic on port 8443 being excluded from SSL Alerts"; flow:established,to_server; flowbits:noalert;
flowbits:set,BS.SSL.Known.Port; classtype:not-suspicious; reference:url,doc.emergingthreats.net/2003030; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003030; rev:5;)

#by matt Jonkman
#TLS/SSL State Machine for 8081 and up
#if you have sessions that do NOT trip this please let me know.
#I only know this will work for sslv2, sslv3, and most TLS.
#Adding these sigs to prevent known ssl ports from being included. You may need to duplicate some of these
#to exclude known ssl traffic in your environment.
#You can also avoid falses by suppressing sigs 2003002-5 for the hosts that you expect unusual port SSL to/from
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 5222 (msg:"ET POLICY Known SSL traffic on port 5222 (Jabber) being excluded from SSL Alerts"; flow:established,to_server; flowbits:noalert;
flowbits:set,BS.SSL.Known.Port; classtype:not-suspicious; reference:url,doc.emergingthreats.net/2003031; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003031; rev:5;)

#by matt Jonkman
#TLS/SSL State Machine for 8081 and up
```

```
#if you have sessions that do NOT trip this please let me know.
#I only know this will work for sslv2, sslv3, and most TLS.
#Adding these sigs to prevent known ssl ports from being included. You may need to duplicate some of these
#to exclude known ssl traffic in your environment.
#You can also avoid falses by suppressing sigs 2003002-5 for the hosts that you expect unusual port SSL to/from
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 5223 (msg:"ET POLICY Known SSL traffic on port 5223 (Jabber) being excluded from SSL Alerts"; flow:established,to_server; flowbits:noalert;
flowbits:set,BS.SSL.Known.Port; classtype:not-suspicious; reference:url,doc.emergingthreats.net/2003032; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003032; rev:5;)

#by matt Jonkman
#TLS/SSL State Machine for 8081 and up
#if you have sessions that do NOT trip this please let me know.
#I only know this will work for sslv2, sslv3, and most TLS.
#Adding these sigs to prevent known ssl ports from being included. You may need to duplicate some of these
#to exclude known ssl traffic in your environment.
#You can also avoid falses by suppressing sigs 2003002-5 for the hosts that you expect unusual port SSL to/from
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 2967 (msg:"ET POLICY Known SSL traffic on port 2967 (Symantec) being excluded from SSL Alerts"; flow:established,to_server; flowbits:noalert;
flowbits:set,BS.SSL.Known.Port; classtype:not-suspicious; reference:url,doc.emergingthreats.net/2003033; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003033; rev:4;)

#by matt Jonkman
#TLS/SSL State Machine for 8081 and up
#if you have sessions that do NOT trip this please let me know.
#I only know this will work for sslv2, sslv3, and most TLS.
#Adding these sigs to prevent known ssl ports from being included. You may need to duplicate some of these
#to exclude known ssl traffic in your environment.
#You can also avoid falses by suppressing sigs 2003002-5 for the hosts that you expect unusual port SSL to/from
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 3128 (msg:"ET POLICY Known SSL traffic on port 3128 (proxy) being excluded from SSL Alerts"; flow:established,to_server; flowbits:noalert;
flowbits:set,BS.SSL.Known.Port; classtype:not-suspicious; reference:url,doc.emergingthreats.net/2003035; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003035; rev:4;)

#by matt Jonkman
#TLS/SSL State Machine for 8081 and up
#if you have sessions that do NOT trip this please let me know.
#I only know this will work for sslv2, sslv3, and most TLS.
#Adding these sigs to prevent known ssl ports from being included. You may need to duplicate some of these
#to exclude known ssl traffic in your environment.
#You can also avoid falses by suppressing sigs 2003002-5 for the hosts that you expect unusual port SSL to/from
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 8080 (msg:"ET POLICY Known SSL traffic on port 8080 (proxy) being excluded from SSL Alerts"; flow:established,to_server; flowbits:noalert;
flowbits:set,BS.SSL.Known.Port; classtype:not-suspicious; reference:url,doc.emergingthreats.net/2003036; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003036; rev:4;)

#by matt Jonkman
#TLS/SSL State Machine for 8081 and up
#if you have sessions that do NOT trip this please let me know.
#I only know this will work for sslv2, sslv3, and most TLS.
#Adding these sigs to prevent known ssl ports from being included. You may need to duplicate some of these
#to exclude known ssl traffic in your environment.
#You can also avoid falses by suppressing sigs 2003002-5 for the hosts that you expect unusual port SSL to/from
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 8292 (msg:"ET POLICY Known SSL traffic on port 8292 (Bloomberg) being excluded from SSL Alerts"; flow:established,to_server; flowbits:noalert;
flowbits:set,BS.SSL.Known.Port; classtype:not-suspicious; reference:url,doc.emergingthreats.net/2003037; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003037; rev:4;)

#by matt Jonkman
#TLS/SSL State Machine for 8081 and up
#if you have sessions that do NOT trip this please let me know.
#I only know this will work for sslv2, sslv3, and most TLS.
#Adding these sigs to prevent known ssl ports from being included. You may need to duplicate some of these
#to exclude known ssl traffic in your environment.
#You can also avoid falses by suppressing sigs 2003002-5 for the hosts that you expect unusual port SSL to/from
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 8294 (msg:"ET POLICY Known SSL traffic on port 8294 (Bloomberg) being excluded from SSL Alerts"; flow:established,to_server; flowbits:noalert;
flowbits:set,BS.SSL.Known.Port; classtype:not-suspicious; reference:url,doc.emergingthreats.net/2003038; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003038; rev:4;)

#by matt Jonkman
#TLS/SSL State Machine for 8081 and up
#if you have sessions that do NOT trip this please let me know.
#I only know this will work for sslv2, sslv3, and most TLS.
#Adding these sigs to prevent known ssl ports from being included. You may need to duplicate some of these
#to exclude known ssl traffic in your environment.
#You can also avoid falses by suppressing sigs 2003002-5 for the hosts that you expect unusual port SSL to/from
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1521 (msg:"ET POLICY Known SSL traffic on port 1521 (Oracle) being excluded from SSL Alerts"; flow:established,to_server; flowbits:noalert;
flowbits:set,BS.SSL.Known.Port; classtype:not-suspicious; reference:url,doc.emergingthreats.net/2003934; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003934; rev:4;)

#by matt Jonkman
#TLS/SSL State Machine for 8081 and up
#if you have sessions that do NOT trip this please let me know.
#I only know this will work for sslv2, sslv3, and most TLS.
#Adding these sigs to prevent known ssl ports from being included. You may need to duplicate some of these
#to exclude known ssl traffic in your environment.
#You can also avoid falses by suppressing sigs 2003002-5 for the hosts that you expect unusual port SSL to/from
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 995 (msg:"ET POLICY Known SSL traffic on port 995 (imaps) being excluded from SSL Alerts"; flow:established,to_server; flowbits:noalert;
flowbits:set,BS.SSL.Known.Port; classtype:not-suspicious; reference:url,doc.emergingthreats.net/2008543; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2008543; rev:2;)

#Client Hello
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024:65535 (msg:"ET POLICY TLS/SSL Client Hello on Unusual Port TLS"; flowbits:isnotset,BS.SSL.Known.Port;
flowbits:isnotset,BS.SSL.Client.Hello; flow:established,to_server; content:"|16 03 01|"; depth:3; content:"|01|"; within:6; content:"|03 01|"; within:5;
flowbits:set,BS.SSL.Client.Hello; flowbits:noalert; classtype:unusual-client-port-connection; reference:url,doc.emergingthreats.net/2003002; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003002; rev:8;)

#Client Hello
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024:65535 (msg:"ET POLICY TLS/SSL Client Hello on Unusual Port SSLv3"; flowbits:isnotset,BS.SSL.Known.Port;
flowbits:isnotset,BS.SSL.Client.Hello; flow:established,to_server; content:"|16 03 00|"; depth:3; content:"|01|"; within:2; content:"|03 00|"; within:3;
flowbits:set,BS.SSL.Client.Hello; flowbits:noalert; classtype:unusual-client-port-connection; reference:url,doc.emergingthreats.net/2003003; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003003; rev:8;)

#Client Hello
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024:65535 (msg:"ET POLICY TLS/SSL Client Hello on Unusual Port Case 2"; flowbits:isnotset,BS.SSL.Known.Port;
flowbits:isnotset,BS.SSL.Client.Hello; flow:established; content:"|01 03 01|"; depth:5; offset:2; flowbits:set,BS.SSL.Client.Hello; flowbits:noalert; classtype:unusual-client-port-
connection; reference:url,doc.emergingthreats.net/2003004; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003004; rev:8;)

#Client Hello
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024:65535 (msg:"ET POLICY TLS/SSL Client Hello on Unusual Port SSLv3"; flowbits:isnotset,BS.SSL.Known.Port;
flowbits:isnotset,BS.SSL.Client.Hello; flow:established; content:"|01 03 00|"; depth:5; flowbits:set,BS.SSL.Client.Hello; flowbits:noalert; classtype:unusual-client-port-connection;
reference:url,doc.emergingthreats.net/2003005; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003005; rev:9;)
```

```
#Client Key exch and setup
#disabled the first two, unnecessary. Can remove these once we're sure they're not needed
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024:65535 (msg:"ET POLICY TLS/SSL Client Key Exchange on Unusual Port"; flowbits:isset,BS.SSL.Client.Hello; flow:established; content:"|16 03
01|"; content:"|10|"; within:6; classtype:unusual-client-port-connection; reference:url,doc.emergingthreats.net/2003006; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003006; rev:8;)

#Client Key exch and setup
#disabled the first two, unnecessary. Can remove these once we're sure they're not needed
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024:65535 (msg:"ET POLICY TLS/SSL Client Key Exchange on Unusual Port SSLv3"; flowbits:isset,BS.SSL.Client.Hello; flow:established;
content:"|16 03 00|"; content:"|10|"; within:6; flowbits:noalert; classtype:unusual-client-port-connection; reference:url,doc.emergingthreats.net/2003007;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003007; rev:8;)

#Client Key exch and setup
#disabled the first two, unnecessary. Can remove these once we're sure they're not needed
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024:65535 (msg:"ET POLICY TLS/SSL Client Cipher Set on Unusual Port"; flowbits:isset,BS.SSL.Client.Hello; flow:established; content:"|14 03 01
00 01 01|"; flowbits:set,BS.SSL.Client.Cipher; flowbits:noalert; classtype:unusual-client-port-connection; reference:url,doc.emergingthreats.net/2003008;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003008; rev:7;)

#Client Key exch and setup
#disabled the first two, unnecessary. Can remove these once we're sure they're not needed
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024:65535 (msg:"ET POLICY TLS/SSL Client Cipher Set on Unusual Port SSLv3"; flowbits:isset,BS.SSL.Client.Hello; flow:established; content:"|14
03 00 00 01 01|"; flowbits:set,BS.SSL.Client.Cipher; flowbits:noalert; classtype:unusual-client-port-connection; reference:url,doc.emergingthreats.net/2003009;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003009; rev:7;)

#Server Hello
#also setting a flowbit no longer used. Can be removed in a few weeks once we're sure it's unused
#
#alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET any (msg:"ET POLICY TLS/SSL Server Hello on Unusual Port"; flowbits:isset,BS.SSL.Client.Hello; flow:established; content:"|16 03 01|";
depth:3; content:"|02|"; within:6; content:"|03 01|"; within:6; flowbits:set,BS.SSL.Server.Hello; flowbits:noalert; classtype:unusual-client-port-connection;
reference:url,doc.emergingthreats.net/2003010; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003010; rev:7;)

#Server Hello
#also setting a flowbit no longer used. Can be removed in a few weeks once we're sure it's unused
#
#alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET any (msg:"ET POLICY TLS/SSL Server Hello on Unusual Port SSLv3"; flowbits:isset,BS.SSL.Client.Hello; flow:established; content:"|16 03
00|"; depth:3; content:"|02|"; within:6; content:"|03 00|"; within:6; flowbits:set,BS.SSL.Server.Hello; flowbits:noalert; classtype:unusual-client-port-connection;
reference:url,doc.emergingthreats.net/2003011; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003011; rev:7;)

#Server cert and key exchange
#Setting a flowbit no longer used. Can be removed in a few weeks
#
#alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET any (msg:"ET POLICY TLS/SSL Server Certificate Exchange on Unusual Port"; flowbits:isset,BS.SSL.Client.Hello; flow:established;
content:"|16 03 01|"; content:"|0b|"; within:6; classtype:unusual-client-port-connection; reference:url,doc.emergingthreats.net/2003012; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003012; rev:8;)

#Server cert and key exchange
#Setting a flowbit no longer used. Can be removed in a few weeks
#
#alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET any (msg:"ET POLICY TLS/SSL Server Certificate Exchange on Unusual Port SSLv3"; flowbits:isset,BS.SSL.Client.Hello; flow:established;
content:"|16 03 00|"; content:"|0b|"; within:6; classtype:unusual-client-port-connection; reference:url,doc.emergingthreats.net/2003013; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003013; rev:7;)

#Server cert and key exchange
#Setting a flowbit no longer used. Can be removed in a few weeks
#
#alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET any (msg:"ET POLICY TLS/SSL Server Key Exchange on Unusual Port"; flowbits:isset,BS.SSL.Client.Hello; flow:established; content:"|16 03
01|"; content:"|0c|"; within:6; flowbits:set,BS.SSL.Server.Key; flowbits:noalert; classtype:unusual-client-port-connection; reference:url,doc.emergingthreats.net/2003014;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003014; rev:7;)

#Server cert and key exchange
#Setting a flowbit no longer used. Can be removed in a few weeks
#
#alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET any (msg:"ET POLICY TLS/SSL Server Key Exchange on Unusual Port SSLv3"; flowbits:isset,BS.SSL.Client.Hello; flow:established;
content:"|16 03 00|"; content:"|0c|"; within:6; flowbits:set,BS.SSL.Server.Key; flowbits:noalert; classtype:unusual-client-port-connection;
reference:url,doc.emergingthreats.net/2003015; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003015; rev:6;)

#Server cert and key exchange
#Setting a flowbit no longer used. Can be removed in a few weeks
#
##alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET any (msg:"ET DELETED TLS/SSL Server Hello Done on Unusual Port"; flowbits:isset,BS.SSL.Server.Key; flow:established; content:"|16 03
01|"; content:"|0e|"; within:6; flowbits:set,BS.SSL.Server.Hello.Done; flowbits:noalert; classtype:unusual-client-port-connection; reference:url,doc.emergingthreats.net/2003016;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003016; rev:7;)

#Server cert and key exchange
#Setting a flowbit no longer used. Can be removed in a few weeks
#
##alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET any (msg:"ET DELETED TLS/SSL Server Hello Done on Unusual Port SSLv3"; flowbits:isset,BS.SSL.Server.Key; flow:established; content:"|16
03 00|"; content:"|0e|"; within:6; flowbits:set,BS.SSL.Server.Hello.Done; flowbits:noalert; classtype:unusual-client-port-connection; reference:url,doc.emergingthreats.net/2003017;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003017; rev:6;)

#Server Cipher set
#
#alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET any (msg:"ET POLICY TLS/SSL Server Cipher Set on Unusual Port"; flowbits:isset,BS.SSL.Client.Cipher; flow:established; content:"|14 03
01 00 01|"; flowbits:set,BS.SSL.Established; flowbits:noalert; classtype:unusual-client-port-connection; reference:url,doc.emergingthreats.net/2003018;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003018; rev:7;)

#Server Cipher set
#
#alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET any (msg:"ET POLICY TLS/SSL Server Cipher Set on Unusual Port SSLv3"; flowbits:isset,BS.SSL.Client.Cipher; flow:established;
content:"|14 03 00 00 01|"; flowbits:set,BS.SSL.Established; flowbits:noalert; classtype:unusual-client-port-connection; reference:url,doc.emergingthreats.net/2003019;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003019; rev:7;)

#Application data stream
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024:65535 (msg:"ET POLICY TLS/SSL Encrypted Application Data on Unusual Port"; flowbits:isset,BS.SSL.Established; flow:established,to_server;
content:"|17 03 01|"; depth:4; threshold:type limit, count 1, seconds 120, track by_src; classtype:unusual-client-port-connection; reference:url,doc.emergingthreats.net/2003020;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003020; rev:9;)

#Application data stream
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024:65535 (msg:"ET POLICY TLS/SSL Encrypted Application Data on Unusual Port SSLv3"; flowbits:isset,BS.SSL.Established;
flow:established,to_server; content:"|17 03 00|"; depth:4; threshold:type limit, count 1, seconds 120, track by_src; classtype:unusual-client-port-connection;
reference:url,doc.emergingthreats.net/2003021; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port; sid:2003021; rev:8;)

#Submitted by Patrick Harper. pcre by Matt Jonkman
#This rule is disabled by default. It should generally be run on the outside of your network, not internally. Enable it where useful.
#
#alert ip any any -> any any (msg:"ET POLICY SSN Detected in Clear Text (dashed)"; pcre:"/ ([0-6]\d\d|7[0-256]\d|73[0-3]|77[0-2])-\d{2}-\d{4} /"; classtype:policy-violation;
reference:url,doc.emergingthreats.net/2001328; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_SSN_in_the_Clear; sid:2001328; rev:13;)

#Submitted by Patrick Harper. pcre by Matt Jonkman
#This rule is disabled by default. It should generally be run on the outside of your network, not internally. Enable it where useful.
#
#alert ip any any -> any any (msg:"ET POLICY SSN Detected in Clear Text (spaced)"; pcre:"/ ([0-6]\d\d|7[0-256]\d|73[0-3]|77[0-2]) \d{2} \d{4} /"; classtype:policy-violation;
reference:url,doc.emergingthreats.net/2001384; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_SSN_in_the_Clear; sid:2001384; rev:13;)
```

```
#Submitted by Patrick Harper. pcre by Matt Jonkman
#This rule is disabled by default. It should generally be run on the outside of your network, not internally. Enable it where useful.
#
#alert ip any any -> any any (msg:"ET POLICY SSN Detected in Clear Text (SSN )"; content:"SSN "; nocase; pcre:"/SSN ([0-6]\d\d|7[0-256]\d|73[0-3]|77[0-2])\d{6} /i"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2007971; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_SSN_in_the_Clear; sid:2007971; rev:3;)

#Submitted by Patrick Harper. pcre by Matt Jonkman
#This rule is disabled by default. It should generally be run on the outside of your network, not internally. Enable it where useful.
#
#alert ip any any -> any any (msg:"ET POLICY SSN Detected in Clear Text (SSN# )"; content:"SSN# "; nocase; pcre:"/SSN# ([0-6]\d\d|7[0-256]\d|73[0-3]|77[0-2])\d{6} /i"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2007972; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_SSN_in_the_Clear; sid:2007972; rev:3;)

#by rich rumble
#PsExec for lan
#
alert tcp any any -> $HOME_NET [139,445] (msg:"ET POLICY PsExec service created"; flow:to_server,established; content:"|5c 00 50 00 53 00 45 00 58 00 45 00 53 00 56 00 43 00 2e 00 45 00 58 00 45|"; classtype:suspicious-filename-detect; reference:url,xinn.org/Snort-psexec.html; reference:url,doc.emergingthreats.net/2010781; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_SecTools; sid:2010781; rev:2;)

#RctrlX
#
alert tcp any any -> $HOME_NET [139,445] (msg:"ET POLICY RemoteControlX rctrlx service created"; flow:to_server,established; content:"|5c 00 72 00 63 00 74 00 72 00 6c 00 78 00 73 00 72 00 76 00 2e 00 65 00 78 00 65|"; classtype:suspicious-filename-detect; reference:url,xinn.org/Snort-rctrlx.html; reference:url,doc.emergingthreats.net/2010782; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_SecTools; sid:2010782; rev:2;)

#By Chich Thierry
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Skype VOIP Checking Version (Startup)"; flow: to_server,established; uricontent:"/ui/"; nocase; uricontent:"/getlatestversion?ver="; nocase; classtype: policy-violation; reference:url,www1.cs.columbia.edu/~library/TR-repository/reports/reports-2004/cucs-039-04.pdf; reference:url,doc.emergingthreats.net/2001595; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Skype; sid:2001595; rev:9;)

#By Chich Thierry
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Skype VOIP Reporting Install"; flow: to_server,established; uricontent:"/ui/"; nocase; uricontent:"/installed"; nocase; classtype: policy-violation; reference:url,www1.cs.columbia.edu/~library/TR-repository/reports/reports-2004/cucs-039-04.pdf; reference:url,doc.emergingthreats.net/2001596; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Skype; sid:2001596; rev:9;)

#By Robert Grabowsky
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Skype User-Agent detected"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| "; content:"Skype"; distance:0; within:100; pcre:"/User-Agent\:[^(\n|\r)]+Skype/i"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002157; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Skype; sid:2002157; rev:6;)

#by Reg Quinton
#
#alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET 33033 (msg:"ET POLICY Skype Bootstrap Node (udp)"; classtype:policy-violation; reference:url,www1.cs.columbia.edu/~library/TR-repository/reports/reports-2004/cucs-039-04.pdf; reference:url,doc.emergingthreats.net/2003022; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Skype; sid:2003022; rev:4;)

#Idea by Martin Holste, sigs by Matt Jonkman
#The idea here is that most legitimate exe downloads are more than 1meg, most malicious are far less than 1 meg.
#This is evadable of course, and doesn't work with non-compliant web servers, but this will catch many...
#First we qualify this as a packet containing the header return info from the get request and is likely binary content
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY Likely Binary in HTTP by Type Flowbit"; flow:established,from_server; flowbits:isnotset,ET.http.binary; content:"HTTP/1"; depth:6; content:"|0d 0a|Content-Type|3a| application/"; nocase; flowbits:noalert; flowbits:set,ET.http.binary; classtype:not-suspicious; reference:url,doc.emergingthreats.net/2007670; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Small_Binary_Downloads; sid:2007670; rev:5;)

#next we check that the content-length is less than 7 digits, thus under 1,000,000 bytes.
#note: I re-check for the leading HTTP/1 to make sure we're still in the header packet, not in the rest of the binary stream
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY Binary Download Smaller than 1 MB Likely Hostile"; flow:established,from_server; flowbits:isset,ET.http.binary; content:"HTTP/1"; depth:6; content:"MZ"; isdataat: 76,relative; content:"This program "; distance: 0; pcre:"/\x0d\x0aContent-Length\: \d{0,6}\x0d\x0a/"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2007671; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Small_Binary_Downloads; sid:2007671; rev:9;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Smilebox Spyware Download"; flow:established,to_server; content:"GET "; depth:4; uricontent:"/download/smilebox/SmileboxInstaller.exe"; nocase; classtype:policy-violation; reference:url,www.smilebox.com/info/privacy.html; reference:url,doc.emergingthreats.net/2009998; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Smilebox; sid:2009998; rev:7;)

#moves to 7090 in samples
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 3000:8000 (msg:"ET P2P Unknown Trojan P2P Download Request"; flow:established,to_server; dsize:<100; content:"|00 00 00 00|"; depth:5; offset:1; content:"|00 01 01 00 00 08 00 00|"; distance:1; within:9; threshold: type both, count 5, seconds 120, track by_src; classtype:trojan-activity; reference:url,www.chinatechnews.com/2008/07/21/7014-baofengcom-shifts-to-internet-video-sector/; reference:url,doc.emergingthreats.net/2008771; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Storm3_Media; sid:2008771; rev:5;)

#moves to 7090 in samples
#
alert tcp $EXTERNAL_NET 3000:8000 -> $HOME_NET any (msg:"ET P2P Unknown Trojan P2P Data Download"; flow:established,from_server; dsize:>1000; content:"|00 00 00|"; depth:5; offset:2; content:"|00 01 01 00 00 05 00 00|"; distance:1; within:9; threshold: type both, count 5, seconds 120, track by_dst; classtype:trojan-activity; reference:url,www.chinatechnews.com/2008/07/21/7014-baofengcom-shifts-to-internet-video-sector/; reference:url,doc.emergingthreats.net/2008770; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Storm3_Media; sid:2008770; rev:5;)

#moved to 5622 in samples
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 3000:8000 (msg:"ET P2P Unknown Trojan P2P Request"; flow:established,to_server; dsize:<60; content:"|00 00 00 00|"; depth:5; offset:1; content:"|00 01 01 00 00 03 00 00|"; distance:1; within:9; threshold: type both, count 5, seconds 120, track by_src; classtype:trojan-activity; reference:url,www.chinatechnews.com/2008/07/21/7014-baofengcom-shifts-to-internet-video-sector/; reference:url,doc.emergingthreats.net/2008772; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Storm3_Media; sid:2008772; rev:5;)

#by Will Metcalf
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY CBS Streaming Video"; flow:established,to_server; content:"GET "; depth:4; content:"Host|3a|"; nocase; content:"cbs.com"; nocase; within:40; uricontent:"/innertube/player.php?"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2007763; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Streaming_News; sid:2007763; rev:4;)

#by Will Metcalf
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY NBC Streaming Video"; flow:established,to_server; content:"GET "; depth:4; content:"Host|3a 20|video.nbcuni.com"; nocase; pcre:"/(\.smil)$/Ui"; classtype: policy-violation; reference:url,doc.emergingthreats.net/2007764; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Streaming_News; sid:2007764; rev:4;)

#by Nathaniel Richmond
#
alert udp $HOME_NET any -> $EXTERNAL_NET 69 (msg:"ET TFTP Outbound TFTP Read Request"; content:"|00 01|"; depth:2; classtype:policy-violation; reference:url,doc.emergingthreats.net/2008120; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_TFTP; sid:2008120; rev:3;)

#by Nathaniel Richmond
#
alert udp $HOME_NET any -> $EXTERNAL_NET 69 (msg:"ET TFTP Outbound TFTP Write Request"; content:"|00 02|"; depth:2; classtype:policy-violation; reference:url,doc.emergingthreats.net/2008116; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_TFTP; sid:2008116; rev:3;)

#by Nathaniel Richmond
#
```

```
alert udp $HOME_NET any -> $EXTERNAL_NET 69 (msg:"ET TFTP Outbound TFTP Data Transfer"; content:"|00 03|"; depth:2; classtype:policy-violation;
reference:url,doc.emergingthreats.net/2008117; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_TFTP; sid:2008117; rev:3;)

#by Nathaniel Richmond
#
alert udp $HOME_NET any -> $EXTERNAL_NET 69 (msg:"ET TFTP Outbound TFTP ACK"; content:"|00 04|"; depth:2; classtype:policy-violation; reference:url,doc.emergingthreats.net/2008118;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_TFTP; sid:2008118; rev:3;)

#by Nathaniel Richmond
#
alert udp $HOME_NET any -> $EXTERNAL_NET 69 (msg:"ET TFTP Outbound TFTP Error Message"; content:"|00 05|"; depth:2; classtype:policy-violation;
reference:url,doc.emergingthreats.net/2008119; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_TFTP; sid:2008119; rev:3;)

#Matt Jonkman, major updates by Chris Byrd
#Experimenting with this idea. When a bot comes up live and starts spamming, it
#does a massive number of dns queries. This may be an extra way to identify infections
#
#alert udp ![$DNS_SERVERS,$SMTP_SERVERS] any -> $DNS_SERVERS 53 (msg:"ET POLICY Possible Spambot Host DNS MX Query High Count"; content: "|01 00|"; offset: 2; depth: 4; content: "|00 0f
00 01|"; distance: 8; threshold:type both, count 30, seconds 10, track by_src; classtype:bad-unknown; reference:url,doc.emergingthreats.net/2003330;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_TROJAN_DNS_Lookups; sid:2003330; rev:6;)

#2008-11-19 added by Frank Knobbe
#The following two sigs were created based on the findings of SIDs 2008779
#and 2008780. That particular keep-alive matched the TeamViewer application.
#The 'unknown trojan' rules are still present in case something else uses
#this pattern, but will likely be removed shortly. The trojan sigs won't
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 5938 (msg:"ET POLICY TeamViewier Keep-alive outbound"; flow:established,to_server; dsize:5; content:"|17 24 1B 00 00|";
flowbits:set,ET.teamviewerkeepaliveout; flowbits:noalert; classtype:misc-activity; reference:url,www.teamviewer.com; reference:url,en.wikipedia.org/wiki/TeamViewer;
reference:url,doc.emergingthreats.net/2008794; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_TeamViewer; sid:2008794; rev:3;)

#2008-11-19 added by Frank Knobbe
#The following two sigs were created based on the findings of SIDs 2008779
#and 2008780. That particular keep-alive matched the TeamViewer application.
#The 'unknown trojan' rules are still present in case something else uses
#this pattern, but will likely be removed shortly. The trojan sigs won't
#
alert tcp $EXTERNAL_NET 5938 -> $HOME_NET any (msg:"ET POLICY TeamViewier Keep-alive inbound"; flow:established,to_client; dsize:5; content:"|17 24 1B 00 00|";
flowbits:isset,ET.teamviewerkeepaliveout; classtype:misc-activity; reference:url,www.teamviewer.com; reference:url,en.wikipedia.org/wiki/TeamViewer;
reference:url,doc.emergingthreats.net/2008795; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_TeamViewer; sid:2008795; rev:3;)

#by jim
#These will false positive a LOT, but use them if you need them. They should be useful.
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY Possible Reference to Terrorist Literature (Moderate Islam...)"; flow: to_client,established; content:"Moderate
Islam is a Prostration to the West"; nocase; threshold: type threshold, track by_dst,count 5, seconds 360; classtype: policy-violation; reference:url,doc.emergingthreats.net/2010570;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Terririst_Literature; sid:2010570; rev:2;)

#by jim
#These will false positive a LOT, but use them if you need them. They should be useful.
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY Possible Reference to Terrorist Literature (Jihad, Martyrdom...)"; flow: to_client,established; content:"Jihad,
Martyrdom and the Killing of Innocents"; nocase; threshold: type threshold, track by_dst,count 5, seconds 360; classtype: policy-violation;
reference:url,doc.emergingthreats.net/2010571; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Terririst_Literature; sid:2010571; rev:2;)

#by jim
#These will false positive a LOT, but use them if you need them. They should be useful.
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY Possible Reference to Terrorist Literature (The Call to Global...)"; flow: to_client,established; content:"The Call
to Global Islamic Resistance"; nocase; threshold: type threshold, track by_dst,count 5, seconds 360; classtype: policy-violation; reference:url,doc.emergingthreats.net/2010572;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Terririst_Literature; sid:2010572; rev:2;)

#by jim
#These will false positive a LOT, but use them if you need them. They should be useful.
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY Possible Reference to Terrorist Literature (Knights under the...)"; flow: to_client,established; content:"Knights
under the Prophet's Banner"; nocase; threshold: type threshold, track by_dst,count 5, seconds 360; classtype: policy-violation; reference:url,doc.emergingthreats.net/2010573;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Terririst_Literature; sid:2010573; rev:3;)

#by jim
#These will false positive a LOT, but use them if you need them. They should be useful.
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY Possible Reference to Terrorist Literature (Jihad against...)"; flow: to_client,established; content:"Jihad Against
Jews and Crusaders World Islamic Front Statement"; nocase; threshold: type threshold, track by_dst,count 5, seconds 360; classtype: policy-violation;
reference:url,doc.emergingthreats.net/2010574; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Terririst_Literature; sid:2010574; rev:2;)

#by jim
#These will false positive a LOT, but use them if you need them. They should be useful.
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY Possible Reference to Terrorist Literature (Declaration of War against the Americans...)"; flow:
to_client,established; content:"Declaration of War against the Americans Occupying the Land of the Two Holy Places"; nocase; threshold: type threshold, track by_dst,count 5, seconds
360; classtype: policy-violation; reference:url,doc.emergingthreats.net/2010575; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Terririst_Literature;
sid:2010575; rev:2;)

#by jim
#These will false positive a LOT, but use them if you need them. They should be useful.
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY Possible Reference to Terrorist Literature (Join the Caravan of Martyrs...)"; flow: to_client,established;
content:"Join the Caravan of Martyrs"; nocase; threshold: type threshold, track by_dst,count 5, seconds 360; classtype: policy-violation; reference:url,doc.emergingthreats.net/2010576;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Terririst_Literature; sid:2010576; rev:2;)

#by jim
#These will false positive a LOT, but use them if you need them. They should be useful.
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY Possible Reference to Terrorist Literature (Sharia and Democracy...)"; flow: to_client,established; content:"Sharia
and Democracy"; nocase; threshold: type threshold, track by_dst,count 5, seconds 360; classtype: policy-violation; reference:url,doc.emergingthreats.net/2010577;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Terririst_Literature; sid:2010577; rev:2;)

#by jim
#These will false positive a LOT, but use them if you need them. They should be useful.
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY Possible Reference to Al Qaeda Propaganda Theme (fardh ain)"; flow: to_client,established; content:"fardh ain";
nocase; threshold: type threshold, track by_dst,count 5, seconds 360; classtype: policy-violation; reference:url,doc.emergingthreats.net/2010578;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Terririst_Literature; sid:2010578; rev:2;)

#by jim
#These will false positive a LOT, but use them if you need them. They should be useful.
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY Possible Reference to Al Qaeda Propaganda Theme/Group (Takfir)"; flow: to_client,established; content:"Takfir";
nocase; threshold: type threshold, track by_dst,count 5, seconds 360; classtype: policy-violation; reference:url,doc.emergingthreats.net/2010579;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Terririst_Literature; sid:2010579; rev:2;)

#by jim
#These will false positive a LOT, but use them if you need them. They should be useful.
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY Possible Reference to Al Qaeda Propaganda Theme (Al-Wala' Wal Bara)"; flow: to_client,established; content:"Al-
Wala' Wal Bara"; nocase; threshold: type threshold, track by_dst,count 5, seconds 360; classtype: policy-violation; reference:url,doc.emergingthreats.net/2010580;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Terririst_Literature; sid:2010580; rev:4;)

#by jim
```

```
#These will false positive a LOT, but use them if you need them. They should be useful.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET POLICY Possible Reference to Terrorist Literature (Moderate Islam...) SMTP"; flow: to_client,established; content:"Moderate Islam
is a Prostration to the West"; nocase; threshold: type threshold, track by_dst,count 5, seconds 360; classtype: policy-violation; reference:url,doc.emergingthreats.net/2010581;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Terririst_Literature; sid:2010581; rev:2;)

#by jim
#These will false positive a LOT, but use them if you need them. They should be useful.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET POLICY Possible Reference to Terrorist Literature (Jihad, Martyrdom...) SMTP"; flow: to_client,established; content:"Jihad,
Martyrdom and the Killing of Innocents"; nocase; threshold: type threshold, track by_dst,count 5, seconds 360; classtype: policy-violation;
reference:url,doc.emergingthreats.net/2010582; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Terririst_Literature; sid:2010582; rev:2;)

#by jim
#These will false positive a LOT, but use them if you need them. They should be useful.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET POLICY Possible Reference to Terrorist Literature (The Call to Global...) SMTP"; flow: to_client,established; content:"The Call to
Global Islamic Resistance"; nocase; threshold: type threshold, track by_dst,count 5, seconds 360; classtype: policy-violation; reference:url,doc.emergingthreats.net/2010583;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Terririst_Literature; sid:2010583; rev:2;)

#by jim
#These will false positive a LOT, but use them if you need them. They should be useful.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET POLICY Possible Reference to Terrorist Literature (Knights under the...) SMTP"; flow: to_client,established; content:"Knights under
the Prophet's Banner"; nocase; threshold: type threshold, track by_dst,count 5, seconds 360; classtype: policy-violation; reference:url,doc.emergingthreats.net/2010584;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Terririst_Literature; sid:2010584; rev:3;)

#by jim
#These will false positive a LOT, but use them if you need them. They should be useful.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET POLICY Possible Reference to Terrorist Literature (Jihad against...) SMTP"; flow: to_client,established; content:"Jihad Against
Jews and Crusaders World Islamic Front Statement"; nocase; threshold: type threshold, track by_dst,count 5, seconds 360; classtype: policy-violation;
reference:url,doc.emergingthreats.net/2010585; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Terririst_Literature; sid:2010585; rev:2;)

#by jim
#These will false positive a LOT, but use them if you need them. They should be useful.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET POLICY Possible Reference to Terrorist Literature (Declaration of War against the Americans...) SMTP"; flow: to_client,established;
content:"Declaration of War against the Americans Occupying the Land of the Two Holy Places"; nocase; threshold: type threshold, track by_dst,count 5, seconds 360; classtype: policy-
violation; reference:url,doc.emergingthreats.net/2010586; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Terririst_Literature; sid:2010586; rev:2;)

#by jim
#These will false positive a LOT, but use them if you need them. They should be useful.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET POLICY Possible Reference to Terrorist Literature (Join the Caravan of Martyrs...) SMTP"; flow: to_client,established;
content:"Join the Caravan of Martyrs"; nocase; threshold: type threshold, track by_dst,count 5, seconds 360; classtype: policy-violation; reference:url,doc.emergingthreats.net/2010587;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Terririst_Literature; sid:2010587; rev:2;)

#by jim
#These will false positive a LOT, but use them if you need them. They should be useful.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET POLICY Possible Reference to Terrorist Literature (Sharia and Democracy...) SMTP"; flow: to_client,established; content:"Sharia and
Democracy"; nocase; threshold: type threshold, track by_dst,count 5, seconds 360; classtype: policy-violation; reference:url,doc.emergingthreats.net/2010588;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Terririst_Literature; sid:2010588; rev:2;)

#by jim
#These will false positive a LOT, but use them if you need them. They should be useful.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET POLICY Possible Reference to Al Qaeda Propaganda Theme (fardh ain) SMTP"; flow: to_client,established; content:"fardh ain"; nocase;
threshold: type threshold, track by_dst,count 5, seconds 360; classtype: policy-violation; reference:url,doc.emergingthreats.net/2010589; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Terririst_Literature; sid:2010589; rev:2;)

#by jim
#These will false positive a LOT, but use them if you need them. They should be useful.
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY Possible Reference to Al Qaeda Propaganda Theme/Group (Takfir) SMTP"; flow: to_client,established;
content:"Takfir"; nocase; threshold: type threshold, track by_dst,count 5, seconds 360; classtype: policy-violation; reference:url,doc.emergingthreats.net/2010590;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Terririst_Literature; sid:2010590; rev:2;)

#by jim
#These will false positive a LOT, but use them if you need them. They should be useful.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET POLICY Possible Reference to Al Qaeda Propaganda Theme (Al-Wala' Wal Bara) SMTP"; flow: to_client,established; content:"Al-Wala'
Wal Bara"; nocase; threshold: type threshold, track by_dst,count 5, seconds 360; classtype: policy-violation; reference:url,doc.emergingthreats.net/2010591;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Terririst_Literature; sid:2010591; rev:4;)

#Submitted by an anonymous researcher
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET POLICY TOR 1.0 Server Key Retrieval"; flow:established,to_server; content:"GET /tor/server/"; depth:16; threshold:type limit,
track by_src, count 1, seconds 30; classtype:policy-violation; reference:url,tor.eff.org; reference:url,doc.emergingthreats.net/2002950; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Tor; sid:2002950; rev:6;)

#Submitted by an anonymous researcher
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET POLICY TOR 1.0 Status Update"; flow:established,to_server; content:"GET /tor/status/"; depth:16; threshold:type limit, track
by_src, count 1, seconds 60; classtype:policy-violation; reference:url,tor.eff.org; reference:url,doc.emergingthreats.net/2002951; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Tor; sid:2002951; rev:5;)

#this sig is good as long as the client isn't recompiled to use an identifier other than TOR..
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 1024: (msg:"ET POLICY TOR 1.0 Inbound Circuit Traffic"; flow:established; content:"TOR"; content:"<identity>"; rawbytes; distance:10; within:35;
threshold:type limit, track by_src, count 1, seconds 120; classtype:policy-violation; reference:url,tor.eff.org; reference:url,doc.emergingthreats.net/2002952;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Tor; sid:2002952; rev:5;)

#this sig is good as long as the client isn't recompiled to use an identifier other than TOR..
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET POLICY TOR 1.0 Outbound Circuit Traffic"; flow:established; content:"TOR"; content:"<identity>"; rawbytes; distance:10;
within:35; threshold:type limit, track by_src, count 1, seconds 120; classtype:policy-violation; reference:url,tor.eff.org; reference:url,doc.emergingthreats.net/2002953;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Tor; sid:2002953; rev:5;)

#by Nathaniel Richmond
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Tor Get Server Request"; flow:established,to_server; uricontent:"/tor/server/"; nocase; classtype: policy-violation;
reference:url,tor.eff.org; reference:url,doc.emergingthreats.net/2008113; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Tor; sid:2008113; rev:4;)

#by Nathaniel Richmond
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Tor Get Status Request"; flow:established,to_server; uricontent:"/tor/status/"; nocase; classtype: policy-violation;
reference:url,tor.eff.org; reference:url,doc.emergingthreats.net/2008115; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Tor; sid:2008115; rev:2;)

#by Mike Cox
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Twitter Status Update"; flow:to_server,established; content:"POST "; depth:5; uricontent:"/status/update";
content:"twitter.com"; nocase; content:"authenticity_token="; nocase; content:"status="; nocase; classtype:policy-violation; reference:url,twitter.com;
reference:url,doc.emergingthreats.net/2010797; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Twitter; sid:2010797; rev:2;)

#from Rodrigo Montoro(Sp0oKeR). This isn't a hostile app, but may be interesting to know who's using it
#Rule by SERPRO-Recife Security Team
```

```
#
#alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"ET POLICY Possible External Ultrasurf Anonymizer DNS Query"; content:"|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00|"; classtype:policy-violation; threshold:type limit, track by_src,count 1, seconds 60; reference:url,doc.emergingthreats.net/2008533; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Ultrasurf; sid:2008533; rev:3;)

#Submitted by Erik Vincent
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Proxy Connection detected"; flow:established; content:"Proxy-Connection"; classtype: attempted-user; reference:url,doc.emergingthreats.net/2001449; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Unauthorized_Proxying; sid:2001449; rev:6;)

#You MUST add the SMTP_SERVERS var to your snort.conf!!!!
#
alert tcp !$SMTP_SERVERS any -> !$HOME_NET 25 (msg:"ET POLICY Outbound Multiple Non-SMTP Server Emails"; flow:established; content:"mail from|3a|"; nocase; threshold: type threshold, track by_src, count 10, seconds 120; classtype: misc-activity; reference:url,doc.emergingthreats.net/2000328; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Unauthorized_SMTP; sid:2000328; rev:12;)

#You MUST add the SMTP_SERVERS var to your snort.conf!!!!
#
alert tcp !$HOME_NET any -> $HOME_NET 25 (msg:"ET POLICY Inbound Frequent Emails - Possible Spambot Inbound"; flow:established; content:"mail from|3a|"; nocase; threshold: type threshold, track by_src, count 10, seconds 60; classtype: misc-activity; reference:url,doc.emergingthreats.net/2002087; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Unauthorized_SMTP; sid:2002087; rev:10;)

#Seeing some bots use 587 as an outbound mail stream. Use this if you do NOT use 587 locally
#
#alert tcp !$SMTP_SERVERS any -> !$HOME_NET 587 (msg:"ET POLICY Outbound SMTP on port 587"; flow:established; content:"mail from|3a|"; nocase; threshold: type threshold, track by_src, count 1, seconds 60; classtype: misc-activity; reference:url,doc.emergingthreats.net/2003864; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Unauthorized_SMTP; sid:2003864; rev:4;)

#by Matt Jonkman, sandnetted binary
#App on port 20000 for this casino stuff. Not malicious, but likely not allowed in most environments
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 20000 (msg:"ET POLICY Gold VIP Club Casino Client in Use"; flow:established,to_server; dsize:25; content:"Gold VIP Club Casino"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2007746; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_VIP_Gold_Casino; sid:2007746; rev:5;)

#Submitted by Jason Alvarado
#
#alert tcp $HOME_NET any -> [208.8.81.0/24,64.68.96.0/19] 443 (msg:"ET POLICY MyWebEx Server Traffic"; flow: to_server,established; dsize: <50; content:"|17|"; offset: 0; depth: 1; threshold: type limit,track by_src, count 1, seconds 360; classtype: policy-violation; reference:url,www.mywebexpc.com; reference:url,doc.emergingthreats.net/2001712; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_WebEx_Traffic; sid:2001712; rev:6;)

#Submitted by Jason Alvarado
#
#alert tcp $HOME_NET any -> [208.8.81.0/24,64.68.96.0/19] $HTTP_PORTS (msg:"ET POLICY MyWebEx Installation"; flow: to_server,established; content:"/pc/r.php?AT=RS"; nocase; threshold: type limit, track by_src, count 1, seconds 30; classtype: policy-violation; reference:url,www.mywebexpc.com; reference:url,doc.emergingthreats.net/2001713; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_WebEx_Traffic; sid:2001713; rev:6;)

#Submitted by Jason Alvarado
#
#alert tcp [208.8.81.0/24,64.68.96.0/19] 443 -> $HOME_NET any (msg:"ET POLICY MyWebEx Incoming Connection"; flow: to_client,established; content:"|16 03|"; offset: 0; depth: 2; content:"Comodo"; nocase; depth: 240; content:"accessanywhere.com"; nocase; offset: 592; depth: 48; classtype: policy-violation; reference:url,www.mywebexpc.com; reference:url,doc.emergingthreats.net/2001714; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_WebEx_Traffic; sid:2001714; rev:6;)

#By Robert Grabowsky
#Updated to have a more unique match than User-Agent.
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY WebshotsNetClient"; flow: to_server,established; content:"WebshotsNetClient"; nocase; within:100; classtype:policy-violation; reference:url,www.webshots.com; reference:url,doc.emergingthreats.net/2002407; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_WebShots; sid:2002407; rev:7;)

#by Jacob Kitchel of infotex
#These are of particular use in detecting recon for phishing, etc.
#
#alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET POLICY Wget User Agent"; flow:established,to_server; content:"|0d 0a|User-Agent|3A| "; nocase; content:"Wget"; nocase; within:50; classtype: attempted-recon; reference:url,www.gnu.org/software/wget; reference:url,doc.emergingthreats.net/2002822; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Web_Crawling; sid:2002822; rev:7;)

#by Jacob Kitchel of infotex
#These are of particular use in detecting recon for phishing, etc.
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY POSSIBLE Web Crawl using Wget"; flow:established,to_server; content:"|0d 0a|User-Agent|3A| "; nocase; content:"Wget"; nocase; within:50; threshold: type both, track by_src, count 10, seconds 60; classtype: attempted-recon; reference:url,www.gnu.org/software/wget/; reference:url,doc.emergingthreats.net/2002823; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Web_Crawling; sid:2002823; rev:5;)

#by Jacob Kitchel of infotex
#These are of particular use in detecting recon for phishing, etc.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY CURL User Agent"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| "; nocase; content:"curl"; nocase; distance:0; within:100; classtype: attempted-recon; reference:url,curl.haxx.se; reference:url,doc.emergingthreats.net/2002824; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Web_Crawling; sid:2002824; rev:7;)

#by Jacob Kitchel of infotex
#These are of particular use in detecting recon for phishing, etc.
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY POSSIBLE Web Crawl using Curl"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| "; nocase; content:"curl"; nocase; distance:0; within:100; threshold: type both, track by_src, count 10, seconds 60; classtype:attempted-recon; reference:url,curl.haxx.se; reference:url,doc.emergingthreats.net/2002825; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Web_Crawling; sid:2002825; rev:7;)

#by Jacob Kitchel of infotex
#These are of particular use in detecting recon for phishing, etc.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY fetch User Agent"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| "; nocase; content:"fetch"; nocase; distance:0; within:50; classtype: attempted-recon; reference:url,gobsd.com/code/freebsd/lib/libfetch; reference:url,doc.emergingthreats.net/2002826; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Web_Crawling; sid:2002826; rev:7;)

#by Jacob Kitchel of infotex
#These are of particular use in detecting recon for phishing, etc.
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY POSSIBLE Crawl using Fetch"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| "; nocase; content:"fetch"; nocase; distance:0; within:50; threshold: type both, track by_src, count 10, seconds 60; classtype: attempted-recon; reference:url,gobsd.com/code/freebsd/lib/libfetch; reference:url,doc.emergingthreats.net/2002827; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Web_Crawling; sid:2002827; rev:6;)

#by Jacob Kitchel of infotex
#These are of particular use in detecting recon for phishing, etc.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY libwww-perl User Agent"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| "; nocase; content:"libwww-perl/"; nocase; distance:0; within:50; classtype: attempted-recon; reference:url,www.linpro.no/lwp/; reference:url,doc.emergingthreats.net/2002934; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Web_Crawling; sid:2002934; rev:7;)

#by Jacob Kitchel of infotex
#These are of particular use in detecting recon for phishing, etc.
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY Possible Web Crawl - libwww-perl User Agent"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| "; nocase; content:"libwww-perl/"; nocase; distance:0; within:50; threshold: type both, track by_src, count 10, seconds 60; classtype: attempted-recon; reference:url,www.linpro.no/lwp/; reference:url,doc.emergingthreats.net/2002935; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Web_Crawling; sid:2002935; rev:6;)

#These aren't security issues necessarily, but you may be interested in seeing how often these crawlers hit you
#
```

```
#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY Googlebot User Agent"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| "; content:"googlebot";
within:50; nocase; classtype:not-suspicious; reference:url,www.google.com/webmasters/bot.html; reference:url,doc.emergingthreats.net/2002828; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Web_Crawling; sid:2002828; rev:7;)

#These aren't security issues necessarily, but you may be interested in seeing how often these crawlers hit you
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY Googlebot Crawl"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| "; content:"googlebot"; within:50;
nocase; threshold: type both, track by_src, count 10, seconds 60; classtype: attempted-recon; reference:url,www.google.com/webmasters/bot.html;
reference:url,doc.emergingthreats.net/2002829; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Web_Crawling; sid:2002829; rev:5;)

#These aren't security issues necessarily, but you may be interested in seeing how often these crawlers hit you
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY Msnbot User Agent"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| "; content:"msnbot"; nocase;
within:30; classtype:not-suspicious; reference:url,search.msn.com/msnbot.htm; reference:url,doc.emergingthreats.net/2002830; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Web_Crawling; sid:2002830; rev:6;)

#These aren't security issues necessarily, but you may be interested in seeing how often these crawlers hit you
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY Msnbot Crawl"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| "; content:"msnbot"; nocase; within:30;
threshold: type both, track by_src, count 10, seconds 60; classtype: attempted-recon; reference:url,search.msn.com/msnbot.htm; reference:url,doc.emergingthreats.net/2002831;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Web_Crawling; sid:2002831; rev:6;)

#These aren't security issues necessarily, but you may be interested in seeing how often these crawlers hit you
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY Yahoo Crawler User Agent"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| "; content:"Yahoo-MMCrawler";
nocase; within:50; classtype:not-suspicious; reference:url,mms-mmcrawler-support@yahoo-inc.com; reference:url,doc.emergingthreats.net/2002832; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Web_Crawling; sid:2002832; rev:7;)

#These aren't security issues necessarily, but you may be interested in seeing how often these crawlers hit you
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY Yahoo Crawler Crawl"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| "; content:"Yahoo-MMCrawler";
within:50; nocase; threshold: type both, track by_src, count 10, seconds 60; classtype: attempted-recon; reference:url,mms-mmcrawler-support@yahoo-inc.com;
reference:url,doc.emergingthreats.net/2002833; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Web_Crawling; sid:2002833; rev:5;)

#by Jacob Kitchel
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY python.urllib User Agent"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| "; nocase;
content:"python.urllib/"; nocase; within:50; classtype: attempted-recon; reference:url,docs.python.org/lib/module-urllib.html; reference:url,doc.emergingthreats.net/2002944;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Web_Crawling; sid:2002944; rev:6;)

#by Jacob Kitchel
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY python.urllib User Agent Web Crawl"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| "; nocase;
content:"python.urllib/"; nocase; within:50; threshold: type both, track by_src, count 10, seconds 60; classtype: attempted-recon; reference:url,docs.python.org/lib/module-urllib.html;
reference:url,doc.emergingthreats.net/2002943; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Web_Crawling; sid:2002943; rev:7;)

#by Jacob Kitchel
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY Java Url Lib User Agent"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| "; nocase; content:"Java/";
nocase; within:50; pcre:"/User-Agent\:[^\n]+Java/\d\.\d+/i"; classtype: attempted-recon; reference:url,www.mozilla.org/docs/netlib/seealso/netmods.html;
reference:url,doc.emergingthreats.net/2002946; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Web_Crawling; sid:2002946; rev:6;)

#by Jacob Kitchel
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY Java Url Lib User Agent Web Crawl"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| "; nocase;
content:"Java/"; nocase; within:50; pcre:"/User-Agent\:[^\n]+Java/\d\.\d+/i"; threshold: type both, track by_src, count 10, seconds 60; classtype: attempted-recon;
reference:url,www.mozilla.org/docs/netlib/seealso/netmods.html; reference:url,doc.emergingthreats.net/2002945; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Web_Crawling; sid:2002945; rev:7;)

#Originally posted by Matt Jonkman, major tweaks by Matt Watchinski.
#Less useful rules are disabled, feel free to enable if you require the information. They are functional and accurate
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Yahoo Mail Inbox View"; flow:to_server,established; uricontent:"/ym/ShowFolder"; nocase; content:"rb=Inbox";
nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/2000041; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Webmail; sid:2000041;
rev:13;)

#Originally posted by Matt Jonkman, major tweaks by Matt Watchinski.
#Less useful rules are disabled, feel free to enable if you require the information. They are functional and accurate
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Yahoo Mail Message View"; flow:to_server,established; uricontent:"/ym/ShowLetter"; nocase; content:"MsgId"; nocase;
classtype: policy-violation; reference:url,doc.emergingthreats.net/2000042; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Webmail; sid:2000042; rev:13;)

#Originally posted by Matt Jonkman, major tweaks by Matt Watchinski.
#Less useful rules are disabled, feel free to enable if you require the information. They are functional and accurate
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Yahoo Mail Message Compose Open"; flow:to_server,established; uricontent:"/ym/Compose"; nocase; classtype: policy-
violation; reference:url,doc.emergingthreats.net/2000043; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Webmail; sid:2000043; rev:13;)

#Originally posted by Matt Jonkman, major tweaks by Matt Watchinski.
#Less useful rules are disabled, feel free to enable if you require the information. They are functional and accurate
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Yahoo Mail Message Send"; flow:to_server,established; uricontent:"/ym/Compose"; nocase; classtype: policy-
violation; reference:url,doc.emergingthreats.net/2000044; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Webmail; sid:2000044; rev:11;)

#Originally posted by Matt Jonkman, major tweaks by Matt Watchinski.
#Less useful rules are disabled, feel free to enable if you require the information. They are functional and accurate
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Yahoo Mail Message Send Info Capture"; flow: to_server,established; content:"crumb="; nocase; content:"Subject=";
nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/2000045; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Webmail; sid:2000045;
rev:11;)

#Originally posted by Matt Jonkman, major tweaks by Matt Watchinski.
#Less useful rules are disabled, feel free to enable if you require the information. They are functional and accurate
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Yahoo Mail General Page View"; flow: to_server,established; uricontent:"/ym/login"; nocase; content:".rand=";
nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/2000341; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Webmail; sid:2000341;
rev:9;)

#Submitted by Jonathan Miner
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Yahoo Briefcase Upload"; flow: to_server,established; content:"briefcase.yahoo.com";
uricontent:"/process_bcmultipart_form"; nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/2001044; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Webmail; sid:2001044; rev:6;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Gmail Inbox Access"; flow: to_server,established; uricontent:"/gmail?view=tl&search=inbox&start="; nocase;
classtype: policy-violation; reference:url,doc.emergingthreats.net/2001424; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Webmail; sid:2001424; rev:6;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Gmail File Send"; flow:to_server,established; content:"Content-Disposition|3a| form-data|3b| name=|22|msgbody|22|";
nocase; content:"name=|22|form-data|3b| file0|22 3b| filename=|22|"; nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/2001425;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Webmail; sid:2001425; rev:9;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Gmail Message Send"; flow: to_server,established; content:"Content-Disposition|3A| form-data|3b| name=|22|to|22|";
nocase; content:"Content-Disposition|3A| form-data|3b| name=|22|msgbody|22|"; nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/2001426;
```

```
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Webmail; sid:2001426; rev:8;)

#by Andrew Wood
#added more unique match
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Winamp Streaming User Agent"; flow:established,to_server; content:"User-Agent|3A|"; nocase; content:"Winamp";
distance:0; within:100; nocase; pcre:"/User-Agent\x3a[^\n]+Winamp/i"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2003168;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Winamp; sid:2003168; rev:8;)

#this sig is to catch HTTP User agents that specify Windows 3.1 as the platform
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Windows 3.1 User-Agent Detected - Possible Malware or Non-Updated System"; flow:established,to_server; content:"|0d
0a|User-Agent|3a| "; content:"Windows 3.1"; within:200; pcre:"/User-Agent\x3a[^\n]+Windows 3.1/i"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2011694;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Windows_31; sid:2011694; rev:3;)

#by evilghost
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Suspicious Microsoft Windows NT 6.1 User-Agent Detected"; flow:established,to_server; content:"|0d 0a|User-Agent|3a
20|Mozilla/4.0 (compatible|3b| "; nocase; content:"|3b 20|Windows NT 6.1|3b 20|"; distance:0; within:40; threshold:type limit, track by_src, seconds 60, count 1; classtype:policy-
violation; reference:url,www.microsoft.com/windows/windows-7/default.aspx; reference:url,doc.emergingthreats.net/2010228; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Windows_7; sid:2010228; rev:4;)

#this sig is to catch HTTP User agents that specify Windows 98 as the platform
#Mostly to catch spyware and auto-downloaders that still use these as fake User Agent strings
#You may also use this to catch any local win98 machines if they're no longer supposed to be in production
#(which for goodness sake they shouldn't!! Haven't been patched for years!)
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Windows 98 User-Agent Detected - Possible Malware or Non-Updated System"; flow:established,to_server; content:"|0d
0a|User-Agent|3a| "; content:"Windows 98"; within:200; pcre:"/User-Agent\x3a[^\n]+Windows 98/i"; classtype:policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/Windows98UA; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Windows_98; sid:2007695; rev:11;)

#this sig is to catch HTTP User agents that specify Windows 98 as the platform
#Mostly to catch spyware and auto-downloaders that still use these as fake User Agent strings
#You may also use this to catch any local win98 machines if they're no longer supposed to be in production
#(which for goodness sake they shouldn't!! Haven't been patched for years!)
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Windows 98 User-Agent Detected - Possible Malware or Non-Updated System (Win98)"; flow:established,to_server;
content:"|0d 0a|User-Agent|3a| "; content:"Win98"; within:200; pcre:"/User-Agent\x3a[^\n]+Win98/i"; classtype:policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/Windows98UA; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Windows_98; sid:2008070; rev:3;)

#by Jacob Kitchel of infotex
#Windows update operates over port 80 or 443 (443 not detected here). It uses this user
#agent with the hostname. This sig can be used to identify internal hosts that are
#not using an internal patching server,
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY External Windows Update in Progress"; flow:established,to_server; content:"Windows-Update-Agent"; content:"Host|3a|
"; nocase; within:20; pcre:"/User-Agent|3a|[^\n]+Windows-Update-Agent/i"; threshold: type limit, count 1, seconds 300, track by_src; classtype:policy-violation;
reference:url,windowsupdate.microsoft.com; reference:url,doc.emergingthreats.net/2002948; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Windows_Updates;
sid:2002948; rev:10;)

#this sig can be used to track internal updates, or updates in general
#
#alert tcp $HOME_NET any -> any $HTTP_PORTS (msg:"ET POLICY Windows Update in Progress"; flow:established,to_server; content:"Windows-Update-Agent"; content:"Host|3a|"; nocase;
within:20; pcre:"/User-Agent\x3a[^\n]+Windows-Update-Agent/i"; threshold: type limit, count 1, seconds 300, track by_src; classtype:policy-violation;
reference:url,windowsupdate.microsoft.com; reference:url,doc.emergingthreats.net/2002949; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Windows_Updates;
sid:2002949; rev:7;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Winpcap Installation in Progress"; flow:established,to_server; uricontent:"/install/banner/"; nocase;
pcre:"/\d/\d+.jpg/Ui"; content:"Host\: www.winpcap.org"; nocase; content:"User-Agent|3a| NSISDL"; nocase; classtype: policy-violation; reference:url,www.winpcap.org;
reference:url,doc.emergingthreats.net/2002866; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Winpcap_Install; sid:2002866; rev:4;)

#moving to policy, it's just a sign of an install. You should note if that was authoried or not
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Software Install Reporting via HTTP - Wise User Agent (Wise) Sometimes Malware Related"; flow:to_server,established;
content:"|0d 0a|User-Agent|3a| Wise"; classtype:trojan-activity; reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=453076771; reference:url,doc.emergingthreats.net/2002167;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Wise; sid:2002167; rev:14;)

#by Mark Tombaugh
#
#alert udp $HOME_NET any -> $EXTERNAL_NET 88 (msg:"ET POLICY X-Box Live Connecting"; content:"<Xbox Version="; content:" Title=0x"; distance:4; within:32; classtype:policy-violation;
reference:url,www.microsoft.com/xbox/; reference:url,doc.emergingthreats.net/2002796; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Xbox; sid:2002796;
rev:4;)

#by Jamian Mason of Deepnines.com
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Yahoo 360 Social Site Access"; flow:established,to_server; content:"Host|3a| 360.yahoo.com"; threshold: type both,
track by_src, count 5, seconds 300; classtype:policy-violation; reference:url,doc.emergingthreats.net/2003454; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Yahoo360; sid:2003454; rev:4;)

#Submitted by Joel Esler
#
#alert tcp any any -> any any (msg:"ET POLICY ZIPPED DOC in transit"; flow:established; content:"|50 4B 03 04|"; content:"|00|"; content:".doc"; nocase; classtype: not-suspicious;
reference:url,doc.emergingthreats.net/2001402; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Zip_Contents; sid:2001402; rev:5;)

#Submitted by Joel Esler
#
#alert tcp any any -> any any (msg:"ET POLICY ZIPPED XLS in transit"; flow:established; content:"|50 4B 03 04|"; content:"|00|"; content:".xls"; nocase; classtype: not-suspicious;
reference:url,doc.emergingthreats.net/2001403; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Zip_Contents; sid:2001403; rev:5;)

#Submitted by Joel Esler
#
#alert tcp any any -> any any (msg:"ET POLICY ZIPPED EXE in transit"; flow:established; content:"|50 4B 03 04|"; content:"|00|"; content:".exe"; nocase; classtype: not-suspicious;
reference:url,doc.emergingthreats.net/2001404; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Zip_Contents; sid:2001404; rev:5;)

#Submitted by Joel Esler
#
#alert tcp any any -> any any (msg:"ET POLICY ZIPPED PPT in transit"; flow:established; content:"|50 4B 03 04|"; content:"|00|"; content:".ppt"; nocase; classtype: not-suspicious;
reference:url,doc.emergingthreats.net/2001405; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Zip_Contents; sid:2001405; rev:5;)

#From David Glosser
#
#alert tcp $EXTERNAL_NET any <> $HOME_NET any (msg:"ET POLICY Possible hidden zip extension .cpl"; flow:established; content:"|20 20 2E 63 70 6C 50 4B|"; classtype: suspicious-filename-
detect; reference:url,doc.emergingthreats.net/2001406; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Zip_Contents; sid:2001406; rev:10;)

#From David Glosser
#
#alert tcp $EXTERNAL_NET any <> $HOME_NET any (msg:"ET POLICY Possible hidden zip extension .pif"; flow:established; content:"|20 20 2E 70 69 66 50 4B|"; classtype: suspicious-filename-
detect; reference:url,doc.emergingthreats.net/2001407; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Zip_Contents; sid:2001407; rev:10;)

#From David Glosser
#
#alert tcp $EXTERNAL_NET any <> $HOME_NET any (msg:"ET POLICY Possible hidden zip extension .scr"; flow:established; content:"|20 20 2E 73 63 72 50 4B|"; classtype: suspicious-filename-
detect; reference:url,doc.emergingthreats.net/2001408; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Zip_Contents; sid:2001408; rev:10;)

#by pedro marinhi
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS p2p Related User Agent (eChanblard)"; flow:to_server,established; content:"GET "; depth:4; content:"|0d
0a|User-Agent|3a| eChanblard|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011232; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_echanblard; sid:2011232; rev:3;)

#by Kevin Ross
#
#alert tcp $HTTP_SERVERS $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET SCAN Unusually Fast 403 Error Messages, Possible Web Application Scan"; flow:from_server,established;
content:"HTTP/1.1 403"; depth:13; threshold: type threshold, track by_dst, count 35, seconds 60; classtype:attempted-recon; reference:url,www.checkupdown.com/status/E403.html;
reference:url,doc.emergingthreats.net/2009749; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_403; sid:2009749; rev:3;)

#by David Wharton
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Absinthe SQL Injection Tool HTTP Header Detected"; flow:established,to_server; content:"|0d 0a|User-Agent|3A|
Absinthe"; nocase; classtype:attempted-recon; reference:url,0x90.org/releases/absinthe; reference:url,doc.emergingthreats.net/2009555; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_Absinthe; sid:2009555; rev:4;)

#by Kevin Ross
#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Acunetix Version 6 Crawl/Scan Detected"; flow:to_server,established; uricontent:"/acunetix-wvs-test-for-some-
inexistent-file"; threshold: type threshold, track by_dst, count 2, seconds 5; classtype:attempted-recon; reference:url,www.acunetix.com/; reference:url,doc.emergingthreats.net/2008571;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Acunetix; sid:2008571; rev:4;)

#by Kevin Ross
#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Acunetix Version 6 (Free Edition) Scan Detected"; flow:to_server,established; content:"(Acunetix Web Vulnerability
Scanner"; nocase; threshold: type limit, count 1, seconds 60, track by_src; classtype:attempted-recon; reference:url,www.acunetix.com/; reference:url,doc.emergingthreats.net/2009646;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Acunetix; sid:2009646; rev:5;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN Amap TCP Service Scan Detected"; flow:to_server; flags:PA; content:"service|3A|thc|3A 2F 2F|"; depth:105;
content:"service|3A|thc"; within:40; classtype:attempted-recon; reference:url,freeworld.thc.org/thc-amap/; reference:url,doc.emergingthreats.net/2010371;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Amap; sid:2010371; rev:2;)

#by Kevin Ross
#
alert udp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN Amap UDP Service Scan Detected"; dsize:<135; content:"THCTHCTHCTHC|20 20 20|"; classtype:attempted-recon;
reference:url,freeworld.thc.org/thc-amap/; reference:url,doc.emergingthreats.net/2010372; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Amap; sid:2010372;
rev:2;)

#by Adam Pointon of Sentinel Security
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN Watchfire AppScan Web App Vulnerability Scanner"; flow:established,to_server;
uricontent:"/appscan_fingerprint/mac_address"; nocase; classtype:attempted-recon; reference:url,www.watchfire.com/products/appscan/default.aspx;
reference:url,doc.emergingthreats.net/2008311; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_AppScan; sid:2008311; rev:4;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Asp-Audit Web Scan Detected"; flow:to_server,established; content:"GET "; depth:4; uricontent:"/?
<//STYLE=x|3a|e/**/xpression(alert('asp-audit'))>"; classtype:attempted-recon; reference:url,www.hacker-soft.net/Soft/Soft_2895.htm; reference:url,wiki.remote-
exploit.org/backtrack/wiki/asp-audit; reference:url,doc.emergingthreats.net/2009479; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_AspAudit; sid:2009479;
rev:7;)

#by Martin Holste
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN Automated Injection Tool User-Agent (AutoGetColumn)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
AutoGetColumn"; classtype:attempted-recon; reference:url,doc.emergingthreats.net/2009154; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_AutoGetColumn;
sid:2009154; rev:6;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Brute Force Exploit Detector HTTP Buffer Overflow Detection"; flow:to_server,established; content:"HEAD "; nocase;
depth:5; uricontent:"AAAAAAAAAAAAA"; content:"HTTP/1.0"; classtype:attempted-recon; reference:url,www.snake-basket.de/bed.html; reference:url,doc.emergingthreats.net/2008596;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_BED; sid:2008596; rev:5;)

#by Michael Sconzo of ERCOT
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN bsqlbf Brute Force SQL Injection"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| bsqlbf"; nocase;
classtype:web-application-activity; reference:url,code.google.com/p/bsqlbf-v2/; reference:url,doc.emergingthreats.net/2008362; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_BSQLBF; sid:2008362; rev:3;)

#These are intended to catch new worms and such scanning internally. Careful of falses.
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 3127 (msg:"ET SCAN Behavioral Unusual Port 3127 traffic, Potential Scan or Backdoor"; flags: S,12; threshold: type both, track by_src, count 10
, seconds 60; classtype: misc-activity; reference:url,doc.emergingthreats.net/2002973; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Backdoors; sid:2002973;
rev:4;)

#by kevin ross
#
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"ET SNMP Attempted UDP Access Attempt to Cisco IOS 12.1 Hidden Read/Write Community String ILMI"; content:"ILMI"; nocase;
classtype:attempted-admin; reference:url,www.cisco.com/warp/public/707/cisco-sa-20010228-ios-snmp-community.shtml; reference:url,www.cisco.com/warp/public/707/cisco-sa-20010227-ios-
snmp-ilmi.shtml; reference:url,doc.emergingthreats.net/2011011; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Cisco; sid:2011011; rev:2;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"ET SNMP Attempted TCP Access Attempt to Cisco IOS 12.1 Hidden Read/Write Community String ILMI"; flow:to_server,established;
content:"ILMI"; nocase; classtype:attempted-admin; reference:url,www.cisco.com/warp/public/707/cisco-sa-20010228-ios-snmp-community.shtml;
reference:url,www.cisco.com/warp/public/707/cisco-sa-20010227-ios-snmp-ilmi.shtml; reference:url,doc.emergingthreats.net/2011012; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_Cisco; sid:2011012; rev:2;)

#by kevin ross
#
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"ET SNMP Attempted UDP Access Attempt to Cisco IOS 12.1 Hidden Read/Write Community String cable-docsis"; content:"cable-docsis";
nocase; classtype:attempted-admin; reference:url,www.cisco.com/warp/public/707/cisco-sa-20010228-ios-snmp-community.shtml;
reference:url,www.iss.net/security_center/reference/vuln/cisco-ios-cable-docsis.htm; reference:url,www.kb.cert.org/vuls/id/840665; reference:cve,2004-1776;
reference:url,doc.emergingthreats.net/2011013; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Cisco; sid:2011013; rev:2;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"ET SNMP Attempted TCP Access Attempt to Cisco IOS 12.1 Hidden Read/Write Community String cable-docsis"; flow:to_server,established;
content:"cable-docsis"; nocase; classtype:attempted-admin; reference:url,www.cisco.com/warp/public/707/cisco-sa-20010228-ios-snmp-community.shtml;
reference:url,www.iss.net/security_center/reference/vuln/cisco-ios-cable-docsis.htm; reference:url,www.kb.cert.org/vuls/id/840665; reference:cve,2004-1776;
reference:url,doc.emergingthreats.net/2011014; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Cisco; sid:2011014; rev:2;)

#by Kevin Ross
#CISCO TORCH SCAN DETECTION RULES
#
alert udp $EXTERNAL_NET any -> $HOME_NET 69 (msg:"ET SCAN Cisco Torch TFTP Scan"; content:"|52 61 6E 64 30 6D 53 54 52 49 4E 47 00 6E 65 74 61 73 63 69 69|"; offset:2; depth:21;
classtype:attempted-recon; reference:url,www.hackingexposedcisco.com/?link=tools; reference:url,www.securiteam.com/tools/5EP0F1FEUA.html; reference:url,doc.emergingthreats.net/2008414;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Cisco_Torch; sid:2008414; rev:2;)

#by Kevin Ross
#CISCO TORCH SCAN DETECTION RULES
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN Cisco Torch IOS HTTP Scan"; flow:to_server,established; content:"User-Agent|3a| Cisco-torch"; classtype:attempted-
recon; reference:url,www.hackingexposedcisco.com/?link=tools; reference:url,www.securiteam.com/tools/5EP0F1FEUA.html; reference:url,doc.emergingthreats.net/2008415;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Cisco_Torch; sid:2008415; rev:5;)
```

```
#by Kevin Ross
#CISCO TORCH SCAN DETECTION RULES
#
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"ET SCAN Cisco Torch SNMP Scan"; content:"public"; content:"|30 0C 06 08 2B 06 01 02 01 01 01 00 05 00|"; classtype:attempted-recon;
reference:url,www.hackingexposedcisco.com/?link=tools; reference:url,www.securiteam.com/tools/5EP0F1FEUA.html; reference:url,doc.emergingthreats.net/2008597;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Cisco_Torch; sid:2008597; rev:2;)

#by Jack Pepper
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN Core-Project Scanning Bot UA Detected"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| core-project/1.0";
classtype:web-application-activity; reference:url,doc.emergingthreats.net/2008529; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Coreproject; sid:2008529;
rev:3;)

#Submitted 2006-10-30 by Frank Knobbe
#
##alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET DELETED Crewbox Proxy Scan"; flow:established,to_server; uricontent:".php?"; nocase;
uricontent:"crewbox.by.ru/crew/"; nocase; classtype:attempted-recon; reference:url,doc.emergingthreats.net/2003156; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_Crewscan; sid:2003156; rev:5;)

#by evilghost
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN crimscanner User-Agent detected"; flow:established,to_server; content:"GET "; depth:4; nocase; content:"|0d 0a|User-
Agent|3a| crimscanner/"; nocase; classtype:network-scan; reference:url,doc.emergingthreats.net/2010954; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_Crimsonscanner; sid:2010954; rev:3;)

#by Adam Pointon of Sentinel Security
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN DEBUG Method Request with Command"; flow:established,to_server; content:"DEBUG "; depth:6; content:"|0d 0a|Command|3a|
"; distance:0; classtype:attempted-recon; reference:url,doc.emergingthreats.net/2008312; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_DEBUG_Method;
sid:2008312; rev:3;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Possible DavTest WebDav Vulnerability Scanner Initial Check Detected"; flow:established,to_server;
content:"PROPFIND "; depth:9; content:"D|3A|propfind xmlns|3A|D=|22|DAV|3A 22|><D|3A|allprop/></D|3A|propfind>"; distance:0; classtype:attempted-recon;
reference:url,www.darknet.org.uk/2010/04/davtest-webdav-vulerability-scanning-scanner-tool/; reference:url,code.google.com/p/davtest/; reference:url,doc.emergingthreats.net/2011088;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Davtest; sid:2011088; rev:2;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN DavTest WebDav Vulnerability Scanner Default User Agent Detected"; flow:established,to_server; content:"|0d
0a|User-Agent|3a| DAV.pm/v"; classtype:attempted-recon; reference:url,www.darknet.org.uk/2010/04/davtest-webdav-vulerability-scanning-scanner-tool/;
reference:url,code.google.com/p/davtest/; reference:url,doc.emergingthreats.net/2011089; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Davtest; sid:2011089;
rev:2;)

#by evilghost
#
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN ICMP Delphi, Likely Precursor to Scan"; itype:8; icode:0; content:"Pinging from Delphi code written"; classtype:misc-
activity; reference:url,www.koders.com/delphi/fid942A4EAF946B244BD3CD9BC83FEAAC35BA1F38AB.aspx; reference:url,doc.emergingthreats.net/2010681; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_Delphi; sid:2010681; rev:2;)

#by Adam Pointon at Sentinel Data Security
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN DirBuster Web App Scan in Progress"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| DirBuster";
classtype:web-application-attack; reference:url,owasp.org; reference:url,doc.emergingthreats.net/2008186; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_DirBuster; sid:2008186; rev:3;)

#by Kevin Ross
#
alert udp $EXTERNAL_NET any -> $HOME_NET 4569 (msg:"ET SCAN Enumiax Inter-Asterisk Exchange Protocol Username Scan"; content:"|00 00|"; content:"|06 0D 06 01 30 13 02 07 08|";
within:10; depth:40; classtype:attempted-recon; reference:url,sourceforge.net/projects/enumiax/; reference:url,doc.emergingthreats.net/2008606;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Enumiax; sid:2008606; rev:2;)

#Submitted by Frank Knobbe
#Note: These are more effective as pass rules to avoid getting hits on other rules that don't really apply. This is benign load balancer probe traffic.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN F5 BIG-IP 3DNS TCP Probe 1"; id: 1; dsize: 24; flags: S,12; content:"|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00|"; window: 2048; classtype: misc-activity; reference:url,www.f5.com/f5products/v9intro/index.html; reference:url,doc.emergingthreats.net/2001609;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_F5_BIG-IP_Probe; sid:2001609; rev:12;)

#Submitted by Frank Knobbe
#Note: These are more effective as pass rules to avoid getting hits on other rules that don't really apply. This is benign load balancer probe traffic.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN F5 BIG-IP 3DNS TCP Probe 2"; id: 2; dsize: 24; flags: S,12; content:"|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00|"; window: 2048; classtype: misc-activity; reference:url,www.f5.com/f5products/v9intro/index.html; reference:url,doc.emergingthreats.net/2001610;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_F5_BIG-IP_Probe; sid:2001610; rev:12;)

#Submitted by Frank Knobbe
#Note: These are more effective as pass rules to avoid getting hits on other rules that don't really apply. This is benign load balancer probe traffic.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN F5 BIG-IP 3DNS TCP Probe 3"; id: 3; dsize: 24; flags: S,12; content:"|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00|"; window: 2048; classtype: misc-activity; reference:url,www.f5.com/f5products/v9intro/index.html; reference:url,doc.emergingthreats.net/2001611;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_F5_BIG-IP_Probe; sid:2001611; rev:12;)

#by atomic-penguin, tweak by matt Jonkman to cover other ftp daemons like freeftpd and warftpd
#
alert tcp $HOME_NET 21 -> $EXTERNAL_NET any (msg:"ET SCAN Potential FTP Brute-Force attempt"; flow:from_server,established; dsize:<100; content:"530 "; depth:4; pcre:"/530\s+
(Login|User|Failed|Not)/smi"; classtype:unsuccessful-user; threshold: type threshold, track by_dst, count 5, seconds 300; reference:url,doc.emergingthreats.net/2002383;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_FTP_Brute_Force; sid:2002383; rev:11;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET SCAN Multiple FTP Root Login Attempts from Single Source - Possible Brute Force Attempt"; flow:established,to_server; content:"USER
"; nocase; depth:5; content:"root"; within:15; nocase; threshold: type threshold, track by_src, count 5, seconds 60; classtype:attempted-recon;
reference:url,doc.emergingthreats.net/2010642; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_FTP_Brute_Force; sid:2010642; rev:3;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET SCAN Multiple FTP Administrator Login Attempts from Single Source - Possible Brute Force Attempt"; flow:established,to_server;
content:"USER "; nocase; depth:5; content:"administrator"; within:25; nocase; threshold: type threshold, track by_src, count 5, seconds 60; classtype:attempted-recon;
reference:url,doc.emergingthreats.net/2010643; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_FTP_Brute_Force; sid:2010643; rev:3;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET FTP Possible FTP Daemon Username SELECT FROM SQL Injection Attempt"; flow:established,to_server; content:"USER"; depth:4;
content:"SELECT"; within:200; nocase; content:"FROM"; distance:0; nocase; pcre:"/SELECT.+FROM/i"; classtype:attempted-user; reference:url,en.wikipedia.org/wiki/SQL_injection;
reference:url,doc.emergingthreats.net/2009981; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_FTP_SQL_Injection; sid:2009981; rev:2;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET FTP Possible FTP Daemon Username DELETE FROM SQL Injection Attempt"; flow:established,to_server; content:"USER"; depth:4;
content:"DELETE"; within:200; nocase; content:"FROM"; distance:0; nocase; pcre:"/DELETE.+FROM/i"; classtype:attempted-user; reference:url,en.wikipedia.org/wiki/SQL_injection;
reference:url,doc.emergingthreats.net/2009982; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_FTP_SQL_Injection; sid:2009982; rev:2;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET FTP Possible FTP Daemon Username INSERT INTO SQL Injection Attempt"; flow:established,to_server; content:"USER"; depth:4;
content:"INSERT"; within:200; nocase; content:"INTO"; distance:0; nocase; pcre:"/INSERT.+INTO/i"; classtype:attempted-user; reference:url,en.wikipedia.org/wiki/SQL_injection;
```

```
reference:url,doc.emergingthreats.net/2009983; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_FTP_SQL_Injection; sid:2009983; rev:2;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET FTP Possible FTP Daemon Username UPDATE SET SQL Injection Attempt"; flow:established,to_server; content:"USER"; depth:4;
content:"UPDATE"; within:200; nocase; content:"SET"; distance:0; nocase; pcre:"/UPDATE.+SET/i"; classtype:attempted-user; reference:url,en.wikipedia.org/wiki/SQL_injection;
reference:url,doc.emergingthreats.net/2009984; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_FTP_SQL_Injection; sid:2009984; rev:2;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET FTP Possible FTP Daemon Username UNION SELECT SQL Injection Attempt"; flow:established,to_server; content:"USER"; depth:4;
content:"UNION"; within:200; nocase; content:"SELECT"; distance:0; nocase; pcre:"/UNION.+SELECT/i"; classtype:attempted-user; reference:url,en.wikipedia.org/wiki/SQL_injection;
reference:url,doc.emergingthreats.net/2009985; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_FTP_SQL_Injection; sid:2009985; rev:2;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET FTP Possible FTP Daemon Username INTO OUTFILE SQL Injection Attempt"; flow:established,to_server; content:"USER"; depth:4;
content:"INTO"; within:200; nocase; content:"OUTFILE"; distance:0; nocase; pcre:"/INTO.+OUTFILE/i"; classtype:attempted-user; reference:url,www.milw0rm.com/papers/372;
reference:url,www.greensql.net/publications/backdoor-webserver-using-mysql-sql-injection; reference:url,websec.wordpress.com/2007/11/17/mysql-into-outfile/;
reference:url,doc.emergingthreats.net/2010081; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_FTP_SQL_Injection; sid:2010081; rev:2;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Possible Fast-Track Tool Spidering User-Agent Detected"; flow:established,to_server; content:"|0d 0a|User-
Agent|3A| pymills-spider/"; classtype:attempted-recon; reference:url,www.offensive-security.com/metasploit-unleashed/Fast-Track-Modes; reference:url,doc.emergingthreats.net/2011721;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Fasttrack_Spider; sid:2011721; rev:2;)

#Matt Jonkman
#Looking for brute forcing of mail services
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 110 (msg:"ET SCAN Rapid POP3 Connections - Possible Brute Force Attack"; flags: S,12; threshold: type both, track by_src, count 10, seconds 120;
classtype: misc-activity; reference:url,doc.emergingthreats.net/2002992; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_General_Services; sid:2002992; rev:5;)

#Matt Jonkman
#Looking for brute forcing of mail services
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 995 (msg:"ET SCAN Rapid POP3S Connections - Possible Brute Force Attack"; flags: S,12; threshold: type both, track by_src, count 10, seconds
120; classtype: misc-activity; reference:url,doc.emergingthreats.net/2002993; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_General_Services; sid:2002993;
rev:5;)

#Matt Jonkman
#Looking for brute forcing of mail services
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 143 (msg:"ET SCAN Rapid IMAP Connections - Possible Brute Force Attack"; flags: S,12; threshold: type both, track by_src, count 10, seconds 120;
classtype: misc-activity; reference:url,doc.emergingthreats.net/2002994; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_General_Services; sid:2002994; rev:5;)

#Matt Jonkman
#Looking for brute forcing of mail services
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 993 (msg:"ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack"; flags: S,12; threshold: type both, track by_src, count 20, seconds 60;
classtype: misc-activity; reference:url,doc.emergingthreats.net/2002995; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_General_Services; sid:2002995; rev:7;)

#Seen being used for vuln scanning.
#The original script it's modified from is legitimate, so there may be some falses
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN Suspicious User-Agent - get-minimal - Possible Vuln Scan"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
get-minimal"; classtype:attempted-admin; reference:url,doc.emergingthreats.net/2003634; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Get-minimal_UA;
sid:2003634; rev:7;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Grabber.py Web Scan Detected"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Grabber"; offset:110;
depth:30; classtype:attempted-recon; reference:url,rgaucher.info/beta/grabber/; reference:url,doc.emergingthreats.net/2009483; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_Grabber.py; sid:2009483; rev:3;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Grendel Web Scan - Default User Agent Detected"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
Mozilla/5.0 (compatible|3b| Grendel-Scan"; nocase; content:"http|3a|//www.grendel-scan.com"; offset:90; distance:1; depth:55; nocase; threshold: type threshold, track by_dst, count 50,
seconds 60; classtype:attempted-recon; reference:url,www.grendel-scan.com; reference:url,doc.emergingthreats.net/2009480; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_Grendel; sid:2009480; rev:4;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Grendel-Scan Web Application Security Scan Detected"; flow:to_server,established; content:"GET "; depth:4;
uricontent:"/random"; nocase; pcre:"/\x2Frandom.+\x2E(html|bat|htm|vbs|do|xdl|htr|swf|wsdl|pl|php3|cfm|cgi|cfc|axd|asp)/Ui"; threshold: type threshold, track by_dst, count 20, seconds
40; classtype:attempted-recon; reference:url,www.grendel-scan.com; reference:url,doc.emergingthreats.net/2009481; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_Grendel; sid:2009481; rev:3;)

#by JP Vossen and Safka : http://library.pantek.com/Mailing%20Lists/snort.org/snort-sigs/03/08/1120.html
#
alert tcp any any -> any 21 (msg:"ET SCAN Grim's Ping ftp scanning tool"; flow:to_server,established; content:"PASS "; content:"gpuser@home.com"; within:18; classtype:network-scan;
reference:url,archives.neohapsis.com/archives/snort/2002-04/0448.html; reference:url,grimsping.cjb.net; reference:url,doc.emergingthreats.net/2007802;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Grims_FTP; sid:2007802; rev:4;)

#by will metcalf
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN HZZP Scan in Progress calc in Headers"; flow:to_server,established; content:"GET "; depth:4;
content:"C|3a|/WINDOWS/system32/calc.exe"; content:"|0d 0a|"; within:9; pcre:"/^.+\x3a\s(test.)?C\:\/WINDOWS\/system32\/calc\.exe(.test)?\r$/m"; classtype: attempted-recon;
reference:url,www.krakowlabs.com/dev.html; reference:url,doc.emergingthreats.net/2011028; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_HZZP; sid:2011028;
rev:5;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Halberd Load Balanced Webserver Detection Scan"; flow:to_server,established; content:"Pragma|3a| no-cache";
content:"Firefox/1.0.3"; offset:40; distance:40; threshold: type threshold, track by_src, count 40, seconds 15; classtype:attempted-recon; reference:url,www.halberd.superadditive.com;
reference:url,doc.emergingthreats.net/2008536; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Halberd; sid:2008536; rev:5;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Hmap Webserver Fingerprint Scan"; flow:to_server,established; content:"GET / HTTP/1.0"; depth:14; content:"|0d
0a|User-Agent|3a| Mozilla"; content:"4.75 [en] (Windows NT 5.0"; offset:20; depth:60; classtype:attempted-recon; reference:url,www.ujeni.murkyroc.com/hmap/;
reference:url,doc.emergingthreats.net/2008537; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Hmap; sid:2008537; rev:5;)

#by Kevin Ross
#Turned content matches into uricontent matches for performance, new uricontent match for traversal= also and incremented revision number.
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Httprecon Web Server Fingerprint Scan"; flow:to_server,established; content:"GET "; depth:4;
uricontent:"/etc/passwd?format="; uricontent:"><script>alert('xss')"; uricontent:"traversal="; classtype:attempted-recon; reference:url,www.computec.ch/projekte/httprecon/;
reference:url,doc.emergingthreats.net/2008627; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Httprecon; sid:2008627; rev:6;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Httprint Web Server Fingerprint Scan"; flow:established,to_server; content:"GET "; depth:4;
uricontent:"/antidisestablishmentarianism"; classtype:attempted-recon; reference:url,www.net-square.com/httprint/; reference:url,www.net-square.com/httprint/httprint_paper.html;
reference:url,doc.emergingthreats.net/2008416; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Httprint; sid:2008416; rev:4;)

#by Jonathan Scheidell
#
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN IBM NSA User Agent"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| "; nocase; content:"Network-Services-
Auditor"; within:50; threshold: type limit, track by_src,count 1, seconds 60; classtype:attempted-recon; reference:url,ftp.inf.utfsm.cl/pub/Docs/IBM/Tivoli/pdfs/sg246021.pdf;
reference:url,doc.emergingthreats.net/2003171; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_IBM_NSA; sid:2003171; rev:6;)

#by evilghost
#
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN ICMP =XXXXXXXX Likely Precursor to Scan"; itype:8; icode:0; content:"=XXXXXXXX"; classtype:misc-activity;
reference:url,doc.emergingthreats.net/2010686; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_ICMP; sid:2010686; rev:2;)

#Submitted by Joseph Gama
#
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN ICMP PING IPTools"; itype: 8; icode: 0; content:"|A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7
A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7|"; depth: 64; classtype: misc-activity; reference:url,www.ks-
soft.net/ip-tools.eng; reference:url,www.ks-soft.net/ip-tools.eng/index.htm; reference:url,doc.emergingthreats.net/2000575; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_IPTools; sid:2000575; rev:7;)

#by evilghost
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN HTTP GET invalid method case"; flow:established,to_server; content:"get "; depth:4; nocase; content:!"GET "; depth:4;
classtype:bad-unknown; reference:url,www.w3.org/Protocols/rfc2616/rfc2616-sec9.html; reference:url,doc.emergingthreats.net/2011031; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_Invalid_Method; sid:2011031; rev:2;)

#by evilghost
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN HTTP POST invalid method case"; flow:established,to_server; content:"post "; depth:5; nocase; content:!"POST ";
depth:5; classtype:bad-unknown; reference:url,www.w3.org/Protocols/rfc2616/rfc2616-sec9.html; reference:url,doc.emergingthreats.net/2011032; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_Invalid_Method; sid:2011032; rev:2;)

#by evilghost
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN HTTP HEAD invalid method case"; flow:established,to_server; content:"head "; depth:5; nocase; content:!"HEAD ";
depth:5; classtype:bad-unknown; reference:url,www.w3.org/Protocols/rfc2616/rfc2616-sec9.html; reference:url,doc.emergingthreats.net/2011033; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_Invalid_Method; sid:2011033; rev:2;)

#by evilghost
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN HTTP OPTIONS invalid method case"; flow:established,to_server; content:"options "; depth:8; nocase; content:!"OPTIONS
"; depth:8; classtype:bad-unknown; reference:url,www.w3.org/Protocols/rfc2616/rfc2616-sec9.html; reference:url,doc.emergingthreats.net/2011034;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Invalid_Method; sid:2011034; rev:2;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN OWASP Joomla Vulnerability Scanner Detected"; flow:established,to_server; content:"HEAD "; depth:5;
uricontent:"/joomla/"; content:"|0d 0a|User-Agent|3a| Mozilla/5.0 (Windows\; U\; Windows NT 5.2\; en-US\; rv|3a|1.9.0.3) Gecko/2008092417 Firefox/3.0.3";
pcre:"/(/joomla/admin|/joomla/administrator|/joomla/manage|/joomla/administration)/U"; threshold: type threshold, track by_dst, count 4, seconds 15; classtype:attempted-recon;
reference:url,www.owasp.org/index.php/Category%3aOWASP_Joomla_Vulnerability_Scanner_Project; reference:url,doc.emergingthreats.net/2009837; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_Joomla; sid:2009837; rev:4;)

#by Kevin Ross
#
alert udp $EXTERNAL_NET any -> $HOME_NET 1434 (msg:"ET SCAN NNG MS02-039 Exploit False Positive Generator - May Conceal A Genuine Attack"; content:"nng Snort (Snort)"; offset:90;
threshold:type threshold, track by_dst, count 4, seconds 15; classtype:misc-activity; reference:url,packetstormsecurity.nl/filedesc/nng-4.13r-public.rar.html;
reference:url,doc.emergingthreats.net/2008560; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_MS02-039; sid:2008560; rev:2;)

#by Jamie Riden
#
#alert tcp any any -> any 502 (msg:"ET SCAN Modbus Scanning detected"; content:"|00 00 00 00 00 02|"; flow:established,to_server; depth:6; threshold: type both, track by_src, count 100,
seconds 10; classtype:bad-unknown; reference:url,code.google.com/p/modscan/; reference:url,www.rtaautomation.com/modbustcp/; reference:url,doc.emergingthreats.net/2009286;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Modbus; sid:2009286; rev:3;)

#By Jeff Kell, tweaks by Dale Handy
#
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 3306 (msg:"ET SCAN MYSQL 4.0 brute force root login attempt"; flow:to_server,established; content:"|01|"; offset:3; depth:4;
content:"root|00|"; nocase; distance:5; within:5; threshold:type both,track by_src,count 5,seconds 60; classtype:protocol-command-decode;
reference:url,www.redferni.uklinux.net/mysql/MySQL-323.html; reference:url,doc.emergingthreats.net/2001906; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_Mysql; sid:2001906; rev:6;)

#Dale Handy
#
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 3306 (msg:"ET SCAN MYSQL 4.1 brute force root login attempt"; flow:to_server,established; content:"|01|"; offset:3; depth:4;
content:"root|00|"; nocase; distance:32; within:5; threshold:type both,track by_src,count 5,seconds 60; classtype:protocol-command-decode;
reference:url,www.redferni.uklinux.net/mysql/MySQL-Protocol.html; reference:url,doc.emergingthreats.net/2002842; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_Mysql; sid:2002842; rev:4;)

#by Kevin Ross
#
alert tcp $HOME_NET 3306 -> any any (msg:"ET SCAN Non-Allowed Host Tried to Connect to MySQL Server"; flow:from_server,established; content:"|6A 04|Host|20 27|"; depth:70; content:"|27
20|is not allowed to connect to this MySQL server"; distance:0; classtype:attempted-recon; reference:url,www.cyberciti.biz/tips/how-do-i-enable-remote-access-to-mysql-database-
server.html; reference:url,doc.emergingthreats.net/2010493; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Mysql; sid:2010493; rev:2;)

#by Kevin Ross
#
alert tcp $HOME_NET 3306 -> $EXTERNAL_NET any (msg:"ET SCAN Multiple MySQL Login Failures, Possible Brute Force Attempt"; flow:from_server,established; content:"|15 04|"; depth:64;
content:"|32 38 30 30 30|Access denied for user|20|"; distance:0; content:"using password|3A 20|"; threshold: type threshold, track by_src, count 5, seconds 120; classtype:attempted-
recon; reference:url,doc.emergingthreats.net/2010494; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Mysql; sid:2010494; rev:2;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Mini MySqlatOr SQL Injection Scanner"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
prog.CustomCrawler"; offset:60; classtype:attempted-recon; reference:url,www.scrt.ch/pages_en/minimysqlator.html; reference:url,doc.emergingthreats.net/2008729;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Mysqlator; sid:2008729; rev:4;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Default Mysqloit User Agent Detected - Mysql Injection Takover Tool"; flow:established,to_server; content:"|0d
0a|User-Agent|3a| Mysqloit"; classtype:attempted-recon; reference:url,code.google.com/p/mysqloit/; reference:url,doc.emergingthreats.net/2009882;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Mysqloit; sid:2009882; rev:2;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Possible Mysqloit Operating System Fingerprint/SQL Injection Test Scan Detected"; flow:established,to_server;
uricontent:"+UNION+select+'BENCHMARK(10000000,SHA1(1))"; classtype:attempted-recon; reference:url,code.google.com/p/mysqloit/; reference:url,doc.emergingthreats.net/2009883;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Mysqloit; sid:2009883; rev:4;)

#Submitted by Joseph Gama
#updated by mareadmin 4/2010
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN NMAP -sS window 2048"; fragbits:!D; dsize:0; flags:S,12; ack:0; window:2048; threshold: type both, track by_dst, count 1,
seconds 60; classtype:attempted-recon; reference:url,doc.emergingthreats.net/2000537; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_NMAP; sid:2000537; rev:8;)

#Submitted by Joseph Gama
#updated by mareadmin 4/2010
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN NMAP -sO"; dsize:0; ip_proto:21; threshold: type both, track by_dst, count 1, seconds 60; classtype:attempted-recon;
reference:url,doc.emergingthreats.net/2000536; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_NMAP; sid:2000536; rev:7;)
```

```
#Submitted by Joseph Gama
#updated by mareadmin 4/2010
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN NMAP -sS window 1024"; fragbits:!D; dsize:0; flags:S,12; ack:0; window:1024; threshold: type both, track by_dst, count 1,
seconds 60; classtype:attempted-recon; reference:url,doc.emergingthreats.net/2000537; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_NMAP; sid:2009582; rev:2;)

#Submitted by Joseph Gama
#updated by mareadmin 4/2010
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN NMAP -sS window 3072"; fragbits:!D; dsize:0; flags:S,12; ack:0; window:3072; threshold: type both, track by_dst, count 1,
seconds 60; classtype:attempted-recon; reference:url,doc.emergingthreats.net/2000537; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_NMAP; sid:2009583; rev:2;)

#Submitted by Joseph Gama
#updated by mareadmin 4/2010
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN NMAP -sS window 4096"; fragbits:!D; dsize:0; flags:S,12; ack:0; window:4096; threshold: type both, track by_dst, count 1,
seconds 60; classtype:attempted-recon; reference:url,doc.emergingthreats.net/2000537; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_NMAP; sid:2009584; rev:1;)

#Submitted by Joseph Gama
#updated by mareadmin 4/2010
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN NMAP -sA (1)"; fragbits:!D; dsize:0; flags:A,12; window:1024; threshold: type both, track by_dst, count 1, seconds 60;
classtype:attempted-recon; reference:url,doc.emergingthreats.net/2000538; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_NMAP; sid:2000538; rev:8;)

#Submitted by Joseph Gama
#updated by mareadmin 4/2010
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN NMAP -sA (2)"; fragbits:!D; dsize:0; flags:A,12; window:3072; threshold: type both, track by_dst, count 1, seconds 60;
classtype:attempted-recon; reference:url,doc.emergingthreats.net/2000540; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_NMAP; sid:2000540; rev:8;)

#Submitted by Joseph Gama
#updated by mareadmin 4/2010
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN NMAP -f -sF"; fragbits:!M; dsize:0; flags:F,12; ack:0; window:2048; threshold: type both, track by_dst, count 1, seconds 60;
classtype:attempted-recon; reference:url,doc.emergingthreats.net/2000543; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_NMAP; sid:2000543; rev:7;)

#Submitted by Joseph Gama
#updated by mareadmin 4/2010
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN NMAP -f -sN"; fragbits:!M; dsize:0; flags:0,12; ack:0; window:2048; threshold: type both, track by_dst, count 1, seconds 60;
classtype:attempted-recon; reference:url,doc.emergingthreats.net/2000544; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_NMAP; sid:2000544; rev:7;)

#Submitted by Joseph Gama
#updated by mareadmin 4/2010
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN NMAP -f -sS"; fragbits:!M; dsize:0; flags:S,12; ack:0; window:2048; threshold: type both, track by_dst, count 1, seconds 60;
classtype:attempted-recon; reference:url,doc.emergingthreats.net/2000545; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_NMAP; sid:2000545; rev:7;)

#Submitted by Joseph Gama
#updated by mareadmin 4/2010
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN NMAP -f -sX"; fragbits:!M; dsize:0; flags:FPU,12; ack:0; window:2048; threshold: type both, track by_dst, count 1, seconds
60; classtype:attempted-recon; reference:url,doc.emergingthreats.net/2000546; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_NMAP; sid:2000546; rev:7;)

#by Jaime Blasco
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap NSE)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Nmap
NSE"; classtype:web-application-attack; reference:url,doc.emergingthreats.net/2009359; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_NMAP; sid:2009359; rev:2;)

#by Jaime Blasco
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| Mozilla/5.0 (compatible|3b| Nmap Scripting Engine"; nocase; classtype:web-application-attack; reference:url,doc.emergingthreats.net/2009358;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_NMAP; sid:2009358; rev:2;)

#by Bob Grabowsky
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN Nessus User Agent"; flow: established,to_server; content:"User-Agent|3a|"; depth:300; nocase; content:"Nessus";
nocase; distance:0; within:40; pcre:"/User-Agent\:[^\n]+Nessus/i"; threshold: type limit, track by_src,count 1, seconds 60; classtype: attempted-recon; reference:url,www.nessus.org;
reference:url,doc.emergingthreats.net/2002664; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Nessus; sid:2002664; rev:7;)

#by will metcalf
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Netsparker Default User-Agent"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Mozilla/4.0
(compatible|3b| MSIE 6.0|3b| Windows NT 5.1|3b| SV1|3b| .NET CLR 1.1.4322|3b| Netsparker)"; threshold:type limit,track by_src,count 1,seconds 60; classtype: attempted-recon;
reference:url,www.mavitunasecurity.com/communityedition/; reference:url,doc.emergingthreats.net/2011029; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_NetSparker; sid:2011029; rev:5;)

#by will metcalf
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Netsparker Scan in Progress"; flow:to_server,established; uricontent:"/Netsparker-"; threshold:type limit,track
by_src,count 1,seconds 60; classtype: attempted-recon; reference:url,www.mavitunasecurity.com/communityedition/; reference:url,doc.emergingthreats.net/2011030;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_NetSparker; sid:2011030; rev:4;)

#These are intended to catch new worms and such scanning internally. Careful of falses.
#
alert tcp $HOME_NET any -> any 445 (msg:"ET SCAN Behavioral Unusual Port 445 traffic, Potential Scan or Infection"; flags: S,12; threshold: type both, track by_src, count 70 , seconds
60; classtype: misc-activity; reference:url,doc.emergingthreats.net/2001569; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Netbios; sid:2001569; rev:13;)

#These are intended to catch new worms and such scanning internally. Careful of falses.
#
alert tcp $HOME_NET any -> any 139 (msg:"ET SCAN Behavioral Unusual Port 139 traffic, Potential Scan or Infection"; flags: S,12; threshold: type both, track by_src, count 70 , seconds
60; classtype: misc-activity; reference:url,doc.emergingthreats.net/2001579; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Netbios; sid:2001579; rev:13;)

#These are intended to catch new worms and such scanning internally. Careful of falses.
#
alert tcp $HOME_NET any -> any 137 (msg:"ET SCAN Behavioral Unusual Port 137 traffic, Potential Scan or Infection"; flags: S,12; threshold: type both, track by_src, count 70 , seconds
60; classtype: misc-activity; reference:url,doc.emergingthreats.net/2001580; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Netbios; sid:2001580; rev:13;)

#These are intended to catch new worms and such scanning internally. Careful of falses.
#
alert tcp $HOME_NET any -> any 135 (msg:"ET SCAN Behavioral Unusual Port 135 traffic, Potential Scan or Infection"; flags: S,12; threshold: type both, track by_src, count 70 , seconds
60; classtype: misc-activity; reference:url,doc.emergingthreats.net/2001581; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Netbios; sid:2001581; rev:13;)

#These are intended to catch new worms and such scanning internally. Careful of falses.
#
alert tcp $HOME_NET any -> any 1434 (msg:"ET SCAN Behavioral Unusual Port 1434 traffic, Potential Scan or Infection"; flags: S,12; threshold: type both, track by_src, count 40 , seconds
60; classtype: misc-activity; reference:url,doc.emergingthreats.net/2001582; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Netbios; sid:2001582; rev:13;)

#These are intended to catch new worms and such scanning internally. Careful of falses.
#
alert tcp $HOME_NET any -> any 1433 (msg:"ET SCAN Behavioral Unusual Port 1433 traffic, Potential Scan or Infection"; flags: S,12; threshold: type both, track by_src, count 40 , seconds
60; classtype: misc-activity; reference:url,doc.emergingthreats.net/2001583; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Netbios; sid:2001583; rev:14;)

#by Kevin Ross. Use these externally only, they'll be very noisy internally!
#
#alert udp $HOME_NET 137 -> $EXTERNAL_NET any (msg:"ET SCAN Multiple NBTStat Query Responses to External Destination, Possible Automated Windows Network Enumeration"; content:"|20 43 4b
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21|"; depth:55; threshold: type threshold, track by_dst, count 10, seconds 60;
classtype:attempted-recon; reference:url,technet.microsoft.com/en-us/library/cc940106.aspx; reference:url,doc.emergingthreats.net/2009767; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_Netbios; sid:2009767; rev:4;)
```

```
#This one may be too sensitive
#
#alert udp $HOME_NET 137 -> $EXTERNAL_NET any (msg:"ET SCAN NBTStat Query Response to External Destination, Possible Windows Network Enumeration"; content:"|20 43 4b 41 41 41 41 41 41
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21|"; depth:55; classtype:attempted-recon; reference:url,technet.microsoft.com/en-us/library/cc940106.aspx;
reference:url,doc.emergingthreats.net/2009768; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Netbios; sid:2009768; rev:4;)

#by Bill Scherr IV
#
alert tcp $EXTERNAL_NET any -> $HOME_NET [135,139,445,1024:2048] (msg:"ET SCAN DCERPC rpcmgmt ifids Unauthenticated BIND"; flow:established,to_server; content:"|05|"; content:"|80 bd a8
af 8a 7d c9 11 be f4 08 00 2b 10 29 89|"; distance:31; classtype:attempted-recon; reference:url,www.symantec.com/avcenter/reference/Vista_Network_Attack_Surface_RTM.pdf;
reference:url,www.blackhat.com/presentations/win-usa-04/bh-win-04-seki-up2.pdf; reference:url,seclists.org/fulldisclosure/2003/Aug/0432.html;
reference:url,doc.emergingthreats.net/2009832; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Netbios; sid:2009832; rev:3;)

#by Matt Jonkman
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN Nikto Web App Scan in Progress"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Mozilla/4.75 (Nikto";
threshold: type both, count 5, seconds 60, track by_src; classtype:web-application-attack; reference:url,www.cirt.net/code/nikto.shtml; reference:url,doc.emergingthreats.net/2002677;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Nikto; sid:2002677; rev:9;)

#by Cunningpike
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET SCAN PRO Search Crawler Probe"; flow:to_server,established; content:"PASS "; nocase; depth:5; content:"crawler"; nocase; within:30;
pcre:"/^PASS\s+PRO(-|\s)*search\s+Crawler/smi"; classtype:not-suspicious; reference:url,sourceforge.net/project/showfiles.php?group_id=149797;
reference:url,doc.emergingthreats.net/2008179; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_PRO_Search; sid:2008179; rev:3;)

#by evilghost
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN pangolin SQL injection tool"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| pangolin"; classtype:web-
application-activity; reference:url,www.lifedork.net/pangolin-best-sql-injection-tool.html; reference:url,doc.emergingthreats.net/2010343; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_Pangolin; sid:2010343; rev:4;)

#not a malicious too,l, a testing tool
#sig by Adam Pointon of Sentinelsecurity.com.au
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN Paros Proxy Scanner Detected"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|"; content:"Paros/";
distance:0; within:150; pcre:"/User-Agent\:[^\n]+Paros\//"; classtype:attempted-recon; reference:url,www.parosproxy.org; reference:url,doc.emergingthreats.net/2008187;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Paros_Proxy; sid:2008187; rev:6;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN Pavuk User Agent Detected - Website Mirroring Tool for Off-line Analysis"; flow:established,to_server; content:"|0d
0a|User-Agent|3a| pavuk"; nocase; classtype:attempted-recon; reference:url,pavuk.sourceforge.net/about.html; reference:url,doc.emergingthreats.net/2009827;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Pavuk; sid:2009827; rev:2;)

#by Dennis Distler
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN ProxyReconBot CONNECT method to Mail"; flow:established,to_server; content:"CONNECT "; depth:8; content:"|3A|25
HTTP/"; within:200; classtype:misc-attack; reference:url,doc.emergingthreats.net/2003869; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_ReconBot; sid:2003869;
rev:6;)

#by Dennis Distler
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN ProxyReconBot POST method to Mail"; flow:established,to_server; content:"POST "; depth:5; content:"|3A|25 HTTP/";
within:200; classtype: misc-attack; reference:url,doc.emergingthreats.net/2003870; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_ReconBot; sid:2003870; rev:6;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN SQLBrute SQL Scan Detected"; flow:to_server,established; content:"AND not exists (select * from
master..sysdatabases)"; offset:60; depth:60; classtype:attempted-recon; reference:url,www.justinclarke.com/archives/2006/03/sqlbrute.html;
reference:url,www.darknet.org.uk/2007/06/sqlbrute-sql-injection-brute-force-tool/; reference:url,doc.emergingthreats.net/2009477; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_SQLBrute; sid:2009477; rev:2;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN SQLCheck Database Scan Detected"; flow:to_server,established; content:"%20FROM%20customers"; content:"|0d 0a|User-
Agent|3a| Lynx/2.8.6rel.4 libwww-FM/2.14"; offset:40; distance:70; threshold: type threshold, track by_dst, count 10, seconds 20; classtype:attempted-recon; reference:url,wiki.remote-
exploit.org/backtrack/wiki/SQLcheck; reference:url,doc.emergingthreats.net/2009478; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_SQLCheck; sid:2009478;
rev:3;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN SQLNinja MSSQL Version Scan"; flow:to_server,established; content:"?param=a";
content:"if%20not%28substring%28%28select%20%40%40version"; distance:2; threshold: type threshold, track by_src, count 2, seconds 3; classtype:attempted-recon;
reference:url,sqlninja.sourceforge.net/index.html; reference:url,doc.emergingthreats.net/2009038; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_SQLNinja;
sid:2009038; rev:2;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN SQLNinja MSSQL XPCmdShell Scan"; flow:to_server,established; content:"?param=a";
content:"exec%20master%2E%2Exp%5Fcmdshell"; distance:2; classtype:attempted-recon; reference:url,sqlninja.sourceforge.net/index.html; reference:url,doc.emergingthreats.net/2009039;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_SQLNinja; sid:2009039; rev:2;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN SQLNinja MSSQL User Scan"; content:"?param=a"; flow:to_server,established;
content:"if%20ascii%28substring%28%28select%20system%5Fuser"; distance:2; threshold: type threshold, track by_src, count 20, seconds 10; classtype:attempted-recon;
reference:url,sqlninja.sourceforge.net/index.html; reference:url,doc.emergingthreats.net/2009040; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_SQLNinja;
sid:2009040; rev:3;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN SQLNinja MSSQL Database User Rights Scan"; flow:to_server,established; content:"?param=a";
content:"if%20is%5Fsrvrolemember%28%27sysadmin"; distance:2; classtype:attempted-recon; reference:url,sqlninja.sourceforge.net/index.html; reference:url,doc.emergingthreats.net/2009041;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_SQLNinja; sid:2009041; rev:3;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN SQLNinja MSSQL Authentication Mode Scan"; flow:to_server,established; content:"?param=a";
content:"if%20not%28%28select%20serverproperty%28%27IsIntegratedSecurityOnly"; distance:2; classtype:attempted-recon; reference:url,sqlninja.sourceforge.net/index.html;
reference:url,doc.emergingthreats.net/2009042; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_SQLNinja; sid:2009042; rev:4;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN SQLNinja Attempt To Recreate xp_cmdshell Using sp_configure"; flow:to_server,established; content:"?param=a";
content:"exec%20master%2E%2Esp%5Fconfigure%20%27show%20advanced%20options"; distance:2; classtype:attempted-admin; reference:url,sqlninja.sourceforge.net/index.html;
reference:url,doc.emergingthreats.net/2009043; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_SQLNinja; sid:2009043; rev:3;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN SQLNinja Attempt To Create xp_cmdshell Session"; flow:to_server,established; content:"?param=a";
content:"exec%20master%2E%2Exp%5Fcmdshell%20%27cmd%20%2FC%20%25TEMP"; distance:2; classtype:attempted-admin; reference:url,sqlninja.sourceforge.net/index.html;
reference:url,doc.emergingthreats.net/2009044; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_SQLNinja; sid:2009044; rev:3;)

#Stephen Nesman
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN SQL Injection Attempt (Agent uil2pn)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| uil2pn|0d 0a|";
classtype:web-application-attack; reference:url,www.prevx.com/filenames/89385984947861762-X1/UIL2PN.EXE.html; reference:url,doc.emergingthreats.net/2010215;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_SQLScan; sid:2010215; rev:3;)
```

```
#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN SQL Power Injector SQL Injection User Agent Detected"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
SQL Power Injector"; content:"Security tool (Make sure it is used with the administrator consent)"; within:100; classtype:attempted-recon;
reference:url,www.sqlpowerinjector.com/index.htm; reference:url,en.wikipedia.org/wiki/Sql_injection; reference:url,doc.emergingthreats.net/2009769;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_SQL_Power_Injector; sid:2009769; rev:2;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN SQLix SQL Injection Vector Scan"; flow:established,to_server; content:"GET "; depth:4; content:"myVAR=1234";
content:"Windows 98"; offset:36; within:120; classtype:attempted-recon; reference:url,www.owasp.org/index.php/Category%3aOWASP_SQLiX_Project;
reference:url,doc.emergingthreats.net/2008654; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_SQLix; sid:2008654; rev:4;)

#by Kevin Ross
#new version rotates UA, but this is still good for older versions
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Sqlmap SQL Injection Scan"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| sqlmap";
classtype:attempted-recon; reference:url,sqlmap.sourceforge.net; reference:url,doc.emergingthreats.net/2008538; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_SQLmap; sid:2008538; rev:4;)

#Submitted by Matt Jonkman
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"ET SCAN Potential SSH Scan"; flags:S,12; threshold: type threshold, track by_src, count 5, seconds 120; classtype: attempted-recon;
reference:url,en.wikipedia.org/wiki/Brute_force_attack; reference:url,doc.emergingthreats.net/2001219; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_SSH_Brute_Force; sid:2001219; rev:18;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 22 (msg:"ET SCAN Potential SSH Scan OUTBOUND"; flags:S,12; threshold: type threshold, track by_src, count 5, seconds 120; classtype: attempted-
recon; reference:url,en.wikipedia.org/wiki/Brute_force_attack; reference:url,doc.emergingthreats.net/2003068; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_SSH_Brute_Force; sid:2003068; rev:6;)

#by Jabal Raval
#this string is very unlikely to be seen in normal traffic
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"ET SCAN LibSSH Based SSH Connection - Often used as a BruteForce Tool"; flow:established,to_server; content:"SSH-"; content:"libssh";
within:20; classtype:misc-activity; threshold: type limit, track by_src, count 1, seconds 30; reference:url,doc.emergingthreats.net/2006435; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_SSH_Brute_Force; sid:2006435; rev:6;)

#This is the same as above but has a threshold to help keep events down, and more readily identify brute force attacks
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack!"; flow:established,to_server; content:"SSH-"; content:"libssh";
within:20; threshold: type both, count 5, seconds 30, track by_src; classtype:attempted-admin; reference:url,doc.emergingthreats.net/2006546; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_SSH_Brute_Force; sid:2006546; rev:5;)

#Idea from dynamicnet
#
#alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 443 (msg:"ET SCAN Possible SSL Brute Force attack or Site Crawl"; flow: established; flags: S; threshold: type threshold, track by_src,
count 100, seconds 60; classtype: attempted-dos; reference:url,doc.emergingthreats.net/2001553; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_SSL_Brute_or_Crawl; sid:2001553; rev:7;)

#by Kevin Ross
#
alert udp $EXTERNAL_NET any -> $HOME_NET 5060 (msg:"ET SCAN Sipp SIP Stress Test Detected"; content:"sip|3a|sipp@"; content:"Subject|3a| Performance Test"; offset:90; distance:90;
threshold: type threshold, track by_dst, count 20, seconds 15; classtype:attempted-recon; reference:url,sourceforge.net/projects/sipp/; reference:url,doc.emergingthreats.net/2008579;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Sipp; sid:2008579; rev:3;)

#by Kevin Ross
#
alert udp $EXTERNAL_NET any -> $HOME_NET 5060 (msg:"ET SCAN Sipsak SIP scan"; content:"sip|3a|sipsak@"; offset:90; classtype:attempted-recon; reference:url,sipsak.org/;
reference:url,doc.emergingthreats.net/2008598; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Sipsack; sid:2008598; rev:3;)

#by Kevin Ross
#
alert udp $EXTERNAL_NET any -> $HOME_NET 5060 (msg:"ET SCAN Sipvicious Scan"; content:"From|3A 20 22|sipvicious"; threshold: type limit, count 1, seconds 10, track by_src;
classtype:attempted-recon; reference:url,blog.sipvicious.org; reference:url,doc.emergingthreats.net/2008578; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_Sipvicious; sid:2008578; rev:4;)

#These Detect the Latest Sipvious Scanner Version (0.2.6)
#
alert udp $EXTERNAL_NET any -> $HOME_NET 5060 (msg:"ET SCAN Sipvicious User-Agent Detected (friendly-scanner)"; content:"|0d 0a|User-Agent|3A| friendly-scanner"; classtype:attempted-
recon; reference:url,code.google.com/p/sipvicious/; reference:url,blog.sipvicious.org/; reference:url,doc.emergingthreats.net/2011716; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_Sipvicious; sid:2011716; rev:2;)

#These Detect the Latest Sipvious Scanner Version (0.2.6)
#
alert udp $EXTERNAL_NET any -> $HOME_NET 5060 (msg:"ET SCAN Sipvicious User-Agent Detected (sundayddr)"; content:"|0d 0a|User-Agent|3A| sundayddr"; threshold: type limit, count 1,
seconds 60, track by_src; classtype:attempted-recon; reference:url,code.google.com/p/sipvicious/; reference:url,blog.sipvicious.org/; reference:url,doc.emergingthreats.net/2011766;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Sipvicious; sid:2011766; rev:3;)

#by Kevin Ross
#
alert udp $EXTERNAL_NET any -> $HOME_NET 5060 (msg:"ET SCAN Sivus VOIP Vulnerability Scanner SIP Scan"; content:"SIVuS_VoIP_Scanner <sip|3a|SIVuS"; offset:130; threshold:type threshold,
track by_src, count 3, seconds 10; classtype:attempted-recon; reference:url,www.security-database.com/toolswatch/SiVus-VoIP-Security-Scanner-1-09.html;
reference:url,www.vopsecurity.org/; reference:url,doc.emergingthreats.net/2008609; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Sivius; sid:2008609; rev:4;)

#by Kevin Ross
#
alert udp $EXTERNAL_NET any -> $HOME_NET 5060 (msg:"ET SCAN Sivus VOIP Vulnerability Scanner SIP Components Scan"; content:"sip|3a|sivus-discovery@vopsecurity.org"; offset:110;
classtype:attempted-recon; reference:url,www.security-database.com/toolswatch/SiVus-VoIP-Security-Scanner-1-09.html; reference:url,www.vopsecurity.org/;
reference:url,doc.emergingthreats.net/2008610; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Sivius; sid:2008610; rev:3;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Skipfish Web Application Scan Detected"; flow:established,to_server; content:"|0d 0a|User-Agent|3A| Mozilla/5.0
SF"; threshold:type limit, count 10, seconds 60, track by_src; classtype:attempted-recon; reference:url,isc.sans.org/diary.html?storyid=8467; reference:url,code.google.com/p/skipfish/;
reference:url,doc.emergingthreats.net/2010953; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Skipfish; sid:2010953; rev:2;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Skipfish Web Application Scan Detected (2)"; flow:established,to_server; content:"GET "; depth:4;
uricontent:".old"; content:"|0d 0a|User-Agent|3A| Mozilla/5.0 SF/"; content:"Range|3A| bytes=0-199999"; within:100; classtype:attempted-recon; reference:url,isc.sans.org/diary.html?
storyid=8467; reference:url,code.google.com/p/skipfish/; reference:url,doc.emergingthreats.net/2010956; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Skipfish;
sid:2010956; rev:2;)

#by mareadmin
#springenwerk-xss-scanner (tested with 0.4.5)
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Springenwerk XSS Scanner User-Agent Detected"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
Springenwerk"; offset:30; nocase; classtype:attempted-recon; threshold: type limit, count 1, seconds 60, track by_src; reference:url,springenwerk.org/;
reference:url,doc.emergingthreats.net/2010508; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Springenwerk; sid:2010508; rev:3;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Stompy Web Application Session Scan"; flow:to_server,established; content:"Session Stomper"; offset:100; depth:25;
classtype:attempted-recon; reference:url,www.darknet.org.uk/2007/03/stompy-the-web-application-session-analyzer-tool/; reference:url,doc.emergingthreats.net/2008605;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Stompy; sid:2008605; rev:2;)
```

```
#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN Suspicious User-Agent inbound (bot)"; flow:to_server,established; content:"User-Agent|3a| bot/"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008228; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Suspicious; sid:2008228;
rev:6;)

#These are intended to catch new worms and such scanning internally. Careful of falses.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 23 (msg:"ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force"; flags: S,12; threshold: type both, track
by_src, count 30, seconds 60; classtype: misc-activity; reference:url,www.rapid7.com/nexpose-faq-answer2.htm; reference:url,doc.emergingthreats.net/2001904;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Telnet; sid:2001904; rev:6;)

#These are intended to catch new worms and such scanning internally. Careful of falses.
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 23 (msg:"ET SCAN Behavioral Unusually fast outbound Telnet Connections, Potential Scan or Brute Force"; flags: S,12; threshold: type both,
track by_src, count 30, seconds 60; classtype: misc-activity; reference:url,www.rapid7.com/nexpose-faq-answer2.htm; reference:url,doc.emergingthreats.net/2008230;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Telnet; sid:2008230; rev:2;)

#Works for other proto's, may as well extend the idea
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 3389 (msg:"ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection"; flags: S,12; threshold: type both, track
by_src, count 20, seconds 360; classtype: misc-activity; reference:url,doc.emergingthreats.net/2001972; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_Term_Server; sid:2001972; rev:16;)

#Scanner using this UA, looking for many common vulns
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Toata Scanner User-Agent Detected"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Toata dragostea mea
pentru diavola"; offset:30; threshold: type limit, count 1, seconds 60, track by_src; classtype:attempted-recon; reference:url,isc.sans.org/diary.html?storyid=5599;
reference:url,doc.emergingthreats.net/2009159; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Toata_UA; sid:2009159; rev:5;)

#by Jack Pepper
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 8080 (msg:"ET SCAN Tomcat Auth Brute Force attempt (admin)"; flow:to_server,established; content:"Authorization|3a| Basic YWRtaW46";
threshold: type threshold, track by_src, count 30, seconds 30; classtype:web-application-attack; reference:url,doc.emergingthreats.net/2008453;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Tomcat_Brute; sid:2008453; rev:4;)

#by Jack Pepper
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 8080 (msg:"ET SCAN Tomcat Auth Brute Force attempt (tomcat)"; flow:to_server,established; content:"Authorization|3a| Basic dG9tY2F0";
threshold: type threshold, track by_src, count 30, seconds 30; classtype:web-application-attack; reference:url,doc.emergingthreats.net/2008454;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Tomcat_Brute; sid:2008454; rev:4;)

#by Jack Pepper
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 8080 (msg:"ET SCAN Tomcat Auth Brute Force attempt (manager)"; flow:to_server,established; content:"Authorization|3a| Basic bWFuYWdlcjp";
threshold: type threshold, track by_src, count 30, seconds 30; classtype:web-application-attack; reference:url,doc.emergingthreats.net/2008455;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Tomcat_Brute; sid:2008455; rev:4;)

#by Jack Pepper
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN Tomcat admin-admin login credentials"; flow:to_server,established; uricontent:"/manager/html"; nocase; content:"|0d
0a|Authorization|3a| Basic YWRtaW46YWRtaW4=|0d 0a|"; flowbits:set,ET.Tomcat.login.attempt; classtype:attempted-admin; reference:url,tomcat.apache.org;
reference:url,doc.emergingthreats.net/2009217; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Tomcat_Brute; sid:2009217; rev:6;)

#by Jack Pepper
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN Tomcat admin-blank login credentials"; flow:to_server,established; uricontent:"/manager/html"; nocase; content:"|0d
0a|Authorization|3a| Basic YWRtaW46|0d 0a|"; flowbits:set,ET.Tomcat.login.attempt; classtype:attempted-admin; reference:url,tomcat.apache.org;
reference:url,doc.emergingthreats.net/2009218; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Tomcat_Brute; sid:2009218; rev:5;)

#by Jack Pepper
#
alert tcp $HOME_NET $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET SCAN Tomcat Successful default credential login from external source"; flow:from_server,established;
flowbits:isset,ET.Tomcat.login.attempt; content:"HTTP/1."; depth:7; content:" 200 OK"; distance:1; within:10; classtype:successful-admin; reference:url,tomcat.apache.org;
reference:url,doc.emergingthreats.net/2009219; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Tomcat_Brute; sid:2009219; rev:2;)

#by Jack Pepper
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN Tomcat upload from external source"; flow:to_server,established; flowbits:isset,ET.Tomcat.login.attempt; content:"POST
"; nocase; depth:5; uricontent:"/manager/html/upload"; nocase; classtype:successful-admin; reference:url,tomcat.apache.org; reference:url,doc.emergingthreats.net/2009220;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Tomcat_Brute; sid:2009220; rev:3;)

#by evilghost
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN Tomcat Web Application Manager scanning"; flow:established,to_server; content:"GET "; depth:4; nocase;
uricontent:"/manager/html"; nocase; content:"|0d 0a|User-Agent|3a| Mozilla/3.0 (compatible|3b| Indy Library)|0d 0a|"; content:"|0d 0a|Authorization|3a| Basic"; classtype:attempted-
recon; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Tomcat_Brute; reference:url,doc.emergingthreats.net/2010019; sid:2010019; rev:6;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Suspicious User-Agent Containing SQL Inject/ion, Likely SQL Injection Scanner"; flow:established,to_server;
content:"|0d 0a|User-Agent|3A|"; content:"SQL"; nocase; within:200; content:"Inject"; nocase; distance:0; pcre:"/User-Agent\x3A[^\n]+sql[^\n]+inject/i"; classtype:attempted-recon;
reference:url,www.owasp.org/index.php/SQL_Injection; reference:url,doc.emergingthreats.net/2010087; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_UA;
sid:2010087; rev:3;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner"; flow:established,to_server; content:"|0d
0a|User|2D|Agent|3A|"; content:"web"; nocase; within:200; content:"scan"; nocase; distance:0; pcre:"/User-Agent\x3A[^\n]+web[^\n]+scan/i"; classtype:attempted-recon;
reference:url,doc.emergingthreats.net/2010088; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_UA; sid:2010088; rev:2;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Suspicious User-Agent Containing Security Scan/ner, Likely Scan"; flow:established,to_server; content:"|0d
0a|User|2D|Agent|3A|"; content:"security"; nocase; within:200; content:"scan"; nocase; distance:0; pcre:"/User-Agent\x3A[^\n]+security[^\n]+scan/i"; classtype:attempted-recon;
reference:url,doc.emergingthreats.net/2010089; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_UA; sid:2010089; rev:2;)

#by matt jonkman
#intended to catch internal hosts doing upnp requests that maybe shouldn't be
#and external hosts making internal requests.
#have seen some malware samples looking for upnp hosts
#
alert tcp $HOME_NET any -> $HOME_NET 2555 (msg:"ET SCAN Internal to Internal UPnP Request tcp port 2555"; flow:established,to_server; content:"GET "; depth:4; content:"/upnp/"; nocase;
pcre:"/\/upnp\/[a-z0-9]{8}-[a-z0-9]{4}-[a-z0-9]{4}-[a-z0-9]{16}\//i"; classtype:attempted-recon; reference:url,www.upnp-hacks.org/upnp.html;
reference:url,doc.emergingthreats.net/2008092; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_UPnP; sid:2008092; rev:3;)

#by matt jonkman
#intended to catch internal hosts doing upnp requests that maybe shouldn't be
#and external hosts making internal requests.
#have seen some malware samples looking for upnp hosts
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 2555 (msg:"ET SCAN External to Internal UPnP Request tcp port 2555"; flow:established,to_server; content:"GET "; depth:4; content:"/upnp/";
nocase; pcre:"/\/upnp\/[a-z0-9]{8}-[a-z0-9]{4}-[a-z0-9]{4}-[a-z0-9]{16}\//i"; classtype:attempted-recon; reference:url,www.upnp-hacks.org/upnp.html;
reference:url,doc.emergingthreats.net/2008093; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_UPnP; sid:2008093; rev:5;)

#by matt jonkman
#intended to catch internal hosts doing upnp requests that maybe shouldn't be
#and external hosts making internal requests.
```

```
#have seen some malware samples looking for upnp hosts
#
alert udp $EXTERNAL_NET any -> $HOME_NET 1900 (msg:"ET SCAN External to Internal UPnP Request udp port 1900"; content:"MSEARCH * HTTP/1.1"; depth:18; content:"MAN|3a| ssdp|3a|"; nocase;
distance:0; classtype:attempted-recon; reference:url,www.upnp-hacks.org/upnp.html; reference:url,doc.emergingthreats.net/2008094; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_UPnP; sid:2008094; rev:4;)

#by Matt Jonkman
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 5800:5820 (msg:"ET SCAN Potential VNC Scan 5800-5820"; flags:S,12; threshold: type threshold, track by_src, count 5, seconds 60;
classtype:attempted-recon; reference:url,doc.emergingthreats.net/2002910; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_VNC; sid:2002910; rev:4;)

#by Matt Jonkman
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 5900:5920 (msg:"ET SCAN Potential VNC Scan 5900-5920"; flags:S,12; threshold: type threshold, track by_src, count 5, seconds 60;
classtype:attempted-recon; reference:url,doc.emergingthreats.net/2002911; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_VNC; sid:2002911; rev:4;)

#by Kevin Ross
#
alert udp $EXTERNAL_NET any -> $HOME_NET 5060 (msg:"ET SCAN Smap VOIP Device Scan"; content:"<sip|3a|smap@"; offset:80; depth:40; classtype:attempted-recon;
reference:url,www.go2linux.org/smap-find-voip-enabled-devices; reference:url,doc.emergingthreats.net/2008526; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_VOIP_SMAP; sid:2008526; rev:5;)

#by Kevin Ross
#
alert udp $EXTERNAL_NET any -> $HOME_NET 5060 (msg:"ET SCAN Voiper Toolkit Torturer Scan"; content:"interesting-Method"; content:"sip|3a|1_unusual.URI"; content:"to-be!sure"; offset:20;
depth:60; classtype:attempted-recon; reference:url,sourceforge.net/projects/voiper; reference:url,doc.emergingthreats.net/2008568; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_Voiper; sid:2008568; rev:3;)

#by Kevin Ross
#
alert udp $EXTERNAL_NET any -> $HOME_NET 5060 (msg:"ET SCAN Voiper Fuzzing Scan"; content:"sip|3a|tester@"; content:"Via|3a| SIP/2.0"; offset:20; depth:60; threshold: type threshold,
track by_dst, count 5, seconds 15; classtype:attempted-recon; reference:url,sourceforge.net/projects/voiper; reference:url,doc.emergingthreats.net/2008577;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Voiper; sid:2008577; rev:3;)

#by Will Metcalf
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN w3af User Agent"; flow: established,to_server; content:"User-Agent|3a|"; depth:300; nocase; content:"w3af";
distance:0; within:100; pcre:"/User-Agent\:[^\n]+w3af\.sourceforge\.net/i"; classtype: attempted-recon; reference:url,w3af.sourceforge.net;
reference:url,doc.emergingthreats.net/2007757; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_W3AF; sid:2007757; rev:6;)

#will metcalf
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN w3af Scan In Progress ARGENTINA Req Method"; flow:to_server,established; content:"ARGENTINA "; depth:10;
classtype: attempted-recon; reference:url,w3af.sourceforge.net; reference:url,doc.emergingthreats.net/2011027; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_W3AF; sid:2011027; rev:3;)

#by Kevin Ross
#Put in Uricontent match and expanded user agent to be 0d 0a and 3a and incremented revision number.
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN WSFuzzer Web Application Fuzzing"; flow:to_server,established; uricontent:"/ServiceDefinition"; content:"|0d
0a|User-Agent|3A| Python-urllib/"; classtype:attempted-recon; reference:url,www.owasp.org/index.php/Category%3aOWASP_WSFuzzer_Project; reference:url,doc.emergingthreats.net/2008628;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_WSFuzzer; sid:2008628; rev:5;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Possible WafWoof Web Application Firewall Detection Scan"; flow:established,to_server; content:"GET "; depth:4;
uricontent:"/<invalid>hello.html"; classtype:attempted-recon; reference:url,code.google.com/p/waffit/; reference:url,doc.emergingthreats.net/2011720;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Wafwoof; sid:2011720; rev:2;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Wapiti Web Server Vulnerability Scan"; flow:to_server,established; content:"GET /"; depth:5; content:"?
http|3A|//www.google."; within:100; nocase; content:"|0d 0a|User-Agent|3A 20|Python-httplib2"; distance:0; classtype:attempted-recon; reference:url,wapiti.sourceforge.net/;
reference:url,doc.emergingthreats.net/2008417; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Wapiti; sid:2008417; rev:7;)

#by kevin ross
#
#alert tcp $HTTP_SERVERS $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET SCAN Unusually Fast 400 Error Messages (Bad Request), Possible Web Application Scan"; flow:from_server,established;
content:"HTTP/1.1 400"; depth:13; threshold: type threshold, track by_dst, count 30, seconds 60; classtype:attempted-recon; reference:url,www.w3.org/Protocols/rfc2616/rfc2616-
sec10.html; reference:url,support.microsoft.com/kb/247249; reference:url,doc.emergingthreats.net/2009884; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Web;
sid:2009884; rev:2;)

#by kevin ross
#
#alert tcp $HTTP_SERVERS $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET SCAN Unusually Fast 404 Error Messages (Page Not Found), Possible Web Application Scan/Directory Guessing Attack";
flow:from_server,established; content:"HTTP/1.1 404"; depth:13; threshold: type threshold, track by_dst, count 30, seconds 60; classtype:attempted-recon;
reference:url,www.w3.org/Protocols/rfc2616/rfc2616-sec10.html; reference:url,en.wikipedia.org/wiki/HTTP_404; reference:url,doc.emergingthreats.net/2009885;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Web; sid:2009885; rev:2;)

#by Axn Jxn
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN WebHack Control Center User-Agent Inbound (WHCC/)"; flow:to_server,established; content:"WHCC"; nocase; depth:300;
pcre:"/User-Agent\x3a[^\n]+WHCC/i"; classtype:trojan-activity; reference:url,www.governmentsecurity.org/forum/index.php?showtopic=5112&pid=28561&mode=threaded&start=;
reference:url,doc.emergingthreats.net/2003924; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_WebHack; sid:2003924; rev:8;)

#by markus manzke
#Proxy-Scanner - 2
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Open-Proxy ScannerBot (webcollage-UA) "; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
webcollage/1.135a"; nocase; classtype:bad-unknown; reference:url, stateofsecurity.com/?p=526; reference:url,www.botsvsbrowsers.com/details/214715/index.html;
reference:url,doc.emergingthreats.net/2010768; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Webcollage; sid:2010768; rev:4;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN WebShag Web Application Scan Detected"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| webshag";
classtype:attempted-recon; reference:url,www.scrt.ch/pages_en/outils.html; reference:url,doc.emergingthreats.net/2009158; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_Webshag; sid:2009158; rev:3;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN WhatWeb Web Application Fingerprint Scanner Default User-Agent Detected"; flow:established,to_server; content:"|0d
0a|User-Agent|3A| WhatWeb/"; classtype:attempted-recon; reference:url,www.morningstarsecurity.com/research/whatweb; reference:url,doc.emergingthreats.net/2010960;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_WhatWeb; sid:2010960; rev:2;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Wikto Scan"; flow:to_server,established; content:"GET "; depth:4; uricontent:"/.adSensePostNotThereNoNobook";
classtype:attempted-recon; reference:url,www.sensepost.com/research/wikto/WiktoDoc1-51.htm; reference:url,doc.emergingthreats.net/2008617; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_Wikto; sid:2008617; rev:4;)

#This is the improved sig I just posted but I have changed what is $HOME_NET in the ruleset to be $HTTP_SERVERS
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Wikto Backend Data Miner Scan"; flow:to_server,established; content:"GET "; depth:4;
uricontent:"/actSensePostNotThereNoNotive"; classtype:attempted-recon; reference:url,www.sensepost.com/research/wikto/WiktoDoc1-51.htm; reference:url,doc.emergingthreats.net/2008629;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Wikto; sid:2008629; rev:5;)

#by Kevin Ross
#
```

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN WITOOL SQL Injection Scan"; flow:to_server,established; uricontent:"union+select"; uricontent:"select+user";
content:"|0d 0a|User-Agent|3a| Mozilla/4.0 (compatible|3b| MSIE 6.0|3b| Windows NT 5.0|3b| MyIE2"; threshold: type threshold, track by_dst, count 30, seconds 30; classtype:attempted-
recon; reference:url,witool.sourceforge.net/; reference:url,doc.emergingthreats.net/2009833; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Witool; sid:2009833;
rev:3;)

#by Kevin Ross
#
alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET SCAN Port Unreachable Response to Xprobe2 OS Fingerprint Scan"; itype:3; dsize:>69; content:"securityfocus";
content:"securityfocus"; offset:50; distance:6; classtype:attempted-recon; reference:url,xprobe.sourceforge.net/; reference:url,doc.emergingthreats.net/2009298;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_Xprobe2; sid:2009298; rev:2;)

#by jack pepper
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN ZmEu exploit scanner"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| Made by ZmEu"; threshold: type
limit, track by_src, seconds 180, count 1; classtype:web-application-attack; reference:url,doc.emergingthreats.net/2010705; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/SCAN/SCAN_ZmEu; sid:2010715; rev:5;)

#by evilghost
#
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN ICMP @hello request, Likely Precursor to Scan"; itype:8; icode:0; content:"@hello ???"; classtype:misc-activity;
reference:url,doc.emergingthreats.net/2010641; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_hello; sid:2010641; rev:2;)

#by Kevin Ross
#catches 95% of fuzzes, remove threshold to catch 100% but may FP
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Possible jBroFuzz Fuzzer Detected"; flow:to_server,established; content:"|0d 0a|Host|3a| localhost"; content:"|0d
0a|User-Agent|3a| Mozilla/5.0 (Windows|3b| U|3b| Windows NT 5.1|3b| en-GB|3b| rv|3b|1.8.1.1) Gecko/20061204 Firefox/2.0.0.1"; depth:130; distance:0; threshold: type threshold, track
by_src, count 3, seconds 6; classtype:attempted-recon; reference:url,www.owasp.org/index.php/Category%3aOWASP_JBroFuzz; reference:url,doc.emergingthreats.net/2009476;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_jBroFuzz; sid:2009476; rev:5;)

#Matt Jonkman, From spyware listening post data
#
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|"; nocase;
content:"2Search"; within:150; pcre:"/User-Agent\:[^\n]+2Search/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003335; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_2search; sid:2003335; rev:8;)

#Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS 404Search Spyware User Agent"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| 404search";
classtype: trojan-activity; reference:url,doc.emergingthreats.net/2001852; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_404Search; sid:2001852;
rev:26;)

#Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Adload.Generic Spyware User-Agent (91castInstallKernel)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| 91cast"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003640; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_91cast; sid:2003640; rev:9;)

#Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Pigeon.AYX/AVKill Related User-Agent (CTTBasic)"; flow: established,to_server; content:"|0d 0a|User-Agent|3a|
CTT"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2009236; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_AVKill;
sid:2009236; rev:7;)

#Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Adwave.com Related Spyware User-Agent (STBHOGet)"; flow:to_server,established; content:"User-Agent|3a|
STBHOGet|0d 0a|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003500; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Adwave; sid:2003500; rev:7;)

#Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Alawar Toolbar Spyware User-Agent (Alawar Toolbar)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
Alawar Toolbar"; nocase; classtype:trojan-activity; reference:url,www.bleepingcomputer.com/uninstall/68/Alawar-Toolbar.html; reference:url,doc.emergingthreats.net/2003506;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Alawar; sid:2003506; rev:8;)

#New from Chris Taylor and the User agents project
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Alexa Search Toolbar User-Agent (Alexa Toolbar)"; flow: to_server,established; content:"|0d 0a|User-Agent|3a|
Alexa Toolbar|0d 0a|"; classtype:trojan-activity; reference:url,www.spywareguide.com/product_show.php?id=418; reference:url,doc.emergingthreats.net/2002166;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Alexa; sid:2002166; rev:13;)

#New from Chris Taylor and the User agents project
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Alexa Search Toolbar User-Agent 2 (Alexa Toolbar)"; flow: to_server,established; content:"|0d 0a|User-
Agent|3a|"; content:"Alexa Toolbar"; distance:0; within:200; pcre:"/User-Agent\:[^\n]+Alexa/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008085;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Alexa; sid:2008085; rev:6;)

#New from Chris Taylor and the User agents project
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Altnet PeerPoints Manager Traffic"; flow: established,to_server; content:"User-Agent|3a|"; nocase;
content:"Peer Points"; within:150; pcre:"/User-Agent\:[^\n]+Peer Points/i"; classtype: policy-violation; reference:url,doc.emergingthreats.net/2001640;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Altnet; sid:2001640; rev:20;)

#New from Chris Taylor and the User agents project
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS AntiVermins.com Fake Antispyware Package User Agent"; flow:to_server,established; content:"User-Agent|3a|";
nocase; content:"AntiVerminser"; within:150; pcre:"/User-Agent\:[^\n]+AntiVerminser/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003336;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Antivermin; sid:2003336; rev:7;)

#New from Chris Taylor and the User agents project
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Antivermins.com Spyware/Adware User-Agent (AntiVermeans)"; flow:to_server,established; content:"User-Agent|3a|
AntiVermeans"; nocase; classtype:trojan-activity; reference:url,www.bleepingcomputer.com/forums/topic69886.htm; reference:url,doc.emergingthreats.net/2003531;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Antivermin; sid:2003531; rev:6;)

#New from Chris Taylor and the User agents project
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Toplist.cz Related Spyware User-Agent (BWL Toplist)"; flow:to_server,established; content:"User-Agent|3a| BWL
Toplist"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003505; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_BWL;
sid:2003505; rev:6;)

#by evilghost
#
#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:"|0d 0a|User-
Agent|3a|"; nocase; content:"|5C|"; within:200; content:!"|5C|Citrix|5C|ICA Client|5C|"; nocase; pcre:"/User-Agent\:.*[^\x5c]\x5c[^\x5c\x3d\x2f\x3b\x28\x29]+/i"; classtype:bad-unknown;
reference:url,www.w3.org/Protocols/rfc2616/rfc2616-sec14.html; reference:url,mws.amazon.com/docs/devGuide/UserAgent.html; reference:url,doc.emergingthreats.net/2010721;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Backslash; sid:2010721; rev:5;)

#by evilghost
#
#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:"|0d 0a|User-
Agent|3a|"; nocase; content:"|5C|"; within:200; content:!"|5C|Citrix|5C|ICA Client|5C|"; nocase; pcre:"/User-Agent\:.*[^\x5c]\x5c[^\x5c\x3d\x2f\x3b\x28\x29]+/i"; classtype:bad-unknown;
reference:url,www.w3.org/Protocols/rfc2616/rfc2616-sec14.html; reference:url,mws.amazon.com/docs/devGuide/UserAgent.html; reference:url,doc.emergingthreats.net/2010722;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Backslash; sid:2010722; rev:5;)

#by evilghost
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Baidu.com Agent User-Agent (Desktop Web System)"; flow:to_server,established; content:"User-Agent|3a| Desktop
Web System"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003604; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Baidu; sid:2003604; rev:6;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Baidu.com Related Agent User-Agent (iexp)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| iexp";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003608; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Baidu;
sid:2003608; rev:7;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS TROJAN BankSnif/Nethelper User Agent"; flow:to_server,established; content:"User-Agent|3a|"; nocase;
content:"nethelper"; within:150; pcre:"/User-Agent\:[^\n]+nethelper/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2002877;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Banksnif; sid:2002877; rev:11;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Better Internet Spyware User Agent Activity (thnall)"; flow: to_server,established; content:"User-Agent|3a|";
nocase; content:"THNALL"; within:150; pcre:"/User-Agent\:[^\n]+THNALL[^\n]+\.EXE/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2002002;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_BetterInterenet; sid:2002002; rev:28;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Better Internet Spyware User Agent Activity (poller)"; flow: to_server,established; content:"User-Agent|3a|";
nocase; content:"Poller"; within:150; pcre:"/User-Agent\:[^\n]+Poller/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2002005;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_BetterInterenet; sid:2002005; rev:26;)

#by jamie blasco at alienvault
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Win32.OnLineGames User Agent Detected (BigFoot)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
BigFoot"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010678; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_BigFoot; sid:2010678; rev:3;)

#by Pedro Marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent BlueSky"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| BlueSky|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011084; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_BlueSky; sid:2011084;
rev:3;)

#by Pedro Marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Browseraid.com Agent"; flow: to_server,established; content:"User-Agent|3a|"; nocase; content:"Browser Adv";
within:100; pcre:"/User-Agent\:[^\n]+Browser Adv/i"; classtype: trojan-activity; reference:url,www.browseraid.com; reference:url,doc.emergingthreats.net/2001295;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Browseraid; sid:2001295; rev:20;)

#by Pedro Marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS CoolWebSearch Spyware User-Agent (iefeatsl)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
iefeatsl"; nocase; classtype:trojan-activity; reference:url,www.applicationsignatures.com/backend/index.php; reference:url,doc.emergingthreats.net/2003570;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_CWS; sid:2003570; rev:7;)

#by Pedro Marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS CoolWebSearch Spyware (Feat)"; flow: to_server,established; content:"|0d 0a|User-Agent|3a| Feat"; nocase;
classtype:trojan-activity; reference:url,www.spywareguide.com/product_show.php?id=599; reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=453075759;
reference:url,www.doxdesk.com/parasite/CoolWebSearch.html; reference:url,doc.emergingthreats.net/2002160; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_CWS; sid:2002160; rev:15;)

#from the spyware lp
#by matt jonkman
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET DELETED Casalemedia.com Related User Agent (0 0 ...)"; flow: established,to_server; content:"|0d 0a|User-Agent|3a|
0|3a|0|3a|"; pcre:"/\x0d\x0aUser-Agent\: 0\:0\:[^\n]{120}/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007647; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Casalemedia; sid:2007647; rev:8;)

#from the spyware lp
#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Casino Related Spyware User-Agent Detected (Viper 4.0)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| Mozilla/5.0 (compatible, Viper 4.0)|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008586; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Casino; sid:2008586; rev:5;)

#by jaime blasco of alienvault
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS chnsystem.com Spyware User-Agent (Update1.0)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
Update1.0"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010680; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Chnsystem;
sid:2010680; rev:3;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (ClickAdsByIE)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
ClickAdsByIE"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010220; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_ClickAdsbyIE; sid:2010220; rev:3;)

#Matt Jonkman form SpywareLP Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS clickspring.com Spyware Install User-Agent (CS Fingerprint Module)"; flow:to_server,established; content:"|0d
0a|User-Agent|3a| CS Fingerprint Module"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003425; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Clickspring; sid:2003425; rev:8;)

#Matt Jonkman form SpywareLP Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Surfaccuracy.com Spyware Install User-Agent (SF Installer)"; flow:to_server,established; content:"User-
Agent|3a|"; nocase; content:"SF Installer"; within:150; pcre:"/User-Agent\:[^\n]+SF Installer/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003428;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Clickspring; sid:2003428; rev:9;)

#Matt Jonkman form SpywareLP Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS xxxtoolbar.com Spyware Install User-Agent"; flow:to_server,established; content:"|0d 0a|User-Agent|3a 32 8b 86
85 86 8e 85 86 8c 0d 0a|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003429; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Clickspring; sid:2003429; rev:8;)

#Matt Jonkman form SpywareLP Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS CommonName.com Spyware/Adware User-Agent (CommonName Agent)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| CommonName"; nocase; classtype:trojan-activity; reference:url,www.pestpatrol.com/spywarecenter/pest.aspx?id=453078618; reference:url,doc.emergingthreats.net/2003532;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Commonname; sid:2003532; rev:7;)

#Matt Jonkman form SpywareLP Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Context Plus Spyware Activity (1)"; flow: established,to_server; content:"User-Agent|3a|"; nocase;
content:"Apropos"; within:150; pcre:"/User-Agent\:[^\n]+Apropos/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2001703; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_ContextPlus; sid:2001703; rev:30;)

#Matt Jonkman form SpywareLP Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Context Plus Spyware Activity (2)"; flow: established,to_server; content:"User-Agent|3a|"; nocase;
content:"Envolo"; within:150; pcre:"/User-Agent\:[^\n]+Envolo/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2001706; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_ContextPlus; sid:2001706; rev:31;)
```

```
#Matt Jonkman form SpywareLP Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Context Plus User Agent (PTS)"; flow: to_server,established; content:"|0d 0a|User-Agent|3a| PTS";
classtype:trojan-activity; reference:url,www.contextplus.net; reference:url,doc.emergingthreats.net/2002403; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_ContextPlus; sid:2002403; rev:10;)

#from spyware lp
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Cpushpop.com Spyware User Agent (CPUSH_UPDATER)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
CPUSH_"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006553; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Cpush;
sid:2006553; rev:7;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (CustomSpy)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| |28|CustomSpy|29
0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011271; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Customspy;
sid:2011271; rev:3;)

#jeremy at sudosecure
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Deepdo Toolbar User-Agent (FavUpdate)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| FavUpdate";
classtype:trojan-activity; reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=Deepdo%20Toolbar&threatid=129378; reference:url,doc.emergingthreats.net/2008457;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Deepdo; sid:2008457; rev:7;)

#Sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Deepdo.com Toolbar/Spyware User Agent (DeepdoUpdate)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| DeepdoUpdate/"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2006386; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Deepdo; sid:2006386; rev:7;)

#Sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS sgrunt Dialer User Agent (sgrunt)"; flow:to_server,established; content:"User-Agent|3a|"; nocase;
content:"sgrunt"; within:150; pcre:"/User-Agent\:[^\n]+sgrunt/i"; classtype:trojan-activity; reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=453096347;
reference:url,doc.emergingthreats.net/2003385; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Dialer; sid:2003385; rev:7;)

#Sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS dialno Dialer User Agent (dialno)"; flow:to_server,established; content:"User-Agent|3a|"; nocase;
content:"dialno"; within:150; pcre:"/User-Agent\:[^\n]+dialno/i"; threshold: type limit, count 5, seconds 60, track by_src; classtype:trojan-activity;
reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=453096347; reference:url,doc.emergingthreats.net/2003387; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Dialer; sid:2003387; rev:8;)

#Sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Dropspam.com Spyware Install User-Agent (DSInstall)"; flow:to_server,established; content:"User-Agent|3a|";
nocase; content:"DSInstall"; within:150; pcre:"/User-Agent\:[^\n]+DSInstall/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003439;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Dropspam; sid:2003439; rev:7;)

#Sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS EELoader User-Agent - Unknown (multiple) Malware Packages"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| EELoader"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003613; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_EELoader; sid:2003613; rev:8;)

#Sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE EZULA Spyware User Agent"; flow: established,to_server; content:"|0d 0a|User-Agent|3a| ezula"; classtype: trojan-
activity; reference:url,doc.emergingthreats.net/2001854; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_EZULA; sid:2001854; rev:22;)

#Sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Ezula Related Calling Home"; flow: to_server,established; content:"|0d 0a|User-Agent|3a| mez|0d 0a|"; nocase;
classtype: trojan-activity; reference:url,www.ezula.com; reference:url,www.spyany.com/program/article_spw_rm_eZuLa.html; reference:url,doc.emergingthreats.net/2000586;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_EZULA; sid:2000586; rev:30;)

#Sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Easy Search Bar Spyware User Agent"; flow: established,to_server; content:"|0d 0a|User-Agent|3a| ESB";
classtype: trojan-activity; reference:url,doc.emergingthreats.net/2001853; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_EasySearch; sid:2001853;
rev:23;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS ErrorNuker FakeAV User-Agent (ERRN2004 (Windows XP))"; flow:established,to_server; content:"GET "; depth:4;
content:"|0d 0a|User-Agent|3a| ERRN200"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009861; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_ErrorNuker; sid:2009861; rev:4;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Errorsafe.com Fake antispyware User Agent (ErrorSafe Updater)"; flow:to_server,established; content:"User-
Agent|3a|"; nocase; content:"ErrorSafe Updater"; within:150; pcre:"/User-Agent\:[^\n]+ErrorSafe Updater/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003346;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Errorsafe; sid:2003346; rev:7;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Evidencenuker.com Fake AV/Anti-Spyware User-Agent (EVNUKER)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| EVNUKER"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003567; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_EvidenceNuker; sid:2003569; rev:8;)

#by Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (FaceCooker)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| FaceCooker";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010717; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FaceCooker;
sid:2010717; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Internet-antivirus.com Related Fake AV User-Agent Detected (Update Internet Antivirus)";
flow:established,to_server; content:"|0d 0a|User-Agent|3a| Update Internet Antivirus"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008647;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV; sid:2008647; rev:6;)

#by Pedro Marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS WinFixer Trojan Related User-Agent Detected (ElectroSun NetInstaller)"; flow:established,to_server;
content:"|0d 0a|User-Agent|3a| ElectroSun "; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008608; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV; sid:2008608; rev:6;)

#by Pedro Marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS malwarewipeupdate.com Spyware User-Agent (MalwareWipe)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| MalwareWipe|0d 0a|"; nocase; classtype:trojan-activity; reference:url,www.malwarewipeupdate.com; reference:url,research.sunbelt-software.com/threatdisplay.aspx?
name=MalwareWipe&threatid=43086; reference:url,doc.emergingthreats.net/2003489; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV;
sid:2003489; rev:9;)

#by Pedro Marinho
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Virusblast.com Fake AV/Anti-Spyware User-Agent (ad-protect)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| ad-protect"; nocase; classtype:trojan-activity; reference:url,spywarewarrior.com/rogue_anti-spyware.htm; reference:url,www.virusblast.com;
reference:url,doc.emergingthreats.net/2003476; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV; sid:2003476; rev:7;)

#by Pedro Marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Terminexor.com Spyware User-Agent (DInstaller2)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
DInstaller"; nocase; classtype:trojan-activity; reference:url,www.terminexor.com; reference:url,netrn.net/spywareblog/archives/2004/12/23/more-rip-off-ware-terminexor;
reference:url,doc.emergingthreats.net/2003477; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV; sid:2003477; rev:7;)

#by Pedro Marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Errornuker.com Fake Anti-Spyware User-Agent (ERRORNUKER)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| ERRORNUKER"; nocase; classtype:trojan-activity; reference:url,www.spywarewarrior.com/rogue_anti-spyware.htm; reference:url,www.errornuker.com;
reference:url,doc.emergingthreats.net/2003478; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV; sid:2003478; rev:7;)

#by Pedro Marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Drivecleaner.com Spyware User-Agent (DriveCleaner Updater)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| DriveCleaner Updater"; nocase; classtype:trojan-activity; reference:url,www.drivecleaner.com; reference:url,research.sunbelt-software.com/threatdisplay.aspx?
name=DriveCleaner&threatid=44533; reference:url,doc.emergingthreats.net/2003486; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV;
sid:2003486; rev:7;)

#data by dxp and jpepper
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Systemdoctor.com/Antivir2008 related Fake Anti-Virus User-Agent (AntivirXP)"; flow:established,to_server;
content:"|0d 0a|User-Agent|3a| "; content:"Antivir"; pcre:"/User-Agent\:[^\n]+\;\sAntivir/"; threshold:type limit, count 1, seconds 60, track by_src; classtype:trojan-activity;
reference:url,www.wiki-security.com/wiki/Parasite/Antivirus2008; reference:url,doc.emergingthreats.net/2008549; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV; sid:2008549; rev:8;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Cleancop.co.kr Fake AV User-Agent (CleancopUpdate)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
Cleancop"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008484; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV;
sid:2008484; rev:5;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Searchtool.co.kr Fake Product User-Agent (searchtoolup)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| searchtool"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008485; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV; sid:2008485; rev:5;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS AntiSpywareMaster.com Fake AV User-Agent"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
AsmUpdater"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008294; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV;
sid:2008294; rev:5;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Dokterfix.com Fake AV User Agent (Magic NetInstaller)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| Magic NetInstaller|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007977; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV; sid:2007977; rev:5;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Easydownloadsoft.com Fake Anti-Virus User Agent (IM Downloader)"; flow:established,to_server; content:"|0d
0a|User-Agent|3a| IM Downloader|0d 0a|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008000; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV; sid:2008000; rev:5;)

#check.mycomclean.com, by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Mycomclean.com Spyware User Agent (HTTP_GET_COMM)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
HTTP_GET_COMM|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007881; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV; sid:2007881; rev:5;)

#check.mycomclean.com, by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Mycomclean.com Spyware User Agent (SHINI)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| SHINI|0d
0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007882; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV;
sid:2007882; rev:5;)

#check.mycomclean.com, by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Virusheat.com Fake Anti-Spyware User Agent (VirusHeat 4.3)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| VirusHeat"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007883; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV; sid:2007883; rev:5;)

#check.mycomclean.com, by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Antivirgear.com Fake Anti-Spyware User Agent (AntiVirGear)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| AntiVirGear"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2007697; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV; sid:2007697; rev:7;)

#by matt jonkman, from sandnet analysis re 200c2baf2b23e8db5f7145941548c69d
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Alfaantivirus.com Fake Anti-Virus User Agent (IM Download)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| IM Download|0d 0a|"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2007759; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV; sid:2007759; rev:5;)

#drpcclean.com by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Drpcclean.com Related Spyware User Agent (DrPCClean Transmit)"; flow:to_server,established; content:"|0d
0a|User-Agent|3a| DrPCClean"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007839; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV; sid:2007839; rev:5;)

#errclean.com related, by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Errclean.com Related Spyware User Agent (Locus NetInstaller)"; flow:to_server,established; content:"|0d
0a|User-Agent|3a| Locus"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007845; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV; sid:2007845; rev:6;)

#errclean.com related, by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Avsystemcare.com Fake AV User Agent (LocusSoftware, NetInstaller)"; flow:to_server,established; content:"|0d
0a|User-Agent|3a| LocusSoftware, NetInstaller"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008150; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV; sid:2008150; rev:5;)

#errclean.com related, by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS IEDefender (iedefender.com) Fake Antispyware User Agent (IEDefender 2.1)"; flow:established,to_server;
content:"|0d 0a|User-Agent|3a| IEDefender "; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2007690; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV; sid:2007690; rev:7;)

#errclean.com related, by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Winxpperformance.com Related Spyware User Agent (Microsoft Internet Browser)"; flow:established,to_server;
content:"|0d 0a|User-Agent|3a| Microsoft Internet Browser|0d 0a|"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2007660;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV; sid:2007660; rev:8;)
```

```
#errclean.com related, by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS VirusProtectPro Spyware User Agent (VirusProtectPro)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| VirusProtectPro"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2007617; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV; sid:2007617; rev:7;)

#errclean.com related, by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Ufixer.com Fake Antispyware User Agent (Ultimate Fixer)"; flow: established,to_server; content:"|0d 0a|User-Agent|3a| Ultimate Fixer"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007645; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV; sid:2007645; rev:8;)

#errclean.com related, by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Vikiller.com Fake Antispyware User Agent (vikiller ctrl...)"; flow: established,to_server; content:"|0d 0a|User-Agent|3a| vikiller ctrl"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007582; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FakeAV; sid:2007582; rev:7;)

#by Jaime Blasco at alienvault
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Fast Browser Search)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Fast Browser Search"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010676; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FastBrowserSearch; sid:2010676; rev:3;)

#by Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Forthgoer User Agent - Likely Hostile"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Forthgoer"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011247; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Forthgoer; sid:2011247; rev:3;)

#by Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Yourscreen.com Spyware User Agent (FreezeInet)"; flow:to_server,established; content:"User-Agent|3a|"; nocase; content:"FreezeInet"; within:150; pcre:"/User-Agent\:[^\n]+FreezeInet/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003355; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Freeze; sid:2003355; rev:7;)

#by Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Freeze.com Spyware User-Agent (YourScreen123)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| YourScreen"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003405; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Freeze; sid:2003405; rev:8;)

#by Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Fun Web Products Spyware User Agent (3)"; flow: established,to_server; content:"MyWay"; depth:300; pcre:"/User-Agent\x3a[^\n]+MyWay/i"; threshold:type limit, count 1, seconds 360, track by_src; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2001864; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FunWeb; sid:2001864; rev:6;)

#by Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Fun Web Products Spyware User Agent (1)"; flow: established,to_server; content:"User-Agent|3a|"; nocase; content:"FunWebProducts"; within:150; pcre:"/User-Agent\:[^\n]+FunWebProducts/i"; classtype: trojan-activity; threshold: type limit, count 1, seconds 360, track by_src; reference:url,doc.emergingthreats.net/2001855; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_FunWeb; sid:2001855; rev:22;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (GM Login)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| GM Login|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011273; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_GM; sid:2011273; rev:3;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Grandstreet Interactive Spyware User Agent Activity (1)"; flow: to_server,established; content:"|0d 0a|User-Agent|3a| IEP"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2002021; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_GSI; sid:2002021; rev:25;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Gamehouse.com User Agent (GAMEHOUSE.NET.URL)"; flow:to_server,established; content:"User-Agent|3a|"; nocase; content:"GAMEHOUSE"; within:150; pcre:"/User-Agent\:[^\n]+GAMEHOUSE/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003347; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Gamehouse; sid:2003347; rev:7;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Gamehouse.com Related Spyware User-Agent (Sprout Game)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Sprout Game|0d 0a|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003498; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Gamehouse; sid:2003498; rev:7;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Adsincontext.com Related Spyware User-Agent (Connector v1.2)"; flow: established; content:"|0d 0a|User-Agent|3a| Connector v"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008372; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_GeneralAdware; sid:2008372; rev:8;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Ask.com Toolbar/Spyware User Agent"; flow:established,to_server; content:"User-Agent|3a|"; nocase; content:"AskPBar"; within:150; pcre:"/User-Agent\:[^\n]+AskPBar/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2006381; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_GeneralAdware; sid:2006381; rev:7;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS AskSearch Spyware User-Agent (AskSearchAssistant)"; flow:to_server,established; content:"User-Agent|3a| "; nocase; content:"AskSearch"; distance:0; within:150; pcre:"/User-Agent\:[^\n]+AskSearch/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003493; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_GeneralAdware; sid:2003493; rev:7;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS AskSearch Toolbar Spyware User-Agent (AskBar)"; flow:to_server,established; content:"User-Agent|3a| "; nocase; content:"AskBar"; within:150; pcre:"/User-Agent\:[^\n]+AskBar/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003496; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_GeneralAdware; sid:2003496; rev:7;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS AskSearch Toolbar Spyware User-Agent (AskTBar)"; flow:to_server,established; content:"User-Agent|3a| "; nocase; content:"AskTBar"; within:150; pcre:"/User-Agent\:[^\n]+AskTBar/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003494; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_GeneralAdware; sid:2003494; rev:7;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Bestoffersnetwork.com Related Spyware User-Agent (TBONAS)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| TBONAS|0d 0a|"; nocase; classtype:trojan-activity; reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=BestOffersNetworks&threatid=43670; reference:url,doc.emergingthreats.net/2003501; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_GeneralAdware; sid:2003501; rev:7;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS CoolStreaming Toolbar (Conduit related) User-Agent (Coolstreaming Tool-Bar)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Coolstreaming"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003652; reference:url,www.emergingthreats.net/cgi-
```

```
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_GeneralAdware; sid:2003652; rev:7;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS debelizombi.com (Rizo) related Spyware User-Agent (mc_v1.2.6)"; flow:to_server,established; content:"|0d
0a|User-Agent|3a| mc_v1"; nocase; classtype:trojan-activity; reference:url,www.f-secure.com/v-descs/rizo.shtml; reference:url,doc.emergingthreats.net/2003656;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_GeneralAdware; sid:2003656; rev:7;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Debelizombi.com Spyware User Agent (blahrx)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
blahrx"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006778; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_GeneralAdware;
sid:2006778; rev:7;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Effectivebrands.com Spyware User-Agent (atsu)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
atsu|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006370; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_GeneralAdware; sid:2006370; rev:7;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Effectivebrands.com Spyware User-Agent (GTBank)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
GTBank"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003654; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_GeneralAdware; sid:2003654; rev:7;)

#by pedro marinho
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET DELETED HSN.com Toolbar Spyware User-Agent (HSN)"; flow:to_server,established; content:"User-Agent|3a| "; nocase;
content:"HSN"; within:150; pcre:"/User-Agent\:[^\n]+HSN/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003495; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_GeneralAdware; sid:2003495; rev:7;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS klm123.com Spyware User Agent"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| {"; nocase;
pcre:"/User-Agent\: \{[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}\}/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2007616;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_GeneralAdware; sid:2007616; rev:7;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Mirage.ru Related Spyware User Agent (szNotifyIdent)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| szNotifyIdent"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006782; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_GeneralAdware; sid:2006782; rev:7;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Popads123.com Related Spyware User Agent (LmaokaazLdr)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| LmaokaazLdr"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2007694; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_GeneralAdware; sid:2007694; rev:7;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Trafficadvance.net Spyware User-Agent (Internet 1.0)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| Internet 1."; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003655; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_GeneralAdware; sid:2003655; rev:7;)

#by pedro marinho
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET DELETED Unidentified Spyware User Agent (0 0 + 128 chars)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
0|3a|0|3a|"; nocase; pcre:"/User-Agent\: 0\:0\:[^\x0a|\x0d]{128}/"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2007615; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_GeneralAdware; sid:2007615; rev:7;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Zredirector.com Related Spyware User Agent (BndDriveLoader)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| BndDriveLoader"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2007693; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_GeneralAdware; sid:2007693; rev:7;)

#by Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Trojan.Win32.InternetAntivirus User Agent Detected (General Antivirus)"; flow:to_server,established;
content:"|0d 0a|User-Agent|3a| General Antivirus"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010679; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_GeneralAntivrus_FakeAV; sid:2010679; rev:3;)

#by Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS UbrenQuatroRusDldr Downloader User Agent (UbrenQuatroRusDldr 096044)"; flow:established,to_server; content:"|0d
0a|User-Agent|3a| UbrenQuatroRusDldr"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008202; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_General_Downloaders; sid:2008202; rev:5;)

#by Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS BndVeano4GetDownldr Downloader User Agent (BndVeano4GetDownldr)"; flow:established,to_server; content:"|0d
0a|User-Agent|3a| BndVeano4GetDownldr"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008203; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_General_Downloaders; sid:2008203; rev:5;)

#by Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Geopia.com Fake Anti-Spyware/AV User Agent (fs3update)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| fs3update|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007935; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Geopia; sid:2007935; rev:5;)

#by Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Geopia.com Fake Anti-Spyware/AV User Agent (fian3manager)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| fian3manager|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007938; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Geopia; sid:2007938; rev:5;)

#by Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Gootkit hldr)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Gootkit";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010718; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_GootKit;
sid:2010718; rev:3;)

#by Darren Spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (Launcher)"; flow: to_server,established; content:"|0d0a|User-Agent|3a| Launcher(";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010645; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Gozi;
sid:2010645; rev:3;)

#by Darren Spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Qcbar/Adultlinks Spyware User-Agent (IBSBand)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
IBSBand-"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006362; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_IBS;
sid:2006362; rev:7;)

#by Darren Spruell
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS IE Toolbar User-Agent (IEToolbar)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| IEToolbar";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009766; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_IEToolbar; sid:2009766;
rev:6;)

#from the sandnet
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS iebar Spyware User Agent (iebar)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|"; nocase;
content:"|3b 20|iebar"; within:70; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2007583; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_IEToolbar; sid:2007583; rev:8;)

#from the sandnet
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS ISearchTech.com XXXPornToolbar Activity (MyApp)"; flow: to_server,established; content:"User-Agent|3a|";
nocase; content:"MyApp"; within:150; pcre:"/User-Agent\:[^\n]+MyApp/i"; classtype: trojan-activity; reference:url,www.isearchtech.com; reference:url,doc.emergingthreats.net/2001492;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_ISearch; sid:2001492; rev:31;)

#from the sandnet
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS ISearchTech.com XXXPornToolbar Activity (IST)"; flow: to_server,established; content:"User-Agent|3a|"; nocase;
content:" IST"; within:150; pcre:"/User-Agent\:[^\n]+IST/"; classtype: trojan-activity; reference:url,www.isearchtech.com; reference:url,doc.emergingthreats.net/2001493;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_ISearch; sid:2001493; rev:32;)

#from the sandnet
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS YourSiteBar Activity"; flow: to_server,established; content:"|0d 0a|User-Agent|3a| istsvc|0d 0a|"; nocase;
classtype: trojan-activity; reference:url,www.ysbweb.com; reference:url,doc.emergingthreats.net/2001699; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_ISearch; sid:2001699; rev:259;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (InTeRNeT)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| |5f|InTeRNeT";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011127; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_InTeRNeT; sid:2011127;
rev:6;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (InfoBot) GET"; flow:to_server,established; content:"GET "; nocase; depth:4;
uricontent:"/infobot/index.php?uid="; nocase; content:"|0d 0a|User-Agent|3a| InfoBot"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011276;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Infobot; sid:2011276; rev:4;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Infobox3 Spyware User-Agent"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| InfoBox";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010934; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Infobox; sid:2010934;
rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Movies etc User Agent (IOInstall)"; flow: to_server,established; content:"|0d 0a|User-Agent|3a| IOInstall";
nocase; classtype:trojan-activity; reference:url,www.movies-etc.com; reference:url,doc.emergingthreats.net/2002404; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_InternetOptimizer; sid:2002404; rev:9;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Internet Optimizer User Agent (ROGUE)"; flow: to_server,established; content:"|0d 0a|User-Agent|3a| ROGUE";
nocase; classtype:trojan-activity; reference:url,www.internet-optimizer.com; reference:url,doc.emergingthreats.net/2002405; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_InternetOptimizer; sid:2002405; rev:9;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Internet Optimizer Activity"; flow: to_server,established; content:"User-Agent|3a|"; nocase;
content:"IOKernel"; within:150; pcre:"/User-Agent\:[^\n]+IOKernel/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2001498;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_InternetOptimizer; sid:2001498; rev:27;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Internet-optimizer.com Related Spyware User-Agent (SexTrackerWSI)"; flow:to_server,established; content:"|0d
0a|User-Agent|3a| SexTrackerWSI"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003627; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_InternetOptimizer; sid:2003627; rev:7;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Win32/InternetAntivirus User Agent Detected (Internet Antivirus Pro)"; flow:to_server,established; content:"|0d
0a|User-Agent|3a| Internet Antivirus"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010218; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Internet_Antivirus_Pro; sid:2010218; rev:3;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 3531 (msg:"ET USER_AGENTS JoltID Agent New Code Download"; flow: established; content:"User-Agent|3a|"; nocase; content:"PeerEnabler";
within:150; pcre:"/User-Agent\:[^\n]+PeerEnabler/i"; classtype: trojan-activity; reference:url,www.joltid.com; reference:url,forum.treweeke.com/loficversion/index.php/t597.html;
reference:url,doc.emergingthreats.net/2001652; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_JoltID; sid:2001652; rev:31;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS dns-look-up.com Spyware User-Agent (KRSystem)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
KRSystem"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003625; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KRSystem; sid:2003625; rev:7;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS No-ad.co.kr Fake AV Related User-Agent (U2Clean)"; flow: established,to_server; content:"|0d 0a|User-Agent|3a|
U2Clean"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2009289; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV;
sid:2009289; rev:4;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Fake AV User Agent av1-site.info Related (AV1)"; flow: established,to_server; content:"|0d 0a|User-Agent|3a|
AV1"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2009223; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV;
sid:2009223; rev:5;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Viruskill.co.kr Fake AV User-Agent Detected (virus_kill)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| virus_kill"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009150; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV; sid:2009150; rev:4;)

#by martin Holste
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS N1 Fake AV User-Agent Detected (N1)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| N1|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009157; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV;
sid:2009157; rev:4;)

#by martin Holste
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS ezday.co.kr Related Spyware User-Agent Detected (Ezshop)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| Ezshop"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008594; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV; sid:2008594; rev:5;)
```

```
#from the sandnet, by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Viruscheck.co.kr Fake Antispyware User Agent (viruscheck ctrl...)"; flow: established,to_server; content:"User-
Agent|3a| viruscheck"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007643; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV; sid:2007643; rev:7;)

#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Mycashbank.co.kr Spyware User Agent (pint_agency)"; flow:established,to_server; content:"User-Agent|3a|
pint_agency"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006413; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV; sid:2006413; rev:6;)

#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Platinumreward.co.kr Spyware User Agent (WT_GET_COMM)"; flow:established,to_server; content:"User-Agent|3a|
WT_GET_COMM"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006422; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV; sid:2006422; rev:8;)

#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Vaccineprogram.co.kr Related Spyware User Agent (Museon)"; flow:established,to_server; content:"User-Agent|3a|
Museon"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006418; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV;
sid:2006418; rev:6;)

#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Vaccineprogram.co.kr Related Spyware User Agent (anycleaner)"; flow:established,to_server; content:"User-
Agent|3a| anycleaner"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006419; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV; sid:2006419; rev:6;)

#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Vaccineprogram.co.kr Related Spyware User Agent (pcsafe)"; flow:established,to_server; content:"User-Agent|3a|
pcsafe"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006420; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV;
sid:2006420; rev:6;)

#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Doctorvaccine.co.kr Related Spyware User Agent (DoctorVaccine)"; flow:established,to_server; content:"User-
Agent|3a| DoctorVaccine"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006421; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV; sid:2006421; rev:6;)

#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Doctorvaccine.co.kr Related Spyware User Agent (ers)"; flow:established,to_server; content:"User-Agent|3a|
ers|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007809; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV; sid:2007809; rev:5;)

#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Doctorpro.co.kr Related Spyware User Agent (doctorpro1)"; flow:established,to_server; content:"User-Agent|3a|
doctorpro"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006423; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV;
sid:2006423; rev:6;)

#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Karine.co.kr Related Spyware User Agent (chk Profile)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| chk Profile|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006429; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV; sid:2006429; rev:7;)

#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Karine.co.kr Related Spyware User Agent (Access down)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| Access down|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006430; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV; sid:2006430; rev:7;)

#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Pcclear.co.kr/Pcclear.com Fake AV User-Agent (PCClearPlus)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| PCClear"; classtype:trojan-activity; reference:url,www.pcclear.com; reference:url,www.pcclear.co.kr; reference:url,doc.emergingthreats.net/2008198;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV; sid:2008198; rev:5;)

#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS vaccine-program.co.kr Related Spyware User Agent (vaccine)"; flow:established,to_server; content:"User-
Agent|3a| vaccine"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008200; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV; sid:2008200; rev:5;)

#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS yeps.co.kr Related User Agent (ISecu)"; flow:established,to_server; content:"User-Agent|3a| ISecu";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008204; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV;
sid:2008204; rev:5;)

#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS yeps.co.kr Related User Agent (ISUpd)"; flow:established,to_server; content:"User-Agent|3a| ISUpd";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008205; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV;
sid:2008205; rev:5;)

#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Nguide.co.kr Fake Security Tool User Agent (nguideup)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| nguideup|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007947; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV; sid:2007947; rev:5;)

#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Msconfig.co.kr Related User Agent (BACKMAN)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
BACKMAN|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007958; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV; sid:2007958; rev:5;)

#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Msconfig.co.kr Related User Agent (GLOBALx)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
GLOBAL"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007959; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV;
sid:2007959; rev:5;)

#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Kpang.com Spyware User Agent (auctionplusup)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
auctionplusup|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007900; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV; sid:2007900; rev:5;)

#by victor julien
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Searchspy.co.kr Spyware User Agent (HTTPGETDATA)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
HTTPGETDATA|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007908; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV; sid:2007908; rev:5;)
```

```
#by victor julien
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Searchspy.co.kr Spyware User Agent (HTTPFILEDOWN)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
HTTPFILEDOWN|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007909; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV; sid:2007909; rev:5;)

#by victor julien
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Searchspy.co.kr Spyware User Agent (HTTP_FILEDOWN)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
HTTP_FILEDOWN|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007910; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV; sid:2007910; rev:5;)

#by victor julien
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Donkeyhote.co.kr Spyware User Agent (UDonkey)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
UDonkey|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007927; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV; sid:2007927; rev:5;)

#by victor julien
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Gcashback.co.kr Spyware User Agent (InvokeAd)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
InvokeAd|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007928; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_KoreanFakeAV; sid:2007928; rev:5;)

#by Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Live Enterprise Suite)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Live
Enterprise Suite"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010727; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_LiveAntivurusSuite; sid:2010727; rev:3;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS NewWeb User Agent (Lobo Lunar)"; flow: established,to_server; content:"|0d 0a|User-Agent|3a| Lobo Lunar";
classtype: trojan-activity; reference:url,doc.emergingthreats.net/2009222; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Lobo; sid:2009222;
rev:5;)

#by jaime blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (MxAgent)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| MxAgent"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011125; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_MXAgent; sid:2011125;
rev:3;)

#by jaime blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS MalwareWiped.com Spyware User-Agent (MalwareWiped)"; flow:to_server,established; content:"User-Agent|3a|
MalwareWiped"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003582; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Malwarewiped; sid:2003582; rev:7;)

#by bgallia
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Adwave/MarketScore User Agent (WTA)"; flow: to_server,established; content:"|0d 0a|User-Agent|3a| WTA_";
classtype:trojan-activity; reference:url,www.adwave.com/our_mission.aspx; reference:url,www.marketscore.com; reference:url,doc.emergingthreats.net/2002394;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Marketscore; sid:2002394; rev:10;)

#by bgallia
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS MarketScore.com Spyware User Configuration and Setup Access"; flow: to_server,established; content:"User-
Agent|3a| OSSProxy"; classtype: policy-violation; reference:url,www.marketscore.com; reference:url,www.spysweeper.com/remove-marketscore.html;
reference:url,doc.emergingthreats.net/2001562; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Marketscore; sid:2001562; rev:28;)

#by Pedro Marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent Maxthon"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Mozilla/4.0
(compatible|3b| MSIE 6.0|3b| Windows NT 5.1|3b| SV1|3b| Maxthon)"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011118; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Maxthon; sid:2011118; rev:2;)

#by Pedro Marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Megaupload Spyware User Agent"; flow:to_server,established; content:"User-Agent|3a| Megaupload|0d 0a|";
classtype:trojan-activity; reference:url,www.budsinc.com; reference:url,doc.emergingthreats.net/2003224; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Megaupload; sid:2003224; rev:7;)

#by Pedro Marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS TROJAN Metafisher/Goldun z User Agent"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| z|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2002874; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Metafisher; sid:2002874;
rev:10;)

#Matt Jonkman. Found being used by a goldun variant
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (MSIE XPSP2)"; flow:to_server,established; content:"User-Agent|3a|"; nocase;
content:"MSIEXPSP2"; within:150; pcre:"/User-Agent\:[^\n]+MSIE XPSP2/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003200;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Metafisher; sid:2003200; rev:7;)

#by: Jeremy Conway at sudosecure.net
#ref: 8082ad1a9be4fb87312e2852c1647dd9
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS RubyFortune Spyware Capabilities User-Agent (Microgaming Install Program) - GET"; flow:established,to_server;
content:"GET "; depth:4; content:"|0d 0a|User-Agent|3a| Microgaming Install Program|0d 0a|"; nocase; within:100; classtype:trojan-activity;
reference:url,vil.nai.com/vil/content/v_151034.htm; reference:url,www.emsisoft.com/en/malware/?Adware.Win32.Ruby+Fortune+Casino+3.2.0.25;
reference:url,www.threatexpert.com/reports.aspx?find=mgsmup.com; reference:url,doc.emergingthreats.net/2009783; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Microgaming; sid:2009783; rev:5;)

#by: Jeremy Conway at sudosecure.net
#ref: 8082ad1a9be4fb87312e2852c1647dd9
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Mirar Bar Spyware User-Agent (Mbar)"; flow:to_server,established; content:"User-Agent|3a| Mbar"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003928; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Mirar; sid:2003928;
rev:6;)

#by: Jeremy Conway at sudosecure.net
#ref: 8082ad1a9be4fb87312e2852c1647dd9
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Mirar Bar Spyware User-Agent (Mirar_Toolbar)"; flow:to_server,established; content:"User-Agent|3a|
Mirar_Toolbar"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003929; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Mirar; sid:2003929; rev:6;)

#by: Jeremy Conway at sudosecure.net
#ref: 8082ad1a9be4fb87312e2852c1647dd9
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Mirar Spyware User-Agent (Mirar_KeywordContent)"; flow:to_server,established; content:"User-Agent|3a|
Mirar_KeywordContent|0d 0a|"; nocase; classtype:trojan-activity; reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=453078818; reference:url,doc.emergingthreats.net/2003490;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Mirar; sid:2003490; rev:6;)

#by: Jeremy Conway at sudosecure.net
#ref: 8082ad1a9be4fb87312e2852c1647dd9
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Miva User Agent (TPSystem)"; flow: to_server,established; content:"|0d 0a|User-Agent|3a| TPSystem"; nocase;
classtype:trojan-activity; reference:url,www.miva.com; reference:url,www.findwhat.com; reference:url,doc.emergingthreats.net/2002395; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Miva; sid:2002395; rev:11;)

#by: Jeremy Conway at sudosecure.net
#ref: 8082ad1a9be4fb87312e2852c1647dd9
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Miva Spyware User Agent (Travel Update)"; flow: to_server,established; content:"|0d 0a|User-Agent|3a| Travel
Update|0d 0a|"; classtype:trojan-activity; reference:url,www.miva.com; reference:url,doc.emergingthreats.net/2002396; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Miva; sid:2002396; rev:10;)

#by: Jeremy Conway at sudosecure.net
#ref: 8082ad1a9be4fb87312e2852c1647dd9
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Morpheus Spyware Install User-Agent (SmartInstaller)"; flow:to_server,established; content:"User-Agent|3a|";
nocase; content:"SmartInstaller"; within:150; pcre:"/User-Agent\:[^\n]+SmartInstaller/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003398;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Morpheus; sid:2003398; rev:7;)

#by: Jeremy Conway at sudosecure.net
#ref: 8082ad1a9be4fb87312e2852c1647dd9
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Msgplus.net Spyware/Adware User-Agent (MsgPlus3)"; flow:to_server,established; content:"User-Agent|3a|
MsgPlus3"; nocase; classtype:trojan-activity; reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=Messenger%20Plus!&threatid=14931;
reference:url,doc.emergingthreats.net/2003529; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_MsgPlus; sid:2003529; rev:6;)

#by: Jeremy Conway at sudosecure.net
#ref: 8082ad1a9be4fb87312e2852c1647dd9
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS MyWaySearch Products Spyware User Agent"; flow: established,to_server; content:"User-Agent|3a|"; nocase;
content:"MyWay"; within:150; pcre:"/User-Agent\:[^\n]+MyWay/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2002079; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_MySearch; sid:2002079; rev:15;)

#by: Jeremy Conway at sudosecure.net
#ref: 8082ad1a9be4fb87312e2852c1647dd9
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS MySearch Products Spyware User Agent"; flow: established,to_server; content:"User-Agent|3a|"; nocase;
content:"MySearch"; within:150; pcre:"/User-Agent\:[^\n]+MySearch/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2002080;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_MySearch; sid:2002080; rev:15;)

#by: Jeremy Conway at sudosecure.net
#ref: 8082ad1a9be4fb87312e2852c1647dd9
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Enhance My Search Spyware Activity"; flow: established,to_server; content:"User-Agent|3a|"; nocase;
content:"HelperH"; within:100; pcre:"/User-Agent\:[^\n]+HelperH/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2001746; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_MySearch; sid:2001746; rev:31;)

#by: Jeremy Conway at sudosecure.net
#ref: 8082ad1a9be4fb87312e2852c1647dd9
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Mysearch.com/Morpheus Bar Spyware User-Agent"; flow:to_server,established; content:"User-Agent|3a|"; nocase;
content:"Morpheus"; within:150; pcre:"/User-Agent\:[^\n]+Morpheus/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003396;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_MySearch; sid:2003396; rev:7;)

#by: Jeremy Conway at sudosecure.net
#ref: 8082ad1a9be4fb87312e2852c1647dd9
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS searchenginebar.com Spyware User-Agent (RX Bar)"; flow:to_server,established; content:"User-Agent|3a| RX Bar";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003407; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_MySearch;
sid:2003407; rev:7;)

#by Shirkdog
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Mysearch.com Spyware User-Agent (iMeshBar)"; flow:to_server,established; content:"User-Agent|3a|"; nocase;
content:"iMeshBar"; within:150; pcre:"/User-Agent\:[^\n]+iMeshBar/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003406;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_MySearch; sid:2003406; rev:7;)

#by jaime blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Spyware google-analitid181.com related user agent (My Session)"; flow:to_server,established; content:"|0d
0a|User-Agent|3a| My Session"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010677; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_MySession; sid:2010677; rev:3;)

#by jaime blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS MyWebSearch Spyware User Agent"; flow: established,to_server; content:"User-Agent|3a|"; nocase;
content:"MyWebSearch"; within:150; pcre:"/User-Agent\:[^\n]+MyWebSearch/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2001865;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_MyWeb; sid:2001865; rev:22;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS TROJAN Nanspy User-Agent (XXX)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| XXX";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2010157; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Nanspy;
sid:2010157; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS NavExcel Spyware User-Agent (NavHelper)"; flow:to_server,established; content:"User-Agent|3a| NavHelper";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2005321; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Navhelper;
sid:2005321; rev:6;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS NewWeb/Sudui.com Spyware User Agent (B Register)"; flow:established,to_server; content:"User-Agent|3a| B
Register"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2007597; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_NewWeb; sid:2007597; rev:6;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS NewWeb/Sudui.com Spyware User Agent (updatesodui)"; flow:established,to_server; content:"User-Agent|3a|
updatesodui"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2007598; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_NewWeb; sid:2007598; rev:6;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS NewWeb/Sudui.com Spyware User Agent (aaaabbb)"; flow:established,to_server; content:"User-Agent|3a| aaaabbb";
nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2007599; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_NewWeb;
sid:2007599; rev:6;)

#by Shirkdog, from spyware lp hits
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Oemji Spyware User-Agent (Oemji)"; flow:to_server,established; content:"User-Agent|3a|"; nocase;
content:"Oemji"; within:150; pcre:"/User-Agent\:[^\n]+Oemji/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003468; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Oemji; sid:2003468; rev:7;)

#by m starkey
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS OneStep Adware related User Agent (x)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| x|0d 0a|";
nocase; classtype:trojan-activity; reference:url,www.symantec.com/security_response/writeup.jsp?docid=2008-112613-5052-99&tabid=2; reference:url,doc.emergingthreats.net/2009987;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Onestep; sid:2009987; rev:5;)
```

```
#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent Recuva OpenPage - likely trojan dropper"; flow:to_server,established; content:"|0d
0a|User-Agent|3a| OpenPage"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011101; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_OpenPage; sid:2011101; rev:4;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Personalweb Spyware User-Agent (PWMI/1.0)"; flow:to_server,established; content:"User-Agent|3a| PWMI/"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003926; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_PWMI; sid:2003926;
rev:6;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Pivim Multibar User-Agent (Pivim Multibar)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| Pivim";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009765; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Pivim; sid:2009765;
rev:6;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Popupblockade.com Spyware Related User-Agent (PopupBlockade/1.63.0.2/Reg)"; flow:established,to_server;
content:"|0d 0a|User-Agent|3a| PopupBlockade"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008894; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_PopupBlockade; sid:2008894; rev:5;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Privacyprotector Related Spyware User-Agent (Ssol NetInstaller)"; flow:to_server,established; content:"User-
Agent|3a| Ssol NetInstaller"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008040; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_PrivacyProtector; sid:2008040; rev:5;)

#from castlecops research
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Adload.Generic Spyware User-Agent (ProxyDown)"; flow:to_server,established; content:"User-Agent|3a| ProxyDown";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003639; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Proxydown;
sid:2003639; rev:6;)

#from sandnet analysis
#
#disabled for dupes
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS QQHelper related Spyware User-Agent (H)"; flow:to_server,established; content:"User-Agent|3a| H|0d 0a|";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003749; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_QQ; sid:2003749;
rev:7;)

#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS qq.com related Spyware User-Agent (QQGame)"; flow:to_server,established; content:"User-Agent|3a| QQGame";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003658; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_QQ; sid:2003658;
rev:6;)

#by: Jeremy Conway at sudosecure.net
#ref: 95084b2cd0b845e26fd177856d6e6319
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS QVOD Related Spyware/Malware User-Agent (Qvod)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
Qvod"; nocase; classtype:trojan-activity; reference:url,www.siteadvisor.com/sites/update.qvod.com; reference:url,www.threatexpert.com/reports.aspx?find=update.qvod.com;
reference:url,doc.emergingthreats.net/2009785; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_QVOD; sid:2009785; rev:6;)

#by: Jeremy Conway at sudosecure.net
#ref: 95084b2cd0b845e26fd177856d6e6319
#
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:"|0d 0a|User-Agent|3a| RFRudokop "; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008046; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_RF; sid:2008046; rev:4;)

#by Eoin Miller
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS FakeAV Windows Protection Suite/ReleaseXP.exe User-Agent (Releasexp)"; flow:established,to_server; content:"|0d
0a|User-Agent|3a| Releasexp|0d 0a|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009796; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_ReleaseXP; sid:2009796; rev:6;)

#ref: 08e90268f52d942927c9f89fc9b796fb
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS AV2010 Rogue Security Application User-Agent (AV2010)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| AV2010|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008656; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_RogueAV; sid:2008656; rev:5;)

#ref: 08e90268f52d942927c9f89fc9b796fb
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Shop at Home Select Spyware Activity (Bundle)"; flow: established,to_server; content:"User-Agent|3a| Bundle";
classtype: policy-violation; reference:url,doc.emergingthreats.net/2001702; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_SAHSelect; sid:2001702;
rev:34;)

#ref: 08e90268f52d942927c9f89fc9b796fb
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Shop at Home Select Spyware Activity (SAH)"; flow: established,to_server; content:"User-Agent|3a|"; nocase;
content:"SAH Agent"; within:150; pcre:"/User-Agent\:[^\n]+SAH Agent/i"; classtype: policy-violation; reference:url,doc.emergingthreats.net/2001707;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_SAHSelect; sid:2001707; rev:31;)

#ref: 08e90268f52d942927c9f89fc9b796fb
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Shopathomeselect.com Spyware User Agent Activity"; flow: to_server,established; content:"User-Agent|3a|";
nocase; content:"WebDownloader"; within:150; pcre:"/User-Agent\:[^\n]+WebDownloader/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2002038;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_SAHSelect; sid:2002038; rev:245;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent - Save"; flow:to_server,established; content:"GET "; depth:4; content:"|0d 0a|User-
Agent|3a| Save"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011120; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Save.com; sid:2011120; rev:3;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Search Engine 2000 Spyware User Agent"; flow: established,to_server; content:"User-Agent|3a|"; nocase;
content:"searchengine"; within:100; pcre:"/User-Agent\:[^\n]+searchengine/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2001867;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_SearchEngine2000; sid:2001867; rev:22;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Generic.Malware.dld User-Agent (Sickloader)"; flow:to_server,established; content:"User-Agent|3a| Sickloader";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003644; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Sickloader;
sid:2003644; rev:7;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS SideStep Spyware User Agent Activity"; flow: to_server,established; content:"User-Agent|3a|"; nocase;
content:"SideStep"; within:150; pcre:"/User-Agent\:[^\n]+SideStep/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2002078;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_SideSearch; sid:2002078; rev:25;)

#by pedro marinho
```

```
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Sidesearch Spyware User Agent"; flow: established,to_server; content:"User-Agent|3a| Sidesearch"; classtype:
trojan-activity; reference:url,doc.emergingthreats.net/2001869; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_SideSearch; sid:2001869; rev:24;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Sidebar Related Spyware User Agent (Sidebar Client)"; flow:established,to_server; content:"User-Agent|3a|
Sidebar"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008201; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_SideSearch;
sid:2008201; rev:5;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Smileware Connection Spyware Related User-Agent (Smileware Connection)"; flow:established,to_server;
content:"|0d 0a|User-Agent|3a| Smileware"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008892; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Smileware; sid:2008892; rev:5;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Sogoul.com Spyware User-Agent (SogouIMEMiniSetup)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
SogouIME"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008500; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Sogou;
sid:2008500; rev:5;)

#by Jaime Blacso with alienvault
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (SogouExplorerMiniSetup)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
SogouExplorerMiniSetup"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010675; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_SogouExplorer; sid:2010675; rev:3;)

#by Jaime Blacso with alienvault
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS SpamBlockerUtility Fake Anti-Spyware User Agent (SpamBlockerUtility x.x.x)"; flow:to_server,established;
content:"User-Agent|3a|"; nocase; content:"SpamBlockerUtility "; within:150; pcre:"/User-Agent\:[^\n]+SpamBlockerUtility \d/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2003384; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_SpamBlockerUtility; sid:2003384; rev:7;)

#by Jaime Blacso with alienvault
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Speed-runner.com Fake Speed Test User-Agent (SRInstaller)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| SRInstaller|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008145; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Speedrunner; sid:2008145; rev:5;)

#by Jaime Blacso with alienvault
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Speed-runner.com Fake Speed Test User-Agent (SpeedRunner)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| SpeedRunner|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008146; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Speedrunner; sid:2008146; rev:5;)

#by Jaime Blacso with alienvault
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Speed-runner.com Fake Speed Test User-Agent (SRRecover)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| SRRecover|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008151; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Speedrunner; sid:2008151; rev:5;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS iDownloadAgent Spyware User Agent"; flow:to_server,established; content:"User-Agent|3a|"; nocase;
content:"iDownloadAgent"; within:150; pcre:"/User-Agent\:[^\n]+iDownloadAgent/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2002739;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_SpyAxe; sid:2002739; rev:9;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Spyaxe Spyware User Agent"; flow:to_server,established; content:"User-Agent|3a|"; nocase; content:"spyaxe";
within:150; pcre:"/User-Agent\:[^\n]+spyaxe/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2002807; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_SpyAxe; sid:2002807; rev:9;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Spyaxe Spyware User Agent 2"; flow:to_server,established; content:"User-Agent|3a|"; nocase;
content:"spywareaxe"; within:150; pcre:"/User-Agent\:[^\n]+spywareaxe/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2002808;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_SpyAxe; sid:2002808; rev:9;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS SpyDawn.com Fake Anti-Spyware User-Agent (SpyDawn)"; flow:to_server,established; content:"User-Agent|3a|
SpyDawn|0d 0a|"; nocase; classtype:trojan-activity; reference:url,www.spywareguide.com/spydet_3366_spydawn.html; reference:url,doc.emergingthreats.net/2003499;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Spydawn; sid:2003499; rev:7;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Spyhealer Fake Anti-Spyware Install User-Agent (SpyHealer)"; flow:to_server,established; content:"User-
Agent|3a| SpyHeal"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003399; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Spyhealer; sid:2003399; rev:7;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Spylocked Fake Anti-Spyware User-Agent (SpyLocked)"; flow:to_server,established; content:"User-Agent|3a|
SpyLocked"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2005322; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Spylocked; sid:2005322; rev:6;)

#from spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Statblaster.com Spyware User-Agent (fetcher)"; flow:to_server,established; content:"User-Agent|3a| fetcher|0d
0a|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2005318; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Statblaster; sid:2005318; rev:6;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS STEROID Download User-Agent, possible trojan infection"; flow:established,to_server; content:"|0D 0A|User-
Agent|3a| STEROID Download|0D 0A|"; nocase; classtype:trojan-activity; reference:url,anubis.iseclab.org/?action=result&task_id=17b118a86edba30f4f588db66eaf55d10;
reference:url,security.thejoshmeister.com/2009/09/new-malware-ddos-botexe-etc-and.html; reference:url,doc.emergingthreats.net/2009994; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Steroid; sid:2009994; rev:5;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS SureSeeker Spyware User Agent"; flow: established,to_server; content:"User-Agent|3a|"; nocase;
content:"sureseeker"; within:150; pcre:"/User-Agent\:[^\n]+sureseeker\.com/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2001868;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_SureSeeker; sid:2001868; rev:23;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Surfplayer Spyware User Agent"; flow: established,to_server; content:"User-Agent|3a|"; nocase;
content:"SurferPlugin"; within:150; pcre:"/User-Agent\:[^\n]+SurferPlugin/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2001870;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_SurfPlayer; sid:2001870; rev:22;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (agent)"; flow: to_server,established; content:"|0d 0a|User-Agent|3a| agent"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001891; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2001891; rev:13;)
```

```
#by evilghost
#
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"; content:!"bbc.co.uk"; nocase; content:!"microsoft.com"; nocase; content:!"vmware.com"; nocase; content:!"msn.com"; nocase; content:!"msnbc.com"; nocase;
content:!".live.com"; nocase; threshold:type limit, track by_src, count 2, seconds 360; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002400;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2002400; rev:22;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious Spyware Related User Agent (UtilMind HTTPGet)"; flow: to_server,established; content:"User-
Agent|3a|"; nocase; content:"UtilMind HTTPGet"; within:150; pcre:"/User-Agent\:[^\n]+UtilMind HTTPGet/i"; content:!"Host|3a| www.blueocean.com"; nocase; threshold: type limit, count 1,
track by_src, seconds 360; classtype:trojan-activity; reference:url,www.websearch.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002402;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2002402; rev:13;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (Informer from RBC)"; flow:to_server,established; content:"User-Agent|3a|"; nocase;
content:"Informer from RBC"; within:150; pcre:"/User-Agent\:[^\n]+Informer from RBC/i"; classtype:trojan-activity; reference:url,www.kliksoftware.com;
reference:url,doc.emergingthreats.net/bin/view/Main/2003205; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2003205; rev:7;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (Download Agent) Possibly Related to TrinityAcquisitions.com";
flow:to_server,established; content:"User-Agent|3a| Download Agent"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003243;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2003243; rev:9;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (Autoupdate)"; flow:to_server,established; content:"User-Agent|3a| Autoupdate"; nocase;
content:!"Host|3a| update.nai.com"; nocase; content:!"McAfeeAutoUpdate"; nocase; content:!"nokia.com"; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2003337; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2003337; rev:12;)

#by evilghost
#
#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; content:!"rss"; nocase; pcre:"/User-Agent\:[^\n]+http\:\/\//i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003394;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2003394; rev:7;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Toolbar) Possibly Malware/Spyware"; flow:to_server,established; content:"User-Agent|3a|
Toolbar"; content:!"cf.icq.com"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003463; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2003463; rev:12;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (ms)"; flow:to_server,established; content:"User-Agent|3a| ms|0d 0a|"; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003497; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2003497;
rev:8;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious Mozilla User-Agent - Likely Fake (Mozilla/4.0)"; flow:to_server,established; content:"User-Agent|3a|
Mozilla/4.0|0d 0a|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003492; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2003492; rev:9;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious Mozilla User-Agent - Likely Fake (Mozilla/5.0)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| Mozilla/5.0|0d 0a|"; nocase; content:!"|0d 0a|Host|3a| download.releasenotes.nokia.com"; content:!"Mozilla/5.0|0d 0a|Connection|3a| Close|0d 0a 0d 0a|"; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/2009295; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_Agents_Suspicious; sid:2009295; rev:8;)

#by evilghost
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious Mozilla User-Agent Inbound - Likely Fake (Mozilla/5.0)"; flow:to_server,established; content:"|0d
0a|User-Agent|3a| Mozilla/5.0|0d 0a|"; nocase; classtype:trojan-activity; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_Agents_Suspicious;
reference:url,doc.emergingthreats.net/2010908; sid:2010908; rev:3;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious Mozilla User-Agent typo (MOzilla/4.0)"; flow:to_server,established; content:"User-Agent|3a|
MOzilla/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003513; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2003513; rev:8;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious Mozilla User-Agent Separator - likely Fake (Mozilla/4.0+(compatible +MSIE+)";
flow:to_server,established; content:"User-Agent|3a| Mozilla/4.0+(compatible|3b|+MSIE+/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003530;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2003530; rev:10;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (downloader) - Used by Winfixmaster.com Fake Anti-Spyware and Others";
flow:to_server,established; content:"User-Agent|3a| downloader"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003546;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2003546; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (DIALER)"; flow:to_server,established; content:"User-Agent|3a| DIALER"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003566; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2003566;
rev:7;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (update)"; flow:to_server,established; content:"User-Agent|3a| update|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003583; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2003583;
rev:7;)

#Pluses in a UA, suspicious as well
#
#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";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003584; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2003584;
rev:7;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Spyeye or Other Trojan User-Agent (Windows Updates Manager)"; flow:to_server,established; content:"User-
Agent|3a| Windows Updates Manager"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003585; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2003585; rev:7;)

#Pluses in a UA, suspicious as well
#
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 2"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003586; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2003586; rev:7;)

#Pluses in a UA, suspicious as well
#
```

```
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;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003622; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2003622; rev:7;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious Double User-Agent (User-Agent User-Agent)"; flow:to_server,established; content:"User-Agent|3a|
User-Agent|3a| "; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003626; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2003626; rev:6;)

#Pluses in a UA, suspicious as well
#
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"; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003657; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2003657;
rev:12;)

#Pluses in a UA, suspicious as well
#
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; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003927; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2003927; rev:6;)

#Pluses in a UA, suspicious as well
#
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; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003930; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2003930; rev:8;)

#Pluses in a UA, suspicious as well
#
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;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2004443; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2004443; rev:6;)

#Pluses in a UA, suspicious as well
#
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"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2005320; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2005320; rev:7;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent - Likely Webhancer Related Spyware (TEST)"; flow:to_server,established; content:"User-
Agent|3a| TEST|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2006357; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2006357; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent - Likely Webhancer Related Spyware (Huai_Huai)"; flow:to_server,established;
content:"User-Agent|3a| Huai_Huai|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2006361; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2006361; rev:6;)

#Pluses in a UA, suspicious as well
#
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|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2006365; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2006365; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (006)"; flow:established,to_server; content:"User-Agent|3a| 00"; pcre:"/User-Agent\:
00\d+\x0d\x0a/"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2006388; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2006388; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (Dummy)"; flow: established,to_server; content:"User-Agent|3a| Dummy"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007570; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2007570; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent - Likely 2squared.com related (AntiSpyware)"; flow: established,to_server; content:"User-
Agent|3a| AntiSpyware"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007575; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2007575; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious Spyware User Agent (XXX)"; flow:established,to_server; content:"User-Agent|3a| XXX|0d 0a|"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007648; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2007648; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious Spyware User Agent (QdrBi Starter)"; flow:established,to_server; content:"User-Agent|3a| QdrBi
Starter|0d 0a|"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007659; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2007659; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious Spyware Related User Agent (install_s)"; flow:established,to_server; content:"User-Agent|3a|
install_"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007666; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2007666; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious Spyware Related User Agent (count)"; flow:established,to_server; content:"User-Agent|3a| count|0d
0a|"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007667; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2007667; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (Internet Explorer (compatible))"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| Internet Explorer (compatible)|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007772; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2007772; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent - Possible Spyware Related (Mozilla)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| Mozilla|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007854; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2007854; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent - Possible Trojan Downloader (microsoft)"; flow:to_server,established; content:"|0d
0a|User-Agent|3a| microsoft|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007859; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2007859; rev:5;)
```

```
#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent - Possible Trojan Downloader (Internet Explorer 6.0)"; flow:to_server,established;
content:"|0d 0a|User-Agent|3a| Internet Explorer 6.0|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007860;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2007860; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent - Possible Trojan Downloader (Firefox)"; flow:to_server,established; content:"User-
Agent|3a| Firefox|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007868; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2007868; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (Example)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Example|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007884; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2007884; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (downloader)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| downloader|0d
0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007885; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2007885; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (HTTP_CONNECT)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
HTTP_CONNECT|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007899; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2007899; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (Explorer)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Explorer|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007921; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2007921; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (User-Agent Mozilla/4.0 (compatible ))"; flow:to_server,established; content:"|0d
0a|User-Agent|3a| Mozilla/4.0 (compatible|3b| )|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007929;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2007929; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (_)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| _|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007942; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2007942; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (HTTP)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| HTTP|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007943; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2007943; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (popup)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| popup|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007946; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2007946; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (single dash)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| |2d 0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007880; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2007880; rev:4;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (double dashes)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| |2d 2d 0d
0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007948; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2007948; rev:7;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (Unknown)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Unknown|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007991; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2007991; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (2 spaces)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a 20 20 0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007993; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2007993; rev:10;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (1 space)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a 20 0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007994; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2007994; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (Internet)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Internet|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008013; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008013; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (Win95)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| "; content:"Win95";
within:150; pcre:"/User-Agent\:[^\n]+Win95/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008015; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008015; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (Mozilla/4.0 (compatible ICS))"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| Mozilla/4.0 (compatible|3b| ICS)"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008038; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008038; rev:5;)

#Pluses in a UA, suspicious as well
#
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|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008043; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008043; rev:6;)

#Pluses in a UA, suspicious as well
#
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 ";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008048; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008048; rev:6;)
```

```
#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (Internet Explorer)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Internet
Explorer|0d 0a|"; content:!"|0d0a|Host|3a| pnrws.skype.com|0d0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008052;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008052; rev:7;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious Blank User-Agent (descriptor but no string)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a 0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008066; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008066; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (App4)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| App";
content:!"Host|3a| liveupdate.symanteclive update.com|0d 0a|"; pcre:"/User-Agent\: App\d+/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008073;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008073; rev:7;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Mozilla-web)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Mozilla-web";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008084; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008084; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (INSTALLER)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| INSTALLER|0d
0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008096; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008096; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (IEMGR)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| IEMGR|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008097; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008097; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (GOOGLE)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| GOOGLE|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008098; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008098; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (RBR)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| RBR|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008147; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008147; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (MS Internet Explorer)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| MS
Internet Explorer|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008181; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008181; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Installer)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Installer|0d
0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008184; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008184; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (QQ)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| QQ|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008199; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008199; rev:7;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (TestAgent)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| TestAgent|0d
0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008208; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008208; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (SERVER2_03)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| SERVER";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008209; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008209; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious Misspelled Mozilla User-Agent (Mozila)"; flow:to_server,established; content:"User-Agent|3a|
Mozila"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008210; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008210; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (WinProxy)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| WinProxy|0d 0a|";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008211; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008211; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (sickness29a/0.1)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| sickness";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008214; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008214; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (up2dash updater)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| up2dash";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008215; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008215; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (NSIS_DOWNLOAD)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
NSIS_DOWNLOAD"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008216; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008216; rev:5;)

#Pluses in a UA, suspicious as well
#
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:"|0d 0a|User-Agent|3a|
Mozilla "; content:" biz|0d 0a|"; within:15; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008231; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008231; rev:5;)

#Pluses in a UA, suspicious as well
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (chek)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| chek|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008253; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008253; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (IE)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| IE|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008255; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008255; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Nimo Software HTTP Retriever 1.0)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| Nimo Software HTTP"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008257; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008257; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (AutoHotkey)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| AutoHotkey";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008259; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008259; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (WebForm 1)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| WebForm";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008262; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008262; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (opera)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| opera|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008264; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008264; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Zilla)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Zilla|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008266; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008266; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (contains loader)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| ";
content:" loader"; distance:0; within:100; pcre:"/User-Agent\:[^\n]+loader/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008276;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008276; rev:9;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (ld)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| ld|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008342; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008342; rev:8;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (123)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| 123|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008343; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008343; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (DownloadNetFile)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
DownloadNetFile|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008344; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008344; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (angel)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| angel|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008355; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008355; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Accessing)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Accessing|0d
0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008361; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008361; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (ISMYIE)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| ISMYIE|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008363; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008363; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Playtech Downloader)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
Playtech "; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008365; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008365; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (InetURL)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| InetURL";
content:!"www.dell.com"; content:!"pdfmachine.com"; content:!"gs.apple.com"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008374;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008374; rev:12;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (ErrCode)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| ErrCode|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008378; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008378; rev:8;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (svchost)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| svchost"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008391; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008391; rev:9;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (ReadFileURL)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| ReadFileURL|0d
0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008400; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008400; rev:8;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (PcPcUpdater)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| PcPcUpdater";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008413; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008413; rev:7;)

#Pluses in a UA, suspicious as well
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Inet_read)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| Inet_read";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008422; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008422; rev:7;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (CFS Agent)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| CFS Agent";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008423; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008423; rev:7;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (CFS_DOWNLOAD)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
CFS_DOWNLOAD"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008424; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008424; rev:7;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (HTTP Downloader)"; flow: established,to_server; content:"|0d 0a|User-Agent|3a| HTTP
Downloader"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008428; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008428; rev:7;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (AdiseExplorer)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
AdiseExplorer"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008427; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008427; rev:7;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (HttpDownload)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
HttpDownload"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008429; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008429; rev:7;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Download App)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| Download
App"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008440; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008440; rev:7;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (hacker)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| hacker";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008460; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008460; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (ieguideupdate)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
ieguideupdate"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008463; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008463; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (adsntD)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| adsntD";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008464; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008464; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (NULL)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| NULL";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008488; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008488; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (dwplayer)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| dwplayer";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008489; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008489; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (ieagent)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| ieagent";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008494; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008494; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (antispyprogram)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
antispyprogram"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008495; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008495; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (SUiCiDE/1.5)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| SUiCiDE";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008504; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008504; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent - Possible Trojan Downloader (\xa2\xa2HttpClient)"; flow:established,to_server;
content:"|0d 0a|User-Agent|3a| |5c|xa2|5c|xa2HttpClient|0d 0a|"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008510;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008510; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (C slash slash)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| C|3a|\\";
content:!"\\Citrix\\ICA Client\\"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008512; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008512; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (msIE 7.0)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| msIE";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008513; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008513; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (AVP2006IE)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| AVP200";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008514; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008514; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (winlogon)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| winlogon";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008544; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008544; rev:5;)
```

```
#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Internet HTTP Request)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
Internet HTTP"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008564; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008564; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent Detected (Windows+NT)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
Windows+NT"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008600; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008600; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent Detected (RLMultySocket)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
RLMultySocket|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008603; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008603; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent Detected (Downloader1.2)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
Downloader"; pcre:"/User-Agent\: Downloader\d+\.\d/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008643; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008643; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent Detected (Compatible)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
Compatible|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008657; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008657; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent Detected (GetUrlSize)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
GetUrlSize|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008658; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008658; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent Detected (DigitAl56K/6.3)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
DigitAl56K/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008659; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008659; rev:5;)

#Pluses in a UA, suspicious as well
#
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:"|0d 0a|User-
Agent|3a| aguarovex-loader v"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008663; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008663; rev:5;)

#Pluses in a UA, suspicious as well
#
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:"|0d 0a|User-
Agent|3a| WINS_HTTP_SEND"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008734; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008734; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (FTP)"; flow: to_server,established; content:"|0d 0a|User-Agent|3a| Ftp|0d 0a|"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008735; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008735; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent - Possible Admoke Admware (bdwinrun)"; flow: to_server,established; content:"|0d 0a|User-
Agent|3a| bdwinrun"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008742; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008742; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent - Possible Admoke Admware (bdsclk)"; flow: to_server,established; content:"|0d 0a|User-
Agent|3a| bdsclk"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008743; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008743; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (checkonline)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| checkonline|0d
0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008749; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008749; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Kvadrlson 1.0)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| Kvadrlson ";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008756; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008756; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (miip)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| miip|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008797; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008797; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Mozil1a)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| Mozil1a";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008847; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008847; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Errordigger.com related)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
min|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008912; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008912; rev:5;)

#Pluses in a UA, suspicious as well
#
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:"|0d 0a|User-
Agent|3a| Mozilla/1.0 (compatible|3b| MSIE 8.0|3b|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008913; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008913; rev:6;)

#Pluses in a UA, suspicious as well
#
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:"|0d 0a|User-
Agent|3a| xr|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008914; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008914; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (HELLO)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| HELLO|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008941; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008941; rev:5;)
```

```
#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Yandesk)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| Yandesk|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008916; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008916; rev:5;)

#Pluses in a UA, suspicious as well
#
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:"|0d 0a|User-
Agent|3a| sections|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008919; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008919; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (IE/1.0)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| IE/1.0|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008956; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2008956; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (User-Agent Mozilla/4.0 (compatible))"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| Mozilla/4.0 (compatible)|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008974; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008974; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (BlackSun)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| BlackSun";
classtype:trojan-activity; reference:url,www.bitdefender.com/VIRUS-1000328-en--Trojan.Pws.Wow.NCY.html; reference:url,doc.emergingthreats.net/bin/view/Main/2008983;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2008983; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (IE_6.0)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| IE_6.0";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2009021; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2009021; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (FileDownloader)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
FileDownloader"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2009027; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009027; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (get_site1)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| get_site";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009111; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009111;
rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (GETJOB)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| GETJOB";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009124; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009124;
rev:4;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (runUpdater.html)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
runUpdater|2e|html"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009355; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009355; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (runPatch.html)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
runPatch|2e|html"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009356; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009356; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (Mozilla/4.8 ru)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| Mozilla/4.8
[ru] (Windows NT 6.0|3b| U)|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009438; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009438; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (HelpSrvc)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| HelpSrvc|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009439; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009439;
rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (Internet Antivirus Pro)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
Internet Antivirus Pro|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009440; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009440; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent - Possibly Xema (AgavaDwnl)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
AgavaDwnl|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009445; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009445; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (Macrovision_DM)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
Macrovision_DM"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009445; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009446; rev:4;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (ClickAdsByIE)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
ClickAdsByIE"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009445; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009456; rev:4;)

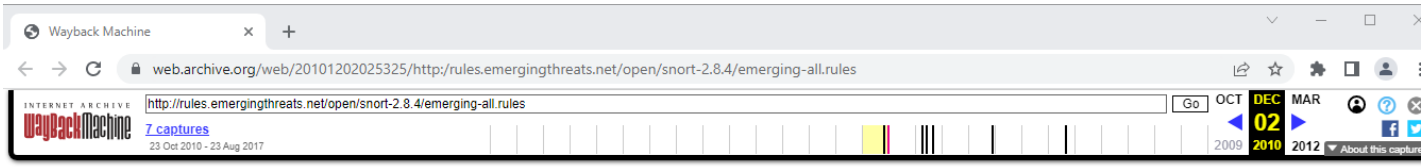
#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious Downloader User-Agent (Windows+NT+5.1)"; flow:established,to_server; content:"|0D 0A|User-
Agent|3a|"; content:"Windows+NT+5.1|0D 0A|"; within:128; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009486; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009486; rev:5;)

#Pluses in a UA, suspicious as well
#
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:"|0d 0a|User-
Agent|3a| Session|0d 0a|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009512; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009512; rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Poker)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Poker|0d 0a|";
```

```
classtype:trojan-activity; reference:url,vil.nai.com/vil/content/v_130975.htm; reference:url,doc.emergingthreats.net/2009534; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009534; rev:5;)

#Pluses in a UA, suspicious as well
#
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:"GET "; depth:4; content:"|0d 0a|User-Agent\: Loands|0d 0a|"; nocase; depth:200; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009537;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009537; rev:4;)
```




```
#Pluses in a UA, suspicious as well
#
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:"GET "; depth:4; content:"|0d 0a|User-Agent\: ms_ie|0d 0a|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009538;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009538; rev:4;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (PCFlashBangA)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
PCFlashBangA|0d 0a|"; classtype:trojan-activity; reference:url,www.ca.com/us/securityadvisor/pest/pest.aspx?id=453113169; reference:url,doc.emergingthreats.net/2009540;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009540; rev:5;)

#Pluses in a UA, suspicious as well
#
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:"GET "; depth:4; content:"|0d 0a|User-Agent\: Forthgoner|0d 0a|"; nocase; depth:200; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009547;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009547; rev:4;)

#Pluses in a UA, suspicious as well
#
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:"|0d 0a|User-Agent|3a| InHold|0d 0a|"; nocase; depth:200; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009544; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009544; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (_TEST_)"; flow: to_server,established; content:"User-Agent|3a| _TEST_"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009545; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009545;
rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (INet)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| INet|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009703; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009703;
rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Mozilla/3.0 (compatible))"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
Mozilla/3.0 (compatible)|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009867; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009867; rev:4;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS PinBall Corp. Related suspicious activity"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
PinBallCorp-BSAI"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009908; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009908; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent - Likely Hostile (User Agent)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| User Agent"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009930; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009930; rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (MyIE/1.0)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| MyIE/";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009991; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009991;
rev:5;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (ONANDON)"; flow:established,to_server; content:"User-Agent|3a| ONANDON|0d 0a|"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009995; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2009995;
rev:6;)

#Pluses in a UA, suspicious as well
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Fake Wget User Agent - Likely Hostile (wget 3.0)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
wget 3.0|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007961; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2007961; rev:7;)

#by Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS TROJAN Drop.Agent.bfsv HTTP Activity (UsER-AgENt)"; flow:established,to_server; content:"GeT "; depth:4;
content:"HttP"; depth:200; content:"|0d 0a|HoST|3a| "; content:"|0d 0a|UsER-AgENt|3a| |0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010129;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2010129; rev:3;)

#by jerry at cybercave
#
alert tcp $HOME_NET any -> any $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Sme32)"; flow: established, to_server; content:"|0d 0a|User-Agent|3a| Sme32|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010137; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2010137;
rev:3;)

#by Bojan
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (M0zilla)"; flow:established,to_server; content:"|0d 0a|User-Agent|3A 20|M0zilla/4.0|20|
(compatible)"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010265; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2010265; rev:2;)

#by darren spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (CrazyBro)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| CrazyBro";
nocase; classtype:trojan-activity; reference:url,www.f-secure.com/v-descs/trojan-proxy_w32_kvadr_gen!a.shtml; reference:url,www.threatexpert.com/report.aspx?
md5=fd2d6bb1d2a9803c49f1e175d558a934; reference:url,www.threatexpert.com/report.aspx?md5=e4664144f8e95cfec510d5efa24a35e7; reference:url,anubis.iseclab.org/?
action=result&task_id=14118b80c1b346124c183394d5b3004b1&format=html; reference:url,doc.emergingthreats.net/2010333; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2010333; rev:3;)

#matt jonkman, general downloader ua
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent - Possible Trojan Downloader (ie)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| ie|0d 0a|"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2007827; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2007827; rev:6;)

#by Deapesh Misra
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious UA string (MSIE7 na)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| Mozilla/4.0
(compatible|3b| MSIE 7.0|3b| na|3b| )"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010461; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2010461; rev:4;)

#by jerry
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (???)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| ???";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010595; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2010595;
rev:3;)

#by jerry
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent Mozilla/3.0"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| Mozilla/3.0
(compatible|3b| Internet Explorer)"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010599; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2010599; rev:2;)

#by jerry
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent WebUpdate"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| WebUpdate|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010600; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2010600;
rev:2;)

#by evilghost
#
#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:"|0d
0a|User-Agent|3a| "; content:!"|0d 0a|User-Agent|3a| Mozilla/"; pcre:"/\x0d\x0aUser-Agent\: \d\d\d/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010697;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2010697; rev:4;)

#by Waldo kitty
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Incorrectly formatted User-Agent string (dashes instead of semicolons) Likely Hostile";
flow:established,to_server; content:"|0d 0a|User-Agent|3a| Mozilla/4.0 (compatible- MSIE 6.0- Windows NT 5.1- SV1- "; classtype:bad-unknown;
reference:url,doc.emergingthreats.net/2010868; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2010868; rev:3;)

#by Waldo kitty
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET USER_AGENTS Fake Mozilla UA Inbound (Mozilla/0.xx)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
Mozilla/0."; classtype:bad-unknown; reference:url,doc.emergingthreats.net/2010904; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2010904; rev:4;)

#by Waldo kitty
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Fake Mozilla UA Outbound (Mozilla/0.xx)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
Mozilla/0."; classtype:bad-unknown; reference:url,doc.emergingthreats.net/2010905; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2010905; rev:4;)

#by Waldo kitty
#
#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:"|0d 0a|User-
Agent|3a| Mozilla/4.0 (compatible|3b| "; content:!")|0d 0a|"; distance:0; pcre:"/\(compatible[^\)]+\n/"; classtype:bad-unknown; reference:url,doc.emergingthreats.net/2010906;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2010906; rev:3;)

#by mareadmin
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious UA - Download Master - Possible Malware Downloader"; flow:established,to_server; content:"|0d
0a|User-Agent|3a| Download Master"; classtype:policy-violation; threshold: type limit, count 1, seconds 60, track by_src; reference:url,www.httpuseragent.org/list/Download+Master-
n727.htm; reference:url,www.westbyte.com/dm/; reference:url,doc.emergingthreats.net/2011146; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2011146; rev:3;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (webcount)"; flow:to_server,established; content:"GET "; depth:4; content:"|0d 0a|User-
Agent|3a| webcount"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011149; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2011149; rev:3;)

#by stillsecure
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (HTTP_Query)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| HTTP_Query|0d
0a|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011678; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
sid:2011678; rev:3;)

#by stillsecure
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (dbcount)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| dbcount|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011679; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2011679;
rev:3;)

#by stillsecure
#re 5823f6065f5e2e49cd011e6acdd23bd9
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (RangeCheck/0.1)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
RangeCheck/0.1|0d 0a|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011718; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2011718; rev:3;)

#by stillsecure
#re 5823f6065f5e2e49cd011e6acdd23bd9
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (SOGOU_UPDATER)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
SOGOU_UPDATER|0d 0a|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011719; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2011719; rev:3;)

#2010-07-14 By Pedro Marinho
#002170330780b29686abccef42c4ce35
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (AskInstallChecker)"; flow:to_server,established; content:"GET "; depth:4; content:"|0d
0a|User-Agent|3a| AskInstallChecker|0d 0a|"; nocase; classtype:trojan-activity; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
reference:url,doc.emergingthreats.net/2011225; sid:2011225; rev:1;)

#cd025fbeb51e2a02793f2c60a2777aa8
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (SeFastSetup)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| SeFastSetup";
classtype:trojan-activity; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; reference:url,doc.emergingthreats.net/2011225; sid:2011226;
rev:1;)

#cd025fbeb51e2a02793f2c60a2777aa8
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (NSIS_Inetc (Mozilla))"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
NSIS|5f|Inetc |28|Mozilla|29|"; classtype:trojan-activity; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious;
reference:url,doc.emergingthreats.net/2011227; sid:2011227; rev:1;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (Suggestion)"; flow:to_server,established; content:"GET "; depth:4; content:"|0d 0a|User-
Agent|3a| Suggestion|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011229; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2011229; rev:3;)

#by pedro marinho
```

```
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Mozilla/4.0 (SP3 WINLD))"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
Mozilla/4.0 |28|SP3 WINLD|29 0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011238; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Suspicious; sid:2011238; rev:3;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Target Saver Spyware User Agent"; flow: established,to_server; content:"|0d 0a|User-Agent|3a| TSA/"; classtype:
trojan-activity; reference:url,doc.emergingthreats.net/2001871; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_TargetSaver; sid:2001871; rev:21;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS TryMedia Spyware User Agent (TryMedia_DM_2.0.0)"; flow:established,to_server; content:"User-Agent|3a|
TryMedia_DM_"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2007600; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_TryMedia; sid:2007600; rev:6;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS UCMore Spyware Activity"; flow: to_server,established; content:"User-Agent|3a|"; nocase; content:"UCmore";
within:150; pcre:"/User-Agent\:[^\n]+UCmore/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2001736; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_UCMore; sid:2001736; rev:267;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS UCMore Spyware Activity User Agent String"; flow: to_server,established; content:"|0d 0a|User-Agent|3a| EI|0d
0a|"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2001996; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_UCMore;
sid:2001996; rev:13;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Ultimate HAckerz Team User-Agent - Likely Trojan Report"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| Mozilla/4.0 (compatible|3b| MSIE 6.0|3b| Windows NT 5.1|3b| SV1|3b| Made by UltimateHackerzTeam)"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010346;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_UltimateHackerz; sid:2010346; rev:3;)

#by jeffrey brown
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS www.vaccinekiller.com Related Spyware User Agent (VaccineKillerIU)"; flow:established,to_server; content:"|0d
0a|User-Agent|3a| VaccineKiller"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009993; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Vaccine; sid:2009993; rev:5;)

#by jeffrey brown
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Visicom Spyware User Agent"; flow: established,to_server; content:"User-Agent|3a|"; nocase; content:"Visicom";
within:150; pcre:"/User-Agent\:[^\n]+Visicom/i"; threshold: type limit, count 1, seconds 360, track by_src; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2001872;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Visicom; sid:2001872; rev:24;)

#by jeffrey brown
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Vombanetwork Spyware User Agent (VombaProductsInstaller)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| Vomba"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007869; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Vomba;
sid:2007869; rev:5;)

#by Axn Jxn
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS WebHack Control Center User-Agent Outbound (WHCC/)"; flow:to_server,established; content:"User-Agent|3a|";
nocase; content:"WHCC"; nocase; distance:0; within:50; pcre:"/User-Agent\:[^\n]+WHCC/i"; classtype:trojan-activity; reference:url,www.governmentsecurity.org/forum/index.php?
showtopic=5112&pid=28561&mode=threaded&start=; reference:url,doc.emergingthreats.net/2003925; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_WebHack; sid:2003925; rev:6;)

#by Axn Jxn
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Webbuying.net Spyware Install User-Agent (wbi_v0.90)"; flow:to_server,established; content:"User-Agent|3a|";
nocase; content:"wbi_v"; within:150; pcre:"/User-Agent\:[^\n]+wbi_v\d/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003441;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Webbuying; sid:2003441; rev:7;)

#by Axn Jxn
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Webbuying.net Spyware Install User-Agent 2 (wb v1.6.4)"; flow:to_server,established; content:"User-Agent|3a|";
nocase; content:"wb v"; within:150; pcre:"/User-Agent\:[^\n]+wb v\d/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003449;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Webbuying; sid:2003449; rev:7;)

#by Axn Jxn
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Win-touch.com Spyware User Agent (WTRecover)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
WTRecover"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2006392; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Win-Touch;
sid:2006392; rev:7;)

#by Axn Jxn
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Win-touch.com Spyware User Agent (WTInstaller)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
WTInstaller"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2006393; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Win-Touch;
sid:2006393; rev:7;)

#by Axn Jxn
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Win-touch.com Spyware User Agent (WinTouch)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
WinTouch"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2008141; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Win-Touch;
sid:2008141; rev:6;)

#by Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Win32.Tdss User Agent Detected (Mozzila)"; flow:established,to_server; content:"|0d 0a|User-Agent\: Mozzila";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010889; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Win32.tdss;
sid:2010889; rev:2;)

#by Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS WinButler User-Agent (WinButler)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| WinButler|0d
0a|"; classtype:trojan-activity; reference:url,www.winbutler.com; reference:url,www.prevx.com/filenames/239975745155427649-0/WINBUTLER.EXE.html;
reference:url,doc.emergingthreats.net/2008190; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_WinButler; sid:2008190; rev:5;)

#Matt Jonkman, from spyware lp data and Castlecops
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Winfixmaster.com Fake Anti-Spyware User-Agent (WinFixMaster)"; flow:to_server,established; content:"User-
Agent|3a| WinFixMaster"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003544; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Winfix; sid:2003544; rev:6;)

#Matt Jonkman, from spyware lp data and Castlecops
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Winfixmaster.com Fake Anti-Spyware User-Agent 2 (WinFix Master)"; flow:to_server,established; content:"User-
Agent|3a| WinFix Master"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003545; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Winfix; sid:2003545; rev:7;)

#Matt Jonkman, from spyware lp data and Castlecops
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Winsoftware.com Fake AV User-Agent (DNS Extractor)"; flow:to_server,established; content:"User-Agent|3a| DNS
Extractor"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003567; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Winfix; sid:2003567; rev:7;)

#Matt Jonkman, from spywarelp data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Winsoftware.com Spyware User-Agent (Updater)"; flow:to_server,established; content:"User-Agent|3a| Updater|0d
0a|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003470; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Winfix;
sid:2003470; rev:7;)

#Matt Jonkman, from spywarelp data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS WinSoftware.com Spyware User-Agent (WinSoftware)"; flow:to_server,established; content:"User-Agent|3a|
WinSoftware"; nocase; classtype:trojan-activity; reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=WinSoftware%20Corporation%2c%20Inc.%20(v)&threatid=90037;
reference:url,doc.emergingthreats.net/2003527; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Winsoftware; sid:2003527; rev:7;)

#Matt Jonkman, from spywarelp data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS WinSoftware.com Spyware User-Agent (NetInstaller)"; flow:to_server,established; content:"User-Agent|3a|
NetInstaller"; nocase; classtype:trojan-activity; reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=WinSoftware%20Corporation,%20Inc.%20(v)&threatid=90037;
reference:url,doc.emergingthreats.net/2003528; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Winsoftware; sid:2003528; rev:6;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent (XieHongWei-HttpDown/2.0)"; flow:to_server,established; content:"GET "; depth:4;
content:"|0d 0a|User-Agent|3a| XieHongWei"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011248; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_XieHongWie; sid:2011248; rev:3;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS XupiterToolbar Spyware User Agent Activity"; flow: to_server,established; content:"User-Agent|3a|"; nocase;
content:"XupiterToolbar"; within:150; pcre:"/User-Agent\:[^\n]+XupiterToolbar/i"; classtype: trojan-activity; reference:url,castlecops.com/tk781-Xupitertoolbar_dll_t_dll.html;
reference:url,doc.emergingthreats.net/2002071; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Xupiter; sid:2002071; rev:13;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (Yodao Desktop Dict)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Yodao";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011123; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Yaodo; sid:2011123;
rev:3;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Hotbar Spyware User Agent"; flow: established,to_server; content:"User-Agent|3a|"; nocase; content:"Hotbar";
within:150; pcre:"/User-Agent\:[^\n]+Hotbar/i"; threshold: type limit, count 1, seconds 360, track by_src; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2001858;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Zango_Hotbar; sid:2001858; rev:23;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Hotbar Spyware User-Agent"; flow: to_server,established; content:"User-Agent|3a| host"; nocase; pcre:"/User-
Agent\:[^\n]+host(ie|oe|oi|ol)/i"; classtype:trojan-activity; reference:url,www.doxdesk.com/parasite/Hotbar.html; reference:url,www.pchell.com/support/hotbar.shtml;
reference:url,doc.emergingthreats.net/2002164; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Zango_Hotbar; sid:2002164; rev:11;)

#Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Zango-Hotbar User Agent"; flow:to_server,established; content:"User-Agent|3a|"; nocase; content:"zb-hb-";
within:150; pcre:"/User-Agent\:[^\n]+zb-hb-/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003223; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Zango_Hotbar; sid:2003223; rev:7;)

#Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Zango-Hotbar User Agent (zbu-hb-)"; flow:to_server,established; content:"User-Agent|3a|"; nocase; content:"zbu-
hb-"; within:150; pcre:"/User-Agent\:[^\n]+zbu-hb-/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003305; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Zango_Hotbar; sid:2003305; rev:8;)

#Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Spamblockerutility.com-Hotbar User Agent (sbu-hb-)"; flow:to_server,established; content:"User-Agent|3a|";
nocase; content:"sbu-hb-"; within:150; pcre:"/User-Agent\:[^\n]+sbu-hb-/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003363;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Zango_Hotbar; sid:2003363; rev:9;)

#Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Hotbar Zango Toolbar Spyware User Agent (ZangoToolbar )"; flow:to_server,established; content:"User-Agent|3a|";
nocase; content:"ZangoToolbar"; within:150; pcre:"/User-Agent\:[^\n]+ZangoToolbar\d/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003365;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Zango_Hotbar; sid:2003365; rev:7;)

#Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Hotbar Tools Spyware User Agent (hbtools)"; flow:to_server,established; content:"User-Agent|3a|"; nocase;
content:"hbtools "; within:150; pcre:"/User-Agent\:[^\n]+hbtools \d/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003383;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Zango_Hotbar; sid:2003383; rev:7;)

#Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS 180 Solutions (Zango Installer) User Agent"; flow:to_server,established; content:"User-Agent|3a|"; nocase;
content:"SAIv"; within:150; pcre:"/User-Agent\:[^\n]+SAIv/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003062; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Zango_Hotbar; sid:2003062; rev:7;)

#Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Zango Seekmo Bar Spyware User-Agent (Seekmo Toolbar)"; flow:to_server,established; content:"User-Agent|3a|";
nocase; content:"Seekmo"; within:150; pcre:"/User-Agent\:[^\n]+Seekmo/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003397;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Zango_Hotbar; sid:2003397; rev:7;)

#Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Zango Cash Spyware User Agent (ZC-Bridgev26)"; flow:established,to_server; content:"User-Agent|3a| ZC-Bridgev";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006780; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Zango_Hotbar;
sid:2006780; rev:6;)

#Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Zango Cash Spyware User Agent (ZC XML-RPC C++ Client)"; flow:established,to_server; content:"User-Agent|3a| ZC
XML-RPC"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006781; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Zango_Hotbar;
sid:2006781; rev:36;)

#Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Gator Agent Traffic"; flow: to_server,established; content:"User-Agent|3a|"; nocase; content:" Gator"; nocase;
within:150; pcre:"/User-Agent\:[^\n]+Gator/i"; classtype: policy-violation; reference:url,doc.emergingthreats.net/2000026; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Zango_Hotbar; sid:2000026; rev:34;)

#Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Wild Tangent Agent Activity"; flow: to_server,established; content:"User-Agent|3a|"; nocase;
content:"WildTangent"; within:150; pcre:"/User-Agent\:[^\n]+Wildtangent/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2001639;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Zango_Hotbar; sid:2001639; rev:27;)

#matt jonkman
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Hotbar Agent Activity"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| PinballCorp"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011691; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Zango_Hotbar;
sid:2011691; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS ZenoSearch Spyware User-Agent"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| ["; pcre:"/User-
Agent\: \[.*\][A-F0-9]{2}-[A-F0-9]{2}-[A-F0-9]{2}-[A-F0-9]{2}/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008279; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_Zeno; sid:2008279; rev:7;)

#by Jerry at cybercave
#
alert tcp $HOME_NET any -> any $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (asp2009)"; flow: established, to_server; content:"|0d 0a|User-Agent|3a| asp2009|0d 0a|";
classtype:trojan-activity; reference:url,www.threatexpert.com/report.aspx?md5=6cad864a439da7bbd6f1cec941cca72b; reference:url,doc.emergingthreats.net/2010136;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_asp2009; sid:2010136; rev:3;)

#by pmarinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent gomtour"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| gomtour|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011087; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_gomtour; sid:2011087;
rev:3;)

#by jaime blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (i-scan)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| i-scan"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011105; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_i-scan; sid:2011105;
rev:3;)

#by jaime blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS iWon Spyware (iWonSearchAssistant)"; flow:to_server,established; content:"User-Agent|3a| iWonSearch";
classtype:trojan-activity; reference:url,www.spywareguide.com/product_show.php?id=461; reference:url,doc.emergingthreats.net/2002169; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_iWon; sid:2002169; rev:12;)

#by Mike Cox
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (iexplore)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| iexplore|0d
0a|"; nocase; classtype:attempted-recon; reference:url,doc.emergingthreats.net/2000466; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_iexplore;
sid:2000466; rev:4;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS iwin.com Games/Spyware User-Agent (iWin GameInfo Installer Helper)"; flow:established,to_server; content:"|0d
0a|User-Agent|3a| iWin "; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008558; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_iwin; sid:2008558; rev:5;)

#by jaime blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User-Agent (lineguide)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| lineguide";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011106; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_lineguide;
sid:2011106; rev:3;)

#by jaime blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Download UBAgent User Agent - lop.com and other spyware"; flow:to_server,established; content:"User-Agent|3a|";
nocase; content:"Download UBAgent"; within:150; pcre:"/User-Agent\:[^\n]+Download UBAgent/i"; classtype:trojan-activity; reference:url,www.spywareinfo.com/articles/lop/;
reference:url,doc.emergingthreats.net/2003345; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_lop; sid:2003345; rev:7;)

#by pmarinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Suspicious User Agent Recuva (www.recuva.com)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
Recuva|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011090; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_recuva;
sid:2011090; rev:3;)

#by pmarinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS ZCOM Adware/Spyware User-Agent (ZCOM Software)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
ZCOM"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008503; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/USER_AGENTS/USER_AGENTS_zcom; sid:2008503;
rev:5;)

#From Chris Norton.
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET VIRUS Generic Downloader Outbound HTTP connection - Downloading Code"; flow:established,to_server; content:"User-Agent|3A|
PE-"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2002695; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/VIRUS_Bankem; sid:2002695; rev:7;)

#BugBear
#Submitted by Brad Doctor, 3/8/2005, for BugBear@MM
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET VIRUS Bugbear@MM virus via SMTP"; flow: established;
content:"uv+LRCQID7dIDFEECggDSLm9df8C/zSNKDBBAAoGA0AEUQ+FEN23f7doqAT/dCQk/xWcEQmDxCTD"; classtype: misc-activity; reference:url,www.symantec.com/avcenter/venc/data/w32.bugbear@mm.html;
reference:url,doc.emergingthreats.net/2001764; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/VIRUS_BugBear; sid:2001764; rev:6;)

#BugBear
#Submitted by Brad Doctor, 3/8/2005, for BugBear@MM
#
#alert tcp $HOME_NET any -> any 139 (msg:"ET VIRUS BugBear@MM virus in Network share"; flow: established; content:"|24 48 fb bb ff e6 63 02 3a 20 41 70 61 63 68 65|"; classtype: misc-
activity; reference:url,www.symantec.com/avcenter/venc/data/w32.bugbear@mm.html; reference:url,doc.emergingthreats.net/2001765; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/VIRUS_BugBear; sid:2001765; rev:6;)

#BugBear
#Submitted by Brad Doctor, 3/8/2005, for BugBear@MM
#
#alert tcp $HOME_NET any -> any 139 (msg:"ET VIRUS BugBear@MM Worm Copied to Startup Folder"; flow: established; content:"|77 00 69 00 6B 00 2E 00 65 00 78 00 65 00 00 00|"; classtype:
misc-activity; reference:url,www.symantec.com/avcenter/venc/data/w32.bugbear@mm.html; reference:url,doc.emergingthreats.net/2001766; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/VIRUS_BugBear; sid:2001766; rev:6;)

#Submitted 2006-05-01 by Mark Tombaugh
#
##alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET DELETED Mytob.X clam SMTP Inbound"; flow:to_server,established; content:"UEsDBAoA"; content:"ojRrPyGt"; distance:8; within:16;
classtype:trojan-activity; reference:url,www3.ca.com/securityadvisor/virusinfo/virus.aspx?ID=42326; reference:url,doc.emergingthreats.net/2002892;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/VIRUS_Nugache; sid:2002892; rev:4;)

#Submitted 2006-05-01 by Mark Tombaugh
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET DELETED Mytob.X clam SMTP Outbound"; flow:to_server,established; content:"UEsDBAoA"; content:"ojRrPyGt"; distance:8; within:16;
classtype:trojan-activity; reference:url,www3.ca.com/securityadvisor/virusinfo/virus.aspx?ID=42326; reference:url,doc.emergingthreats.net/2002893;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/VIRUS_Nugache; sid:2002893; rev:4;)

#Submitted 2006-05-01 by Mark Tombaugh
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET VIRUS W32.Nugache SMTP Inbound"; flow:to_server,established; content:"RE9TIG1v"; content:"GUuDQ0KJ"; distance:1; within:9;
classtype:trojan-activity; reference:url,www.symantec.com/avcenter/venc/data/w32.nugache.a@mm.html; reference:url,doc.emergingthreats.net/2002894;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/VIRUS_Nugache; sid:2002894; rev:4;)

#Submitted 2006-05-01 by Mark Tombaugh
#
```

```
#alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET VIRUS W32.Nugache SMTP Outbound"; flow:to_server,established; content:"RE9TIG1v"; content:"GUuDQ0KJ"; distance:1; within:9;
classtype:trojan-activity; reference:url,www.symantec.com/avcenter/venc/data/w32.nugache.a@mm.html; reference:url,doc.emergingthreats.net/2002895;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/VIRUS_Nugache; sid:2002895; rev:4;)

#by Jonathan Gross. Experimental
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET VIRUS WinUpack Modified PE Header Inbound"; flow:established; content:"|4d 5a 4b 45 52 4e 45 4c 33 32 2e 44 4c 4c 00 00|";
classtype:bad-unknown; reference:url,doc.emergingthreats.net/bin/view/Main/WinPEHeaders; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/VIRUS_PE_Headers;
sid:2003614; rev:4;)

#by Jonathan Gross. Experimental
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET VIRUS WinUpack Modified PE Header Outbound"; flow:established; content:"|4d 5a 4b 45 52 4e 45 4c 33 32 2e 44 4c 4c 00 00|";
classtype:bad-unknown; reference:url,doc.emergingthreats.net/bin/view/Main/WinPEHeaders; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/VIRUS_PE_Headers;
sid:2003615; rev:4;)

#by Dan Clemens of packetninjas.net
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN UpackbyDwing in HTTP Download Possibly Hostile"; flow:from_server,established; content:"UpackByDwing|40|";
content:"PE|00 00|"; within:20; classtype:trojan-activity; reference:url,www.packetninjas.net; reference:url,doc.emergingthreats.net/2008946; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/VIRUS_PE_Headers; sid:2008946; rev:2;)

#by Dan Clemens of packetninjas.net
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN UpackbyDwing in HTTP (2) Possibly Hostile"; flow:from_server,established; content:"PE|00 00|"; content:"Upack|00
00|"; within:255; classtype:trojan-activity; reference:url,www.packetninjas.net; reference:url,doc.emergingthreats.net/2008947; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/VIRUS_PE_Headers; sid:2008947; rev:2;)

#matt jonkman/wes brown
#falsing, needs adjustment
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN VMProtect Packed Binary Inbound via HTTP - Likely Hostile"; flowbits:isset,ET.http.binary;
flow:established,from_server; content:"VirtualProtect|00|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009080; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/VIRUS_PE_Headers; sid:2009080; rev:3;)

#These are by Vlad Tsyrklevich during presentation at Toorcon 06. These are experimental and will likely be high load.
#more information at http://toorcon.org/2006/conference.html?id=29
#These are disabled by default until we learn more about them.
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET VIRUS SHELLCODE CLET polymorphic payload"; classtype:shellcode-detect; dsize: >40; content: "|74 07 eb|"; content: "|e8|";
distance: 1; within: 1; pcre: "/\xeb.[\x58-\x5b]\x31[\xc0\xc9\xd2\xdb][\xb0-\xb3].\x8b.[\x05\x2d\x35\x81\xc1]/sm"; pcre: "/[\x40-\x43\xfd\xff][\x40-\x43\xff][\x40-\x43\x80\xff][\x40-
\x43\xe9-\xeb\xff\x80\x2c][\x40-\x43\x48-\x4b\xe9-\xeb\x01\x2c\x80][\x48-\x4c\xe9-\xeb\x02\x2c][\x03\x48-\x4b][\x48-\x4b]\x74\x07\xeb.\xe8.\xff\xff\xff/smR";
reference:url,toorcon.org/2006/conference.html?id=29; reference:url,doc.emergingthreats.net/2003117; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/VIRUS_Polymorphic_Experimental; sid:2003117; rev:3;)

#These are by Vlad Tsyrklevich during presentation at Toorcon 06. These are experimental and will likely be high load.
#more information at http://toorcon.org/2006/conference.html?id=29
#These are disabled by default until we learn more about them.
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET VIRUS SHELLCODE Shikata Ga Nai polymorphic payload"; classtype:shellcode-detect; dsize: >26; content: "|d9 74 24 f4|"; pcre:
"/[\x29\x2b\x31\x33]\xc9/sm"; pcre: "/[\xd9-\xdb\xdd].{1,11}\xd9\x74\x24\xf4.{0,10}[\x58\x5a\x5b\x5d-\x5f]/sm"; pcre: "/([\x29\x2b\x31\x33\xb8\xba\xbb\xbe\xbf\xd9-\xdb\xdd][^\x00\xff]
[^\x00\xff][^\x00][^\x00\xff][^\x00][^\x00\xff][^\x00\xff][^\x00][^\x00][^\x00\xff][^\x00\xff][^\x00\xff][^\x00][^\x00][\x31\x83][\x42\x43\x46\x47\x50\x53\x56-
\x58\x5a\x5e\x5f\x70\x72\x73\x77\x78\x7a\x7b\x7e\xc0\xc2\xc3\xc6\xc7\xe8\xea\xeb\xee\xef][\x04\x0e\x10\x12\x13\x15\x17\xfc][\x03\x31\x83][\x42\x43\x46\x47\x50\x53\x56-
\x58\x5a\x5e\x5f\x70\x72\x73\x77\x78\x7a\x7b\x7e\xc0\xc2\xc3\xc6\xc7\xe8\xea\xeb\xee\xef][\x04\x0a\x0c\x0e-\x13\x15\x17\xfc][\x03\x83]..[^\x1d\xe2][^\x0a\xf5])|
([\x29\x2b\x31\x33\xb8\xba\xbb\xbd-\xbf\xd9-\xdb\xdd][^\x00][^\x00][^\x00][^\x00][^\x00][^\x00][^\x00][^\x00][\x24\xb1\xd9-\xdb\xdd][^\x00][\x58\x5a\x5b\x5d-\x5f\xb8\xba\xbb\xbd-
\xbf\xd9][^\x00][^\x00][^\x00][^\x00][\x31\x83][\x42\x43\x45-\x47\x50\x53\x55-\x58\x5a\x5d-\x5f\x68\x6a\x6b\x6e-\x70\x72\x73\x75\x77\x78\x7a\x7b\x7d\x7e\xc0\xc2\xc3\xc5-
\xc7\xe8\xea\xeb\xed-\xef][\x04\x0e\x12\x17\xfc][\x03\x31\x83][\x42\x43\x45-\x47\x50\x53\x55-\x58\x5a\x5d-\x5f\x68\x6a\x6b\x6e-\x70\x72\x73\x75\x77\x78\x7a\x7b\x7d\x7e\xc0\xc2\xc3\xc5-
\xc7\xe8\xea\xeb\xed-\xef][\x04\x0a\x0e\x12\x13\x17\xfc][\x03\x83]..[^\xe2][^\xf5])/sm"; reference:url,toorcon.org/2006/conference.html?id=29;
reference:url,doc.emergingthreats.net/2003118; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/VIRUS_Polymorphic_Experimental; sid:2003118; rev:3;)

#These are by Vlad Tsyrklevich during presentation at Toorcon 06. These are experimental and will likely be high load.
#more information at http://toorcon.org/2006/conference.html?id=29
#These are disabled by default until we learn more about them.
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET VIRUS SHELLCODE ADMutate polymorphic payload"; classtype:shellcode-detect; dsize: >45; content: "|e8|"; content: "|ff ff ff|";
distance: 1; within: 3; pcre: "/\xeb[\x26-\x7a].{0,20}(\x5e|\x58\x96|\x58\x89\xc6|\x8b\x34\x24\x83\xec\x04).{0,20}(((\xbb....|\x68....\x5b).{0,20}(\x31\xc9|\x31\xc0\x91))|
((\x31\xc9|\x31\xc0\x91).{0,20}(\xbb....|\x68....\x5b))).{0,20}(\xb1.|\x6a.\x58\x89\xc1|\x6a.\x66\x59).{0,20}(\x31\x1e|\x93\x31\x06\x93|\x8b\x06\x09\xd8\x21\x1e\xf7\x16\x21\x06).{0,20}
(\x46|\x83\xc6\x01|\x96\x40\x96).{0,20}(\x46|\x83\xc6\x01|\x96\x40\x96).{0,20}(\x46|\x83\xc6\x01|\x96\x40\x96).{0,20}(\x46|\x83\xc6\x01|\x96\x40\x96).{0,20}\xe2[\xa0-\xf9].
{0,20}\xeb[\x06-\x20].{0,20}\xe8[\x7f-\xff]\xff\xff\xff/sm"; reference:url,toorcon.org/2006/conference.html?id=29; reference:url,doc.emergingthreats.net/2003119;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/VIRUS_Polymorphic_Experimental; sid:2003119; rev:3;)

#Sobig
#Unknown submitter - Sobig E-F downloading goodies
#
#alert udp $HOME_NET any -> $EXTERNAL_NET 8998 (msg:"ET VIRUS Sobig.E-F Trojan Site Download Request"; dsize: 8; content:"|5c bf 01 29 ca 62 eb f1|"; classtype: trojan-activity;
reference:url,securityresponse.symantec.com/avcenter/venc/data/w32.sobig.e@mm.html; reference:url,doc.emergingthreats.net/2001547; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/VIRUS_Sobig_Trojan_Download_Request; sid:2001547; rev:7;)

#Spy.Win32.Bancos Trojan
#Submitted by Matt Jonkman for Spy.Win32.Bancos Trojan
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET VIRUS Trojan-Spy.Win32.Bancos Download"; flow: established,from_server; content:"[AspackDie!]"; content:"|0f 6d 07 9e 6c
62 6c 68 00 d2 2f 63 6d 64 9d 11 af af 45 c7 72 ac 5f 3138 d0|"; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/pwsteal.bancos.b.html;
reference:url,doc.emergingthreats.net/2001726; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/VIRUS_Trojan-Spy.Win32.Bancos; sid:2001726; rev:8;)

#from sandnet data
#Disabling by default, hits on the VB api, not unique to this virus.
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS Bancos User-Agent Detected"; flow:established,to_server; content:"|0d 0a|User-Agent|3A| vb wininet"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2004114; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/VIRUS_Trojan-Spy.Win32.Bancos; sid:2004114;
rev:4;)

#from castlecops research, http://www.castlecops.com, sig by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET VIRUS AV-Killer.Win32 User Agent Detected (p4r4z1t3v3.one14.J)"; flow:established,to_server; content:"User-Agent|3a|
p4r4z1t3v3"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003638; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/VIRUS_Win32_AV-Killer;
sid:2003638; rev:4;)

#by mr Magic Pants
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET VIRUS Win32.SMTP-Mailer SMTP Outbound"; flow:to_server,established; content:"Subject|3a 20 3a 20|ZOMBIE"; nocase; content:"X-
Library|3a| Indy 9.00.10"; nocase; distance:0; classtype:trojan-activity; reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=Win32.SMTP-Mailer&threatid=48095;
reference:url,www.hauri.net/virus/virusinfo_read.php?code=TRW3000774&start=1; reference:url,doc.emergingthreats.net/2003041; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/VIRUS_Win32_Mailer; sid:2003041; rev:6;)

#by dn1nj4
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1433 (msg:"ET TROJAN Outbound AVISOSVB MSSQL Request"; flow:established,to_server; content:"|54 00 42 00 4c 00 5f 00 41 00 56 00 49 00 53 00 4f
00 53 00 56 00 42 00|"; classtype:trojan-activity; reference:url,www.threatexpert.com/report.aspx?md5=1f5b6d6d94cc6272c937045e22e6d192; reference:url,doc.emergingthreats.net/2011199;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_AVISOSVB; sid:2011199; rev:2;)

#by: Jeremy Conway at sudosecure.net
#ref: bbd144858cb1af3177a02900865d3134
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader Possible AV KILLER"; flow:established,to_server; content:"GET "; depth:4; uricontent:"SoftName="; nocase;
uricontent:"SoftVersion="; nocase; uricontent:"UserIP="; nocase; uricontent:"Mac="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009487;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_AVKiller; sid:2009487; rev:3;)
```

```
#by: Jeremy Conway at sudosecure.net
#ref: 01683fba555b59dac497a390e5afea47
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN AVKiller with Backdoor checkin"; flow:established,to_server; content:"POST "; depth:5; content:"|0d 0a 0d 0a|id=";
nocase; content:"&ip_int="; nocase; content:"&os="; nocase; content:"&av="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009812;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_AVKiller; sid:2009812; rev:2;)

#by: Jeremy Conway at sudosecure.net
#ref: cd3c73136661fea7e33ed41666953bc9
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET VIRUS Adware/Spyware Adrotator for Rogue AV"; flow:established,to_server; content:"GET "; depth:4;
uricontent:"nsi_install.php?"; nocase; uricontent:"aff_id="; nocase; uricontent:"&inst_result="; uricontent:"&id="; nocase; classtype:trojan-activity;
reference:url,www.spywaredetector.net/spyware_encyclopedia/Trojan.Vapsup.htm; reference:url,www.spywaredetector.net/spyware_encyclopedia/Fake AntiSpyware.POWER-ANTIVIRUS-2009.htm;
reference:url,www.threatexpert.com/threats/adware-agent-gen.html; reference:url,novirusthanks.org/blog/2008/11/rogue-antispyware-2009-served-through-beedlyus-ads/;
reference:url,doc.emergingthreats.net/2009548; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Adrotater; sid:2009548; rev:3;)

#by pedro marinho
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET DELETED Agent.END"; flow:to_server,established; content:"GET "; depth:4; uricontent:"idcomp="; uricontent:"&load1=";
uricontent:"&hist=downloaded_user_"; uricontent:"MyValue="; pcre:"/MyValue=[a-f0-9]{32}/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010243;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Agent.end; sid:2010243; rev:2;)

#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Alman Dropper Checkin"; flow:established,to_server; uricontent:"/info.asp?action=post&HD="; uricontent:"&OT=";
uricontent:"&IV="; uricontent:"&AV="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009203; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Alman; sid:2009203; rev:2;)

#by stillsecure
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN MSIL.Amiricil.gen HTTP Checkin"; flow:established,to_server; uricontent:"/registerSession.py?"; nocase;
uricontent:"proj="; nocase; uricontent:"&country="; nocase; uricontent:"&lang="; nocase; uricontent:"&channel="; nocase; uricontent:"source="; nocase; content:"|0d 0a|User-Agent|3a|
NSIS_Inetc (Mozilla)"; classtype:trojan-activity; reference:url,www.threatexpert.com/report.aspx?md5=af0bbdf6097233e8688c5429aa97bbed; reference:url,doc.emergingthreats.net/2011677;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Amiricil; sid:2011677; rev:3;)

#by matt jonkman, www.antispywareexpert.com
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Antispywareexpert.com Fake AS Install Checkin"; flow:established,to_server; uricontent:"/?action=";
uricontent:"&pc_id="; uricontent:"&abbr="; uricontent:"&a="; uricontent:"&l="; uricontent:"&addt"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008502;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Antispywareexpert.com; sid:2008502; rev:2;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Antispywaremaster.com Fake AV Checkin"; flow:established,to_server; uricontent:"?action="; uricontent:"&pc_id=";
uricontent:"&abbr="; uricontent:"&err="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008282; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Antispywaremaster.com; sid:2008282; rev:2;)

#by Pedro Marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32/Antivirus2008"; flow:established,to_server; uricontent:"nick="; nocase; uricontent:"&group="; nocase;
uricontent: "&os="; content:"User-Agent|3a 20|Mozilla|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008483; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Antivirus2008; sid:2008483; rev:5;)

#matt jonkman, re 0546aebf675cbb00f93c8040d394fa5f
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32/Antivirus2008 Fake AV Install Report"; flow:established,to_server; uricontent:"?type=scanner&pin=";
uricontent:"&lnd="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008511; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Antivirus2008;
sid:2008511; rev:2;)

#by dxp
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Armitage Exploit Request"; flow:established,to_server; content:"GET "; depth:4; uricontent:"/bof.php";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009032; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Armitage; sid:2009032; rev:3;)

#by dxp
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Armitage Loader Check-in"; flow:established,to_server; content:"GET "; depth:4; uricontent:"/lds.php";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009036; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Armitage; sid:2009036; rev:3;)

#by mareadmin
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 7777 (msg:"ET TROJAN Arucer Command Execution"; flow:established; content:"|C2 E5 E5 E5 9E DD A4 A3 D4 A6 D4 D3 D1 C8 A0 A7 A1 D3 C8 D1 87 D7
87 C8 A7 A6 D4 A3 C8 D3 D1 D3 D2 D1 A0 DC DD A4 D2 D4 D5 98 E5|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010909; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Arucer; sid:2010909; rev:2;)

#by mareadmin
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 7777 (msg:"ET TROJAN Arucer DIR Listing"; flow:established; content:"|C2 E5 E5 E5 9E D5 D4 D2 D1 A1 D7 A3 A6 C8 D2 A6 A7 D3 C8 D1 84 D7 D7 C8
DD D2 A6 D2 C8 D2 A7 A7 D2 D7 A4 D6 D7 A3 D4 DC A3 98 E5|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010910; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Arucer; sid:2010910; rev:2;)

#by mareadmin
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 7777 (msg:"ET TROJAN Arucer WRITE FILE command"; flow: established; content:"|C2 E5 E5 E5 9E DC DD A1 DC D0 DD A3 A6 C8 A1 D5 A4 D7 C8 D1 83 D4
86 C8 A7 DD D1 D4 C8 D7 D6 D7 A4 A7 D6 D0 D2 A0 D2 A6 DD 98 E5|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010911; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Arucer; sid:2010911; rev:2;)

#by mareadmin
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 7777 (msg:"ET TROJAN Arucer READ FILE Command"; flow:established; content:"|C2 E5 E5 E5 9E A3 D3 A6 D1 D6 A0 D4 A4 C8 D4 D0 D0 D4 C8 D1 D5 D5
D5 C8 A4 D1 DD D6 C8 A6 D6 D3 D4 DC D3 DC A4 A0 A6 D1 D4 98 E5|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010912; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Arucer; sid:2010912; rev:2;)

#by mareadmin
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 7777 (msg:"ET TROJAN Arucer NOP Command"; flow:established; content:"|C2 E5 E5 E5 9E D2 DD D6 A0 A4 A6 A7 A3 C8 A0 A3 DD A7 C8 D1 DC DD 80 C8 A4
D5 D0 DC C8 A3 D5 A7 D0 A7 A1 D4 D7 D3 D1 D4 A0 98 E5|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010913; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Arucer; sid:2010913; rev:2;)

#by mareadmin
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 7777 (msg:"ET TROJAN Arucer FIND FILE Command"; flow:established; content:"|C2 E5 E5 E5 9E A0 A4 D2 A4 D7 A0 A7 D2 C8 D4 A0 D1 DC C8 D1 81 D0
83 C8 A7 D1 A1 DD C8 A1 D3 D3 D1 D0 A7 D2 D1 D1 D5 A0 D6 98 E5|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010914; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Arucer; sid:2010914; rev:2;)

#by mareadmin
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 7777 (msg:"ET TROJAN Arucer YES Command"; flow:established; content:"|C2 E5 E5 E5 9E A0 D7 A4 A6 D0 D5 DD DC C8 D6 DD D7 D5 C8 D1 D6 83 80 C8
DD A4 D1 A1 C8 A4 D2 D5 D7 DD A3 A4 A1 DD A6 D7 DD 98 E5|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010915; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Arucer; sid:2010915; rev:2;)

#by mareadmin
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 7777 (msg:"ET TROJAN Arucer ADD RUN ONCE Command"; flow:established; content:"|C2 E5 E5 E5 9E D6 DD D1 A0 A7 A0 D7 A6 C8 A3 DC A0 A4 C8 D1 83
D3 87 C8 DC D1 A0 A3 C8 A6 DC A1 D7 A1 A4 D0 DD A3 A1 D4 D6 98 E5|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010916; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Arucer; sid:2010916; rev:2;)
```

```
#by mareadmin
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 7777 (msg:"ET TROJAN Arucer DEL FILE Command"; flow:established; content:"|C2 E5 E5 E5 9E D1 A3 D1 A3 D5 A1 DD DD C8 A0 D2 D4 D0 C8 D1 87 D4 83
C8 A7 D6 D4 D4 C8 D3 D4 A0 D0 D6 D5 A6 D7 A6 DD A3 A6 98 E5|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010917; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Arucer; sid:2010917; rev:2;)

#by Daniel Clemens
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN ASProtect/ASPack Packed Binary - Likely Hostile"; flow:from_server,established; content:"|2E 72 73 72 63|";
content:"|2E 61 73 70 61 63 6B|"; within: 50; classtype:trojan-activity; reference:url,www.aspack.com/downloads.aspx; reference:url,bits.packetninjas.org/eblog/;
reference:url,doc.emergingthreats.net/2008575; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Asprotect_Packed; sid:2008575; rev:2;)

#by Joe Stewart of Secureworks
#
#alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"ET TROJAN Asprox-style Message ID"; flow:established,to_server; dsize:<80; content:"Message-ID|3a20|"; depth:12; content:"|0d0a|";
within: 68; flowbits:set,ET.asproxmessageid; flowbits:noalert; classtype: trojan-activity; reference:url,www.secureworks.com/research/threats/danmecasprox;
reference:url,doc.emergingthreats.net/2008221; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Asprox; sid:2008221; rev:4;)

#by Joe Stewart of Secureworks
#
#alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"ET TROJAN Asprox phishing email detected"; flow:established,to_server; content:"From|3a20|"; depth:6; content:"|0d0a|Bcc|3a20|";
within:150; flowbits:isset,ET.asproxmessageid; classtype: trojan-activity; reference:url,www.secureworks.com/research/threats/danmecasprox;
reference:url,doc.emergingthreats.net/2008222; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Asprox; sid:2008222; rev:4;)

#by dxp
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Asprox Form Submission to C&C"; flow:established,to_server; content:"POST "; depth:5; uricontent:"/forum.php";
nocase; content:"Content-Type|3a| multipart/form-data|3b| boundary=1BEF0A57BE110FD467A"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009054;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Asprox; sid:2009054; rev:3;)

#by darren spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Asprox Data Post to C&C"; flow:established,to_server; content:"POST "; depth:5; content:"name=|22|sid|22 0d 0a 0d
0a|"; nocase; content:"name=|22|upt|22 0d 0a 0d 0a|"; nocase; content:"name=|22|hcc|22 0d 0a 0d 0a|"; nocase; classtype:trojan-activity;
reference:url,www.secureworks.com/research/threats/danmecasprox/; reference:url,www.toorcon.org/tcx/18_Brown.pdf; reference:url,doc.emergingthreats.net/2010270;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Asprox; sid:2010270; rev:2;)

#Matt Jonkman
#re c6f326609487aaae451366728ec5cdd9
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 91 (msg:"ET TROJAN Backdoor.Win32.Assasin.20.C Control Session Start"; flow:established,to_server; content:"11000"; depth:5; content:"^";
distance:4; within:5; flowbits:isnotset,ET.assassin.start; flowbits:set,ET.assassin.start; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008675;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Assassin; sid:2008675; rev:4;)

#Matt Jonkman
#re c6f326609487aaae451366728ec5cdd9
#
#alert tcp $EXTERNAL_NET 91 -> $HOME_NET any (msg:"ET TROJAN Backdoor.Win32.Assasin.20.C Control Session Server Reply"; flowbits:isset,ET.assassin.start; flow:established,from_server;
dsize:12; content:"10000002|5e 2a|"; depth:10; flowbits:set,ET.assassin.reply; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008676;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Assassin; sid:2008676; rev:4;)

#Matt Jonkman
#re c6f326609487aaae451366728ec5cdd9
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 91 (msg:"ET TROJAN Backdoor.Win32.Assasin.20.C Control Channel Client Reply"; flow:established,to_server; dsize:10; content:"10000000|5e 2a|";
flowbits:isset,ET.assassin.reply; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008677; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Assassin; sid:2008677; rev:4;)

#by: Jeremy Conway at sudosecure.net
#ref: 8a8f0708b05e0177acc4c57a09c70790 c42c3b5c832ac87221bb5ac88ed3feb7
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Atya Dropper Possible Rootkit - HTTP GET"; flow:established,to_server; content:"GET "; depth:4; uricontent:"b=";
nocase; uricontent:"&idf="; nocase; uricontent:"&v="; nocase; uricontent:"&o="; nocase; classtype:trojan-activity; reference:url,www.paretologic.com/resources/definitions.aspx?
remove=%41%67%65%6e%74%20%41%74%79%61%20%54%72%6f%6a%61%6e; reference:url,doc.emergingthreats.net/2009450; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Atya; sid:2009450; rev:2;)

#by Jaime Blasco at alienvault and matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 443 (msg:"ET TROJAN Aurora Backdoor (C&C) client connection to CnC"; flow:established,to_server; content:"|ff ff ff ff ff ff 00 00 fe ff ff ff
ff ff ff ff ff 88 ff|"; depth:20; flowbits:set,ET.aurora.init; classtype:trojan-activity; reference:url,www.trustedsource.org/blog/373/An-Insight-into-the-Aurora-Communication-
Protocol; reference:url,doc.emergingthreats.net/2010695; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Aurora; sid:2010695; rev:2;)

#by Jaime Blasco at alienvault and matt jonkman
#
alert tcp $EXTERNAL_NET 443 -> $HOME_NET any (msg:"ET TROJAN Aurora Backdoor (C&C) connection CnC response"; flowbits:isset,ET.aurora.init; flow:established,from_server; content:"|cc cc
cc cc cd cc cc cc cd cc cc cc cc cc cc cc cc|"; depth:16; classtype:trojan-activity; reference:url,www.trustedsource.org/blog/373/An-Insight-into-the-Aurora-Communication-Protocol;
reference:url,doc.emergingthreats.net/2010696; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Aurora; sid:2010696; rev:2;)

#by Jaime Blasco at alienvault and matt jonkman
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Autorun.qvi Related HTTP Get on Off Port"; flow:established,to_server; content:"GET /get_r.php?fid="; depth:19;
content:"&mac="; distance:0; within:15; content:"&version="; distance:0; content:"&uuid="; distance:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008755;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Autorun; sid:2008755; rev:2;)

#by: Jeremy Conway at sudosecure.net
#ref: 5af1c119ba1818099b4e4915f5bb15e9
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Generic Win32.Autorun HTTP Post"; flow:established,to_server; content:"POST "; depth:5; uricontent:"cbID="; nocase;
uricontent:"cbVer="; nocase; uricontent:"cbTit="; nocase; content:!"User-Agent\:"; nocase; content:"cbBody="; nocase; classtype:trojan-activity;
reference:url,www.threatexpert.com/threats/worm-win32-autorun.html; reference:url,doc.emergingthreats.net/2009516; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Autorun; sid:2009516; rev:2;)

#General BHOs and the like
#by Jeremy at Sudosecure
#ref: a2404de3a35a263d775ceb451173f304
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Rouge Security Software Win32.BHO.egw"; flow:established,to_server; content:"GET "; depth:4; uricontent:".php?";
nocase; uricontent:"affid="; nocase; uricontent:"subid="; nocase; uricontent:"guid="; nocase; uricontent:"ver="; nocase; uricontent:"key="; nocase; classtype:trojan-activity;
reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=Trojan.Win32.BHO.egw&threatid=313636; reference:url,doc.emergingthreats.net/2008461;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_BHO; sid:2008461; rev:2;)

#by Marcus at unsober
#ref: 30b2cc13a86a15396a25e89c2860351d
#
alert udp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Backdoor Possible Backdoor.Cow Varient (Backdoor.Win32.Agent.lam) C&C traffic"; content:"|6C 3C|"; depth:2; content:"|3E
20|"; within:3; content:"bid="; nocase; within:20; content:"bver="; nocase; within:20; content:"bip="; nocase; within:20; content:"bn="; nocase; within:20; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008465; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Backdoor.Cow; sid:2008465; rev:2;)

#by Pedro Marinho
#re 4bde1bc2f7b6d4e11b1a570aaa52df57
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Backdoor.Win32.Agent.fvt Checkin"; flow:established,to_server; content:"GET "; depth:4; content:".php?"; nocase;
content:"lversion="; nocase; content:"wversion=&eversion=&fid="; nocase; content:"&mac="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008667;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Backdoor.General; sid:2008667; rev:3;)

#matt jonkman, re 1f8169a4694ec450a9f247469b7cbaf4
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN General Win32 Backdoor Checkin POST Packet 1"; flow:established,to_server; uricontent:"/add.php"; content:"|0d
0a|User-Agent|3a| Mozilla/4.0 (compatible|3b| MSIE 6.0|3b| Windows NT 5.1|3b| SV1)|0d 0a|"; flowbits:noalert; flowbits:set,ET.bd1; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2009240; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Backdoor.General; sid:2009240; rev:3;)

#matt jonkman, re 1f8169a4694ec450a9f247469b7cbaf4
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN General Win32 Backdoor Checkin POST"; flow:established,to_server; content:"|0d 0a 0d 0a|Admin="; depth:10;
content:"&UserName="; distance:0; within:25; content:"&IsProxy="; distance:0; within:50; flowbits:isset,ET.bd1; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009241;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Backdoor.General; sid:2009241; rev:2;)

#Matt Jonkman, analysis from captured binary
#Don't know a lot about this one. But the control session is apparently opened by a 00 00 00 00
#Then the bot replies with a packet that begins with the date in form such as 20060622, and
#among other things contains the host OS info.
#Since this is a windos bot, we can assume the word windows will be in there.
#Hopefully we can update these as more is learned. This is sorta crude, but should
#be reliable to not false pos at least....
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 8000 (msg:"ET TROJAN Backdoor.Hupigon Possible Control Connection Being Established"; flow:established,to_server; dsize:4; content:"|00 00 00
00|"; flowbits:set,BSHupigonControlStart; classtype:trojan-activity; reference:url,www.avira.com/en/threats/section/fulldetails/id_vir/1051/bds_hupigon.bo.html;
reference:url,doc.emergingthreats.net/2002974; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Backdoor.Hupigon; sid:2002974; rev:3;)

#Matt Jonkman, analysis from captured binary
#Don't know a lot about this one. But the control session is apparently opened by a 00 00 00 00
#Then the bot replies with a packet that begins with the date in form such as 20060622, and
#among other things contains the host OS info.
#Since this is a windos bot, we can assume the word windows will be in there.
#Hopefully we can update these as more is learned. This is sorta crude, but should
#be reliable to not false pos at least....
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 8000 (msg:"ET TROJAN Backdoor.Hupigon INFECTION - Reporting Host Type"; flow:established,to_server; flowbits:isset,BSHupigonControlStart;
content:"Windows "; flowbits:isset,BSHupigonControlStart; classtype:trojan-activity; reference:url,www.avira.com/en/threats/section/fulldetails/id_vir/1051/bds_hupigon.bo.html;
reference:url,doc.emergingthreats.net/2002975; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Backdoor.Hupigon; sid:2002975; rev:3;)

#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Backdoor.Win32.VB.cfi (related) System Info Upload via FTP"; flow:established,to_server; content:"**********CD-Key
Pack**********"; content:"|0d 0a|Microsoft Windows Product ID CD Key|3a|"; distance:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008005;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Backdoor.VB.cfi; sid:2008005; rev:4;)

#by Scott Melnick
#
alert tcp $HOME_NET !$HTTP_PORTS -> $EXTERNAL_NET 1337 (msg:"ET TROJAN Win32.SkSocket C&C Connection"; flow:established,to_server; flags:PA,12; dsize:1; content:"|04|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007585; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Backdoor.Win32.SkSocket;
sid:2007585; rev:4;)

#by matt jonkman and victor julien
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Backdoor.Win32.VB.brg C&C Checkin"; flow:established,to_server; content:"Status|2a 28|Idle|2e 2e 2e 29 2a|"; depth:17;
offset:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007922; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Backdoor.Win32.VB;
sid:2007922; rev:5;)

#by matt jonkman and victor julien
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Backdoor.Win32.VB.brg C&C Reporting Version"; flow:established,to_server; content:"Version|28 2a|"; depth:9; offset:0;
content:"|29 2a|"; within:8; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007979; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Backdoor.Win32.VB; sid:2007979; rev:5;)

#by matt jonkman and victor julien
#
alert tcp $EXTERNAL_NET 1024: -> $HOME_NET any (msg:"ET TROJAN Backdoor.Win32.VB.brg C&C Kill Command Send"; flow:established,from_server; dsize:<35; content:"kill-"; offset:0; depth:5;
pcre:"/kill\-\d+.\d+.\d+.\d+\:\d+%\d+/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007980; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Backdoor.Win32.VB; sid:2007980; rev:3;)

#by matt jonkman and victor julien
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Backdoor.Win32.VB.brg C&C Kill Command Acknowledge"; flow:established,to_server; dsize:29; content:"Status|28 2a|UDP
Attack Running!|2a 28|"; offset:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007981; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Backdoor.Win32.VB; sid:2007981; rev:4;)

#by matt jonkman and victor julien
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Backdoor.Win32.VB.brg C&C DDoS Outbound"; flow:established,from_server; dsize:>100; content:"|ff ff ff ff|"; depth:4;
content:" own you bitch!"; within:20; content:"|01 01 01 01 01 01 01 01 01 01 01 01 01 01|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007982;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Backdoor.Win32.VB; sid:2007982; rev:3;)

#matt jonkman, re 0ec9e59de960ec4a7d585a9ad7fc5719
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Backdoor.Win32.VB.fdi Bot Reporting to Controller"; flow:established,to_server; content:"state|3a| 0 - zombie is ready for
control"; depth:38; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008507; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Backdoor.Win32.VB; sid:2008507; rev:3;)

#by Jeremy of sudosecure
#ref: 82b9407337a991b52daffd0078d02e6a
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banker/Banbra Variant POST via x-www-form-urlencoded"; flow:established,to_server; uricontent:".php"; content:"POST
"; depth:5; content:"|0D0A|Content-Type|3a20|application/x-www-form-urlencoded|0D0A|Content-Length|3A20|"; depth:150; nocase; content:"from="; nocase; content:"|26|FromMail="; nocase;
content:"|26|destino="; nocase; content:"|26|assunto="; nocase; content:"|26|mensagem="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008331;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banbra; sid:2008331; rev:3;)

#Matt jonkman, re 0d3ff9cfa6b1d6a8aeabaf0d73e1fc5c
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banker/Banbra Related HTTP Post-infection Checkin"; flow:established,to_server; content:"POST "; depth:5;
content:"|0d 0a 0d 0a|tipo=cli&cli="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009296; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banbra; sid:2009296; rev:2;)

#by Matt Jonkman
#Bandook 1.2
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024:65535 (msg:"ET TROJAN Bandook v1.2 Initial Connection and Report"; flowbits:isnotset,BE.Bandook1.2; flow:established,to_server;
content:"&first& # "; pcre:"/# \d+d \d+dh \d+m # /iR"; classtype:trojan-activity; flowbits:set,BE.Bandook1.2; reference:url,www.nuclearwintercrew.com; reference:url,research.sunbelt-
software.com/threatdisplay.aspx?name=Bandook&threatid=40408; reference:url,doc.emergingthreats.net/bin/view/Main/TrojanBandook; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bandook; sid:2003549; rev:5;)

#by Matt Jonkman
#Bandook 1.2
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024:65535 (msg:"ET TROJAN Bandook v1.2 Get Processes"; flowbits:isset,BE.Bandook1.2; flow:established,to_server; dsize:8; content:"|99 9b 86
8a 85 80 9a 9d|"; classtype:trojan-activity; reference:url,www.nuclearwintercrew.com; reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=Bandook&threatid=40408;
reference:url,doc.emergingthreats.net/bin/view/Main/TrojanBandook; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bandook; sid:2003550; rev:5;)

#by Matt Jonkman
#Bandook 1.2
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024:65535 (msg:"ET TROJAN Bandook v1.2 Kill Process Command"; flowbits:isset,BE.Bandook1.2; flow:established,to_server; dsize:>8;
```

```
content:"kill3d"; offset:0; depth:6; classtype:trojan-activity; reference:url,www.nuclearwintercrew.com; reference:url,research.sunbelt-software.com/threatdisplay.aspx?
name=Bandook&threatid=40408; reference:url,doc.emergingthreats.net/bin/view/Main/TrojanBandook; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bandook;
sid:2003551; rev:5;)

#by Matt Jonkman
#Bandook 1.2
#
#alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET any (msg:"ET TROJAN Bandook v1.2 Reporting Socks Proxy Active"; flowbits:isset,BE.Bandook1.2; flow:established,from_server; dsize:7;
content:"sockson"; offset:0; classtype:trojan-activity; reference:url,www.nuclearwintercrew.com; reference:url,research.sunbelt-software.com/threatdisplay.aspx?
name=Bandook&threatid=40408; reference:url,doc.emergingthreats.net/bin/view/Main/TrojanBandook; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bandook;
sid:2003552; rev:5;)

#by Matt Jonkman
#Bandook 1.2
#
#alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET any (msg:"ET TROJAN Bandook v1.2 Reporting Socks Proxy Off"; flowbits:isset,BE.Bandook1.2; flow:established,from_server; dsize:8;
content:"socksoff"; offset:0; classtype:trojan-activity; reference:url,www.nuclearwintercrew.com; reference:url,research.sunbelt-software.com/threatdisplay.aspx?
name=Bandook&threatid=40408; reference:url,doc.emergingthreats.net/bin/view/Main/TrojanBandook; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bandook;
sid:2003553; rev:5;)

#by Matt Jonkman
#Bandook 1.2
#
#alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET any (msg:"ET TROJAN Bandook v1.2 Client Ping Reply"; flowbits:isset,BE.Bandook1.2; flow:established,from_server; dsize:10;
content:"&SEXREPLY&"; offset:0; classtype:trojan-activity; reference:url,www.nuclearwintercrew.com; reference:url,research.sunbelt-software.com/threatdisplay.aspx?
name=Bandook&threatid=40408; reference:url,doc.emergingthreats.net/bin/view/Main/TrojanBandook; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bandook;
sid:2003554; rev:5;)

#Bandook 1.35
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024:65535 (msg:"ET TROJAN Bandook v1.35 Initial Connection and Report"; flowbits:isnotset,BE.Bandook1.35; flow:established,to_server;
content:"|cf 8f|"; offset:0; depth:2; content:"|20 26 26 26|"; distance:50; classtype:trojan-activity; flowbits:set,BE.Bandook1.35; reference:url,www.nuclearwintercrew.com;
reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=Bandook&threatid=40408; reference:url,doc.emergingthreats.net/bin/view/Main/TrojanBandook;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bandook; sid:2003555; rev:5;)

#Bandook 1.35
#
alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET any (msg:"ET TROJAN Bandook v1.35 Keepalive Send"; flowbits:isset,BE.Bandook1.35; flow:established,from_server; dsize:6; content:"|cf ab
a8 a7 ae cf|"; offset:0; classtype:trojan-activity; reference:url,www.nuclearwintercrew.com; reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=Bandook&threatid=40408;
reference:url,doc.emergingthreats.net/bin/view/Main/TrojanBandook; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bandook; sid:2003556; rev:5;)

#Bandook 1.35
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024:65535 (msg:"ET TROJAN Bandook v1.35 Keepalive Reply"; flowbits:isset,BE.Bandook1.35; flow:established,to_server; dsize:9; content:"|cf ab
a8 a4 ae cf 26 26 26|"; offset:0; classtype:trojan-activity; reference:url,www.nuclearwintercrew.com; reference:url,research.sunbelt-software.com/threatdisplay.aspx?
name=Bandook&threatid=40408; reference:url,doc.emergingthreats.net/bin/view/Main/TrojanBandook; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bandook;
sid:2003557; rev:5;)

#Bandook 1.35
#
alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET any (msg:"ET TROJAN Bandook v1.35 Create Registry Key Command Send"; flowbits:isset,BE.Bandook1.35; flow:established,from_server;
dsize:>10; content:"|cf 9b 8c 8e 8a 9b cf|"; offset:0; depth:7; content:"|95|"; distance:5; classtype:trojan-activity; reference:url,www.nuclearwintercrew.com;
reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=Bandook&threatid=40408; reference:url,doc.emergingthreats.net/bin/view/Main/TrojanBandook;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bandook; sid:2003558; rev:5;)

#Bandook 1.35
#
alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET any (msg:"ET TROJAN Bandook v1.35 Create Directory Command Send"; flowbits:isset,BE.Bandook1.35; flow:established,from_server; dsize:>7;
content:"|cf 84 82 8d 80 9b cf 95|"; offset:0; depth:8; classtype:trojan-activity; reference:url,www.nuclearwintercrew.com; reference:url,research.sunbelt-
software.com/threatdisplay.aspx?name=Bandook&threatid=40408; reference:url,doc.emergingthreats.net/bin/view/Main/TrojanBandook; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bandook; sid:2003559; rev:5;)

#Bandook 1.35
#
alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET any (msg:"ET TROJAN Bandook v1.35 Window List Command Send"; flowbits:isset,BE.Bandook1.35; flow:established,from_server; dsize:10;
content:"|cf 8e 80 84 84 8c 9e 80 87 cf|"; offset:0; classtype:trojan-activity; reference:url,www.nuclearwintercrew.com; reference:url,research.sunbelt-software.com/threatdisplay.aspx?
name=Bandook&threatid=40408; reference:url,doc.emergingthreats.net/bin/view/Main/TrojanBandook; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bandook;
sid:2003560; rev:5;)

#Bandook 1.35
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024:65535 (msg:"ET TROJAN Bandook v1.35 Window List Reply"; flowbits:isset,BE.Bandook1.35; flow:established,to_server; dsize:>10; content:"|cf
9e 80 87 85 80 9a 9d cf|"; offset:0; depth:9; content:"|26 26 26|"; distance:10; classtype:trojan-activity; reference:url,www.nuclearwintercrew.com; reference:url,research.sunbelt-
software.com/threatdisplay.aspx?name=Bandook&threatid=40408; reference:url,doc.emergingthreats.net/bin/view/Main/TrojanBandook; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bandook; sid:2003561; rev:5;)

#Bandook 1.35
#
alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET any (msg:"ET TROJAN Bandook v1.35 Get Processes Command Send"; flowbits:isset,BE.Bandook1.35; flow:established,from_server; dsize:8;
content:"|99 9b 86 8a 85 80 9a 9d|"; offset:0; classtype:trojan-activity; reference:url,www.nuclearwintercrew.com; reference:url,research.sunbelt-software.com/threatdisplay.aspx?
name=Bandook&threatid=40408; reference:url,doc.emergingthreats.net/bin/view/Main/TrojanBandook; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bandook;
sid:2003562; rev:5;)

#Bandook 1.35
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024:65535 (msg:"ET TROJAN Bandook v1.35 Get Processes Command Reply"; flowbits:isset,BE.Bandook1.35; flow:established,to_server; dsize:>10;
content:"|cf 9d 82 99 9b 86 8a cf|"; offset:0; depth:8; content:"|26 26 26|"; distance:10; classtype:trojan-activity; reference:url,www.nuclearwintercrew.com;
reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=Bandook&threatid=40408; reference:url,doc.emergingthreats.net/bin/view/Main/TrojanBandook;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bandook; sid:2003565; rev:5;)

#Bandook 1.35
#
alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET any (msg:"ET TROJAN Bandook v1.35 Start Socks5 Proxy Command Send"; flowbits:isset,BE.Bandook1.35; flow:established,from_server;
dsize:>6; content:"|a7 a0 a7 ae 95|"; offset:0; depth:5; classtype:trojan-activity; reference:url,www.nuclearwintercrew.com; reference:url,research.sunbelt-
software.com/threatdisplay.aspx?name=Bandook&threatid=40408; reference:url,doc.emergingthreats.net/bin/view/Main/TrojanBandook; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bandook; sid:2003563; rev:5;)

#Bandook 1.35
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024:65535 (msg:"ET TROJAN Bandook v1.35 Socks5 Proxy Start Command Reply"; flowbits:isset,BE.Bandook1.35; flow:established,to_server; dsize:10;
content:"|9a 86 8a 82 9a 86 87 26 26 26|"; offset:0; classtype:trojan-activity; reference:url,www.nuclearwintercrew.com; reference:url,research.sunbelt-software.com/threatdisplay.aspx?
name=Bandook&threatid=40408; reference:url,doc.emergingthreats.net/bin/view/Main/TrojanBandook; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bandook;
sid:2003564; rev:5;)

#by Joe Stewart
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024:65535 (msg:"ET TROJAN Bandok phoning home (xor by 0xe9 to decode)"; flow:established,to_server; content:"|CF 8F 80 9B 9A 9D CF 95|";
depth:8; dsize:<80; classtype:trojan-activity; reference:url,www.dshield.org/diary.html?date=2007-03-28; reference:url,www.secureworks.com/research/threats/bbbphish/?threat=bbbphish;
reference:url,doc.emergingthreats.net/2003936; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bandook; sid:2003936; rev:4;)

#by Joe Stewart
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Bandook iwebho/BBB-phish trojan leaking user data"; flow:established,to_server; content:"POST|20|/"; depth:6;
content:"|20|HTTP/1.1|0d0a|Content-Type|3a20|application/x-www-form-urlencoded|0d0a|Host|3a20|"; within:150; content:"Content-Length|3a20|"; within:100; content:"|0d0a0d0a|"; within:12;
content:"VISITED_URL"; within:100; classtype:trojan-activity; reference:url,www.secureworks.com/research/threats/bbbphish; reference:url,doc.emergingthreats.net/2003937;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bandook; sid:2003937; rev:4;)

#by Matt Jonkman
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banker.OT Checkin"; flow:established,to_server; content:"POST "; depth:5; content:"User-Agent|3a| Mozilla/3.0
(compatible|3b| Indy Library)|0d 0a 0d 0a|praquem="; content:"&titulo="; content:"&texto="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007823;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banker.General; sid:2007823; rev:3;)

#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banker.OT Checkin (2 packet)"; flow:established,to_server; content:"praquem="; depth:8; content:"&titulo=";
content:"&texto="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008491; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banker.General;
sid:2008491; rev:2;)

#A different one, by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banker.anv Generally Suspicious User-Agent (CustomExchangeBrowser)"; flow:established,to_server; content:"|0d
0a|User-Agent|3a| "; content:"CustomExchangeBrowser"; pcre:"/User-Agent\:[^\n]+CustomExchangeBrowser/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007824;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banker.General; sid:2007824; rev:3;)

#Banker.OPX, by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Banker.OPX HTTP Checkin"; flow:established,to_server; content:"POST "; depth:5; content:"|0d 0a 0d 0a|TIPO=CLIENTE&NOME=";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007901; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banker.General; sid:2007901;
rev:3;)

#Banker.ili by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banker.ili HTTP Checkin"; flow:established,to_server; uricontent:"/ctrl/cnt_boot.php?pgv="; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007940; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banker.General; sid:2007940; rev:2;)

#Banker.ili by matt jonkman
#
alert udp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Banker.ike UDP C&C"; content:"|86 71 3b 72 50 61 7d 95 5f 61 46|"; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2007957; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banker.General; sid:2007957; rev:2;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banker Trojan (General) HTTP Checkin"; flow:established,to_server; uricontent:".php?PC="; uricontent:"&Data=";
uricontent:"&Mac="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007984; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banker.General;
sid:2007984; rev:2;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banker Trojan (General) HTTP Checkin (vit)"; flow:established,to_server; uricontent:".php"; content:"|0d 0a|User-
Agent|3a| Mozilla/3.0 (compatible|3b| Indy Library)|0d 0a|"; content:"vit="; nocase; content:"&bk="; nocase; content:"&dados="; nocase; distance:0; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2007999; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banker.General; sid:2007999; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN Banker.maf SMTP Checkin (Not in the Control...)"; flow:established,to_server; content:"|0a|X-Mailer|3a| Microsoft CDO for
Windows 2000"; content:"|0d 0a|_-=|7c| Not in the Control System 6.0 |7c|=-_|0d 0a|.|0d 0a|"; distance:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008033;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banker.General; sid:2008033; rev:5;)

#matt jonkman, banker.JU
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banker.JU Related HTTP Post-infection Checkin"; flow:established,to_server; uricontent:"/envio.php?"; content:"|0d
0a|User-Agent|3a| Mozilla/3.0 (compatible|3b| Indy Library)|0d 0a 0d 0a|tipo="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008267;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banker.General; sid:2008267; rev:3;)

#by pmarinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Agent.zrm/Infostealer.Bancos Checkin"; flow:established,to_server; content:"GET "; depth:4;
uricontent:"appdata="; nocase; uricontent:"hd="; nocase; uricontent:"mac="; nocase; uricontent:"computador="; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008519; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banker.General; sid:2008519; rev:2;)

#by cjeremy
#ref: 8dce7edf84300fbc258c94ce4b47a366
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Generic Banker Trojan Downloader Config to client"; flow:established,to_client; content:"[Controlinfo]"; nocase;
depth:13; content:"CntInfo="; within:9; nocase; content:"UseSepControl="; within:30; nocase; content:"Names="; within:20; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2009090; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banker.General; sid:2009090; rev:2;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN General Banker.PWS POST Checkin"; flow:established,to_server; content:"POST "; depth:5; content:"|0d 0a|User-
Agent|3a| Mozilla/3.0 (compatible|3b| Indy Library)|0d 0a 0d 0a|IDMAQUINA="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009127;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banker.General; sid:2009127; rev:3;)

#by Dan Clemens
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN PWSteal.Bancos Generic Banker Trojan SCR Download"; flow:to_server,established; uricontent:"/keylogf.jpg"; nocase;
classtype:trojan-activity; reference:url,www.symantec.com/security_response/writeup.jsp?docid=2005-050210-0214-99&tabid=2; reference:url,www.packetninjas.net;
reference:url,doc.emergingthreats.net/2009235; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banker.General; sid:2009235; rev:4;)

#by: Joe Stewart at SecureWorks
#ref: cfcdf7c9066dfab0dcca1683603e4ee6
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN TSPY_BANKER.IDV/Infostealer.Bancos Module Download"; flow:established,to_server; content:"GET|20|/"; depth:5;
content:"| 0d0a|User-Agent|3a20|Mozilla|2f|4.0|2028|compatible|3b20|MSIE|20|6.0| 3b2020|Windows|20|NT|20|5.1|3b20|SV1|3b20|.NET|20|CLR|20|1.1.4322|
3b20|.NET|20|CLR|20|2.0.50727|290d0a|Host|3a20|"; content:"|0d0a|Accept|3a202a2f2a|"; within:80; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009447;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banker.General; sid:2009447; rev:3;)

#by: Jeremy Conway at sudosecure.net
#ref: 43347bed87a3427b97a8a4bb50d3f06c
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Bancos/Banker Info Stealer Post"; flow:established,to_server; content:"POST "; depth:5; content:"|0d 0a|User-
Agent|3a| Mozilla/3.0 (compatible|3b| Indy Library)"; nocase; content:"op="; nocase; content:"servidor="; nocase; content:"senha="; nocase; content:"usuario="; nocase; content:"base=";
nocase; content:"sgdb="; nocase; classtype:trojan-activity; reference:url,www.pctools.com/mrc/infections/id/Trojan.Bancos/; reference:url,www.threatexpert.com/reports.aspx?
find=Trojan.Bancos; reference:url,doc.emergingthreats.net/2009471; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banker.General; sid:2009471; rev:3;)

#by: Jeremy Conway at sudosecure.net
#ref: db255a75745f90e2f1cb807c35d752b0
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banker PWS/Infostealer HTTP GET Checkin"; flow:established,to_server; content:"GET "; depth:4; content:"|0d 0a|User-
Agent|3a| Microsoft Internet Explorer|0d 0a|"; nocase; uricontent:"guid="; nocase; uricontent:"ver="; nocase; uricontent:"stat="; nocase; uricontent:"ie="; nocase; uricontent:"os=";
nocase; uricontent:"ut="; nocase; uricontent:"cpu="; nocase; classtype:trojan-activity; reference:url,www.pctools.com/mrc/infections/id/Trojan.Banker/;
reference:url,doc.emergingthreats.net/2009550; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banker.General; sid:2009550; rev:3;)

#by: Jeremy Conway at sudosecure.net
#ref: 45545f7afce0b3e9d02a9a04ff374dc6
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banker/Bancos/Infostealer Possible Rootkit - HTTP HEAD Request"; flow:established,to_server; content:"HEAD ";
nocase; depth:5; uricontent:".php?action="; nocase; uricontent:"&uid="; nocase; uricontent:"&locale="; nocase; uricontent:"&ver="; nocase; uricontent:"&build="; nocase;
classtype:trojan-activity; reference:url,www.pctools.com/mrc/infections/id/Trojan.Banker/; reference:url,www.anti-spyware-101.com/remove-trojanbanker;
reference:url,doc.emergingthreats.net/2009750; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banker.General; sid:2009750; rev:2;)

#matt jonkman
#banker trojan with a custom cnc
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Banker Trojan CnC AddNew Command"; flow:established,to_server; dsize:<120; content:"[S]ADDNEW|7c|"; depth:10;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009862; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banker.General; sid:2009862; rev:3;)

#matt jonkman
#banker trojan with a custom cnc
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Banker Trojan CnC Hello Command"; flow:established,to_server; dsize:12; content:"[S]hello["; depth:9; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/2009863; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banker.General; sid:2009863; rev:3;)

#matt jonkman
#banker trojan with a custom cnc
#
alert tcp $EXTERNAL_NET 1024: -> $HOME_NET any (msg:"ET TROJAN Banker Trojan CnC Server Ping"; flow:established,from_server; dsize:5; content:"PING|7c|"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2009864; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banker.General; sid:2009864; rev:3;)

#by Darren Spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Patcher/Bankpatch Communication with Controller"; flow:established,to_server; uricontent:"id="; nocase;
uricontent:"&check="; nocase; uricontent:"&version="; nocase; pcre:"/\?id=[A-Za-z]+_[A-Za-z]+&/U"; classtype:trojan-activity;
reference:url,www.symantec.com/security_response/writeup.jsp?docid=2008-081817-1808-99&tabid=2; reference:url,doc.emergingthreats.net/2009408; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bankpatch; sid:2009408; rev:2;)

#by Darren Spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Patcher/Bankpatch Module Download Request"; flow:established,to_server; uricontent:"/dl/AcroIEHelpe"; nocase;
uricontent:".dll"; nocase; pcre:"/\/dl\/AcroIEHelpe(r)?(\d)?\.dll/U"; classtype:trojan-activity; reference:url,www.symantec.com/security_response/writeup.jsp?docid=2008-081817-1808-
99&tabid=2; reference:url,doc.emergingthreats.net/2009409; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bankpatch; sid:2009409; rev:2;)

#Matt Jonkman
#Regular downloader, usually grabs a fw swf exploiting files from brazilian servers. Sends an email on installl
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN Banload Downloader Infection - Sending initial email to owner"; flow:established,to_server; content:"X-Library|3a| Indy 9";
nocase; content:"Dispositivo instalado."; nocase; content:"Maquina pronta para uso."; nocase; content:"Data|3a| "; nocase; content:"Hora|3a| "; nocase; content:"Development by ";
nocase; classtype:trojan-activity; reference:url,www.viruslist.com/en/viruses/encyclopedia?virusid=95586; reference:url,doc.emergingthreats.net/2002977;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banload.Downloader; sid:2002977; rev:4;)

#Matt Jonkman
#Regular downloader, usually grabs a fw swf exploiting files from brazilian servers. Sends an email on installl
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banload User-Agent Detected (ExampleDL)"; flow:established,to_server; content:"User-Agent|3a| ExampleDL";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2004440; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banload.Downloader; sid:2004440;
rev:4;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banload HTTP Checkin"; flow:established,to_server; content:"POST "; depth:5; content:"|0d 0a|User-Agent|3a|
Mozilla/3.0 (compatible|3b| Indy Library)|0d 0a 0d 0a|tipo="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007863; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banload.Downloader; sid:2007863; rev:5;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banload HTTP Checkin Detected"; flow:established,to_server; uricontent:"php?mac="; nocase; uricontent:"&hdd=";
nocase; uricontent:"++++++++"; nocase; uricontent:"&ver="; nocase; uricontent:"&ie="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007864;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banload.Downloader; sid:2007864; rev:2;)

#Disabling, hits on a few legit apps
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banload User-Agent Detected (WebUpdate)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| WebUpdate|0d
0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008074; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banload.Downloader;
sid:2008074; rev:4;)

#Disabling, hits on a few legit apps
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banload HTTP Checkin Detected (envia.php)"; flow:established,to_server; uricontent:"/envia.php"; nocase;
content:"|0d 0a|User-Agent|3a| Mozilla/3.0 (compatible|3b| Indy Library)|0d 0a|"; nocase; content:"praquem="; distance:0; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008256; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banload.Downloader; sid:2008256; rev:3;)

#Disabling, hits on a few legit apps
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banload HTTP Checkin Detected (quem=)"; flow:established,to_server; uricontent:".php"; nocase; content:"|0d 0a|User-
Agent|3a| Mozilla/3.0 (compatible|3b| Indy Library)|0d 0a 0d 0a|quem="; content:"praquem="; distance:0; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008283;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banload.Downloader; sid:2008283; rev:3;)

#by Marcus at unsober.org
#This one uses gadugadu for CnC. Labeled banload but likely it's something else
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 8074 (msg:"ET TROJAN Banload Gadu-Gadu CnC Message Detected"; flowbits:isset,ET.gadu.loggedin; flow:established,to_server; content:"Uruchomiono
trojana, wpisz help aby uzyskac pomoc"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008320; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banload.Downloader; sid:2008320; rev:2;)

#by Will Metcalf
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banload iLLBrain Trojan Activity"; flow:to_server,established; content:"GET "; depth:4; content:"User-Agent|3a|
Microsoft URL Control"; nocase; uricontent:"/iLL"; uricontent:".xxx"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2008328;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banload.Downloader; sid:2008328; rev:5;)

#by bojan zdrnja of ISC
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banload POST Checkin (dados)"; flow:established,to_server; content: "POST "; depth:5; content:"PC="; nocase;
content: "&USER="; nocase; content:"&HASH="; nocase; content:"&DADOS="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008477;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banload.Downloader; sid:2008477; rev:2;)

#by: Jeremy Conway at sudosecure.net
#ref: 373b5b9e7d4d92aee575ba8b4e4549d8
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN BANLOAD Downloader GET Checkin"; flow:established,to_server; content:"GET "; depth:4; uricontent:"mac=";
uricontent:"sys="; uricontent:"yp="; uricontent:"rand="; nocase; pcre:"/mac=[0-9A-Fa-f]{12}&/Ui"; classtype:trojan-activity; reference:url,www.sophos.com/security/analyses/viruses-and-
spyware/trojbanloe.html; reference:url,doc.emergingthreats.net/2009453; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banload.Downloader; sid:2009453;
rev:2;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banload Checkin"; flow:to_server,established; content:"GET "; depth:4; uricontent:"c=voip&ord="; nocase;
uricontent:"=&SCRNSZ"; uricontent:"&BRSRSZ="; uricontent:"&TIMEZONE="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010266;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Banload.Downloader; sid:2010266; rev:2;)

#by matt Jonkman, from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Basine Trojan Checkin"; flow:established,to_server; dsize:>1000; content:"|0d 0a 0d 0a|a="; content:"&b=reported";
distance:0; within:40; content:"&d=report"; distance:0; within:40; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007692; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Basine; sid:2007692; rev:3;)

#by Darren Spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Urlzone/Bebloh Communication with Controller"; flow:established,to_server; content:"GET "; depth:4; uricontent:"?
type=slg&id="; nocase; pcre:"/\?type=slg&id=[0-9A-Z]{18}/U"; classtype:trojan-activity; reference:url,threatinfo.trendmicro.com/vinfo/grayware/ve_graywareDetails.asp?
GNAME=TSPY_BEBLOH.KO&VSect=Td; reference:url,doc.emergingthreats.net/2009351; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bebloh; sid:2009351; rev:4;)
```

```
#by Marcus at sober.org
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Urlzone/Bebloh Trojan Check-in"; flow:established,to_server; content:"POST "; depth:5; uricontent:".php";
content:"N="; content:"&ID="; content:"&DATA="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009520; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bebloh; sid:2009520; rev:2;)

#by jerry at cybercave
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Bebloh C&C HTTP POST"; flow:established,to_server; content:"POST "; depth:5; uricontent:"/ff.ie?rnd="; nocase;
pcre:"/\/ff\.ie\?rnd=\d+/Ui"; content:"|0d 0a 0d 0a|p="; nocase; content:"&ot="; nocase; distance:0; content:"&njeb="; distance:0; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2010565; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bebloh; sid:2010565; rev:3;)

#by deapesh misra
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 81 (msg:"ET TROJAN Bifrose Connect to Controller"; flow:established,to_server; dsize:<20; content:"|09 00 00 9a|"; depth:4; content:"|cc|";
distance:3; within:4; content:"|74|"; distance:3; within:4; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008273; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bifrose; sid:2008273; rev:3;)

#by deapesh misra
#
alert tcp $EXTERNAL_NET 81 -> $HOME_NET any (msg:"ET TROJAN Bifrose Response from Controller"; flow:established,from_server; dsize:9; content:"|05 00 00 00 BC|"; depth:5;
content:"|CC|"; distance:3; within:4; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008274; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bifrose; sid:2008274; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 81 (msg:"ET TROJAN Bifrose Connect to Controller (variant 2)"; flow:established,to_server; dsize:<220; content:"|d2 00 00 9b|"; depth:4;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008532; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bifrose; sid:2008532; rev:2;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Bifrose Connect to Controller (PING PONG)"; flow:stateless; dsize:10; content:"PING |3a|i.|0d 0a|";
classtype:trojan-activity; flowbits:set,ET.bifrose1; reference:url,doc.emergingthreats.net/2009128; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bifrose;
sid:2009128; rev:3;)

#matt jonkman
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Bifrose Response from Controller (PING PONG)"; flow:stateless; flowbits:isset,ET.bifrose1; dsize:9; content:"PONG
|3a|i.|0d|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009129; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bifrose; sid:2009129;
rev:3;)

#by deapesh misra
#
alert tcp $HOME_NET 81 -> $EXTERNAL_NET any (msg:"ET TROJAN Bifrose Response from victim"; flow:established,to_server; dsize:13; content:"|09 00 00 00 9a|"; depth:5; content:"|74|";
distance:7; within:8; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009797; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bifrose;
sid:2009797; rev:2;)

#analysis by Jose Nazario at arbor networks. Sig by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Blackenergy Bot Checkin to C&C"; flow:established,to_server; content:"POST "; depth:5; dsize:<400; content:"|0d
0a|Cache-Control|3a| no-cache|0d 0a 0d 0a|id="; content:"&build_id="; distance:5; pcre:"/id=x.+_[0-9A-F]{8}&build_id=.+/"; classtype:trojan-activity;
reference:url,asert.arbornetworks.com/2007/10/blackenergy-ddos-bot-analysis-available; reference:url,doc.emergingthreats.net/2007668; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Blackenergy; sid:2007668; rev:5;)

#by Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Blackenergy Bot Checkin to C&C (2)"; flow:to_server,established; content:"POST "; depth:5; content:"|0d 0a 0d 0a|";
content:"id="; nocase; distance:0; content:"&ln="; nocase; content:"&cn="; nocase; content:"&nt="; nocase; content:"&bid="; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2010875; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Blackenergy; sid:2010875; rev:3;)

#by spooker
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN BlackEnergy v2.x HTTP Request with Encrypted Variables"; flow:to_server,established; content:"POST "; depth:5;
uricontent:"/getcfg.php"; nocase; content:"|0d 0a 0d 0a|sksgh="; nocase; classtype:trojan-activity; reference:url,www.secureworks.com/research/threats/blackenergy2/?threat=blackenergy2;
reference:url,doc.emergingthreats.net/2010885; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Blackenergy; sid:2010885; rev:2;)

#by spooker
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN BlackEnergy v2.x Plugin Download Request"; flow:to_server,established; content:"POST "; depth:5;
uricontent:"/getcfg.php"; nocase; content:"|0d 0a 0d 0a|"; content:"getp="; distance:0; content:"id="; content:"ln="; content:"bid="; content:"nt="; content:"cn="; classtype:trojan-
activity; reference:url,www.secureworks.com/research/threats/blackenergy2/?threat=blackenergy2; reference:url,doc.emergingthreats.net/2010886; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Blackenergy; sid:2010886; rev:2;)

#fake search site, distributed backdoor.agent.aqr and others
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Blink.com related Backdoor Checkin"; flow:established,to_server; uricontent:"/?vn="; nocase;
uricontent:"&partner="; nocase; uricontent:"&ptag="; nocase; uricontent:"&b="; nocase; uricontent:"&se="; nocase; uricontent:"&au="; nocase; flowbits:set,ET.blink.get; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/2007805; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Blink.com; sid:2007805; rev:2;)

#fake search site, distributed backdoor.agent.aqr and others
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Blink.com related Upgrade Command Given"; flowbits:isset,ET.blink.get; flow:established,from_server; content:"|0d
0a|X-Messaging|3a| This is an important download|0d 0a|Location|3a| http|3a|//"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007806;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Blink.com; sid:2007806; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Boaxxe HTTP POST Checkin"; flow:established,to_server; uricontent:"/u/"; content:"POST "; depth:5; content:"|0d
0a|user-Agent|3a| Internet Explorer|0d 0a|"; content:"|0d 0a 0d 0a|a="; distance:0; content:"&b="; distance:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009297;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Boaxxe; sid:2009297; rev:3;)

#this really isn't Kraken, appears to really be bobax, but reported as kraken.
#These sigs are a first attempt, hopefully this will improve
#disabling, we should delete these soon, like in july 2010
#matt
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 447 (msg:"ET TROJAN Bobax/Kraken/Oderoor TCP 447 CnC Channel Initial Packet Outbound"; flow:established; dsize:24; threshold:type threshold,
track by_src, count 2, seconds 360; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/OdeRoor; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bobax; sid:2008103; rev:3;)

#this really isn't Kraken, appears to really be bobax, but reported as kraken.
#These sigs are a first attempt, hopefully this will improve
#disabling, we should delete these soon, like in july 2010
#matt
#
#alert udp $HOME_NET 1024: -> $EXTERNAL_NET 447 (msg:"ET TROJAN Bobax/Kraken/Oderoor UDP 447 CnC Channel Initial Packet Outbound"; dsize:24; threshold:type threshold, track by_src,
count 2, seconds 360; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/OdeRoor; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bobax; sid:2008104; rev:3;)

#this really isn't Kraken, appears to really be bobax, but reported as kraken.
#These sigs are a first attempt, hopefully this will improve
#disabling, we should delete these soon, like in july 2010
#matt
#
#alert udp $EXTERNAL_NET 447 -> $HOME_NET 1024: (msg:"ET TROJAN Bobax/Kraken/Oderoor UDP 447 CnC Channel Initial Packet Inbound"; dsize:24; threshold:type threshold, track by_src, count
2, seconds 360; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/OdeRoor; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bobax;
sid:2008105; rev:3;)
```

```
#this really isn't Kraken, appears to really be bobax, but reported as kraken.
#These sigs are a first attempt, hopefully this will improve
#disabling, we should delete these soon, like in july 2010
#matt
#
#alert tcp $EXTERNAL_NET 447 -> $HOME_NET 1024: (msg:"ET TROJAN Bobax/Kraken/Oderoor TCP 447 CnC Channel Initial Packet Inbound"; flow:established; dsize:24; threshold:type threshold,
track by_src, count 2, seconds 360; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/OdeRoor; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bobax; sid:2008106; rev:3;)

#this really isn't Kraken, appears to really be bobax, but reported as kraken.
#These sigs are a first attempt, hopefully this will improve
#disabling, we should delete these soon, like in july 2010
#matt
#
#alert udp $EXTERNAL_NET 447 -> $HOME_NET 1024: (msg:"ET TROJAN Possible Bobax/Kraken/Oderoor UDP 447 CnC Channel Inbound"; threshold:type threshold, track by_src, count 5, seconds 60;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/OdeRoor; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bobax; sid:2008107;
rev:3;)

#this really isn't Kraken, appears to really be bobax, but reported as kraken.
#These sigs are a first attempt, hopefully this will improve
#disabling, we should delete these soon, like in july 2010
#matt
#
#alert tcp $EXTERNAL_NET 447 -> $HOME_NET 1024: (msg:"ET TROJAN Possible Bobax/Kraken/Oderoor TCP 447 CnC Channel Inbound"; flow:established; threshold:type threshold, track by_src,
count 5, seconds 60; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/OdeRoor; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bobax; sid:2008108; rev:3;)

#this really isn't Kraken, appears to really be bobax, but reported as kraken.
#These sigs are a first attempt, hopefully this will improve
#disabling, we should delete these soon, like in july 2010
#matt
#
#alert udp $HOME_NET 1024: -> $EXTERNAL_NET 447 (msg:"ET TROJAN Possible Bobax/Kraken/Oderoor UDP 447 CnC Channel Outbound"; threshold:type threshold, track by_src, count 5, seconds 60;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/OdeRoor; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bobax; sid:2008109;
rev:3;)

#this really isn't Kraken, appears to really be bobax, but reported as kraken.
#These sigs are a first attempt, hopefully this will improve
#disabling, we should delete these soon, like in july 2010
#matt
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 447 (msg:"ET TROJAN Possible Bobax/Kraken/Oderoor TCP 447 CnC Channel Outbound"; flow:established; threshold:type threshold, track by_src,
count 5, seconds 60; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/OdeRoor; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bobax; sid:2008110; rev:3;)

#Bofra Worm
#submitted by Matt Jonkman, additions by David Maciejak - Bofra Worm
#
##alert tcp $HOME_NET !$HTTP_PORTS -> $EXTERNAL_NET 1639 (msg:"ET DELETED Bofra Victim Accessing Reactor Page"; flow: from_client,established; content:"GET "; nocase; content:"reactor";
nocase; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/w32.bofra.e@mm.html; reference:url,us.mcafee.com/virusInfo/default.asp?
id=description&virus_k=129631; reference:url,doc.emergingthreats.net/2001430; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bofra; sid:2001430; rev:10;)

#by Jeffrey Brown, re 33f56ffda981afa725d530be3d1e1cfb
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Bravix Checkin"; flow:to_server,established; content:"GET "; depth:4; uricontent:"?wmid="; uricontent:"&l=";
uricontent:"&it="; uricontent:"&s="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008541; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bravix; sid:2008541; rev:2;)

#by darren spruell
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Bredavi Configuration Update Response"; flow:established,from_server; content:"|0d 0a 0d 0a 21|new_config|0a|";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010790; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bredavi; sid:2010790;
rev:2;)

#by darren spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Bredavi Checkin"; flow:established,to_server; uricontent:".php?id="; nocase; uricontent:"&ver="; nocase;
uricontent:"&up="; nocase; uricontent:"&os="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010791; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bredavi; sid:2010791; rev:2;)

#by Darren Spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Bredolab Downloader Communicating With Controller (1)"; flow:established,to_server; uricontent:"action="; nocase;
uricontent:"&entity_list="; nocase; uricontent:"&uid="; nocase; uricontent:"&first="; uricontent:"&guid="; nocase; uricontent:"&rnd="; nocase; classtype:trojan-activity;
reference:url,www.microsoft.com/security/portal/Entry.aspx?Name=TrojanDownloader%3aWin32/Bredolab.B; reference:url,doc.emergingthreats.net/2009353;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bredolab; sid:2009353; rev:8;)

#by Darren Spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Bredolab Downloader Communicating With Controller (2)"; flow:established,to_server; uricontent:"action="; nocase;
uricontent:"&guid="; nocase; uricontent:"&rnd="; nocase; uricontent:"&uid="; nocase; uricontent:"&entity="; nocase; classtype:trojan-activity;
reference:url,www.microsoft.com/security/portal/Entry.aspx?Name=TrojanDownloader%3aWin32/Bredolab.B; reference:url,doc.emergingthreats.net/2009354;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bredolab; sid:2009354; rev:6;)

#by Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Bredolab Check In"; flow:established,to_server; content:"GET "; depth:4; uricontent:"v="; uricontent:"&s=";
uricontent:"&uid="; uricontent:"&p="; uricontent:"&q="; content:"|0d 0a|User-Agent|3a 0d 0a|"; classtype:trojan-activity; reference:url,www.martinsecurity.net/2009/05/20/inside-the-
massive-gumblar-attacka-dentro-del-enorme-ataque-gumblar/; reference:url,doc.emergingthreats.net/2009360; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bredolab; sid:2009360; rev:6;)

#by Darren Spruell
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Bredolab Downloader Response Binaries from Controller"; flow:established,from_server; content:"|0d 0a|Entity-
Info|3a|"; nocase; content:"|0d 0a|Magic-Number|3a|"; nocase; pcre:"/\x0d\x0aEntity-Info\x3a\s+\d+\x3a\d+/"; pcre:"/\x0d\x0aMagic-Number\x3a\s+\d+\|\d+/"; classtype:trojan-activity;
reference:url,www.microsoft.com/security/portal/Entry.aspx?Name=TrojanDownloader%3aWin32/Bredolab.B; reference:url,doc.emergingthreats.net/2009388;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bredolab; sid:2009388; rev:3;)

#Bredolab Infection
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Hiloti/Mufanom Downloader Checkin"; flow:established,to_server; uricontent:"/get"; nocase; uricontent:".php?c=";
nocase; uricontent:"&d="; nocase; pcre:"/\/get\d*\.php\?c=[A-Z]{8}&d=[0-9A-F]{250,}$/U"; classtype:trojan-activity;
reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Trojan%3aWin32%2fHiloti.gen!A; reference:url,doc.emergingthreats.net/2010071;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bredolab; reference:url,blog.fortinet.com/hiloti-the-botmaster-of-disguise/; sid:2010071; rev:6;)

#Bredolab Infection
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Bredolab Infection - Windows Key"; flow:established,to_server; uricontent:"?s=Windows"; nocase; uricontent:"&p=";
nocase; pcre:"/\&p=[0-9A-Za-z]{5}\-[0-9A-Za-z]{5}\-/"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010072; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bredolab; sid:2010072; rev:3;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Syrutrk/Gibon/Bredolab Checkin"; flow:to_server,established; content:"GET "; depth:4; uricontent:"?ddos=x"; nocase;
pcre:"/\x3Fddos\x3D(x\d{1,2}){5,}/Ui"; classtype:trojan-activity; reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Backdoor%3aWin32%2fSyrutrk.A;
reference:url,www.threatexpert.com/report.aspx?md5=a5f94577d00d0306e4ef64bad30e5d37; reference:url,www.threatexpert.com/report.aspx?md5=011d403b345672adc29846074e717865;
```

```
reference:url,doc.emergingthreats.net/2010381; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bredolab; sid:2010381; rev:4;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Fake AV GET"; flow:established,to_server; content:"GET "; depth:4; uricontent:".php?"; nocase; uricontent:"affid=";
nocase; uricontent:"subid="; nocase; uricontent:"type="; nocase; uricontent:"adware"; nocase; classtype:trojan-activity; reference:url,threatexpert.com/report.aspx?
md5=8d1b47452307259f1e191e16ed23cd35; reference:url,doc.emergingthreats.net/2010382; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bredolab; sid:2010382;
rev:3;)

#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Brontok User-Agent Detected (Brontok.A3 Browser)"; flow:established,to_server; content:"User-Agent|3a| Brontok";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006999; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Brontok; sid:2006999;
rev:4;)

#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Brontok/Joseray User-Agent Detected (Joseray.A3 Browser)"; flow:established,to_server; content:"User-Agent|3a|
Joseray"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008765; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Brontok;
sid:2008765; rev:3;)

#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Buzus FTP Log Upload"; flow:established,to_server; dsize:100<>500; content:"|20 20 20 20|"; depth:4;
content:"************CD-Key Pack************"; distance:0; content:"Microsoft Windows Product ID CD Key\: "; distance:0; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008750; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Buzus; sid:2008750; rev:3;)

#by Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Buzus Posting Data"; flow:established,to_server; content:"POST "; nocase; depth:5; uricontent:"/fdsupdate"; nocase;
content:"|0d 0a 0d 0a|PUTF"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010064; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Buzus;
sid:2010064; rev:3;)

#matt jonkman, labeled logsnif, bzub2, dopip
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Bzub2 Related RPC/Http Checkin"; flow:established,to_server; uricontent:"/rpc.php?a=ftp%3A%2F%2F"; nocase;
uricontent:"&b="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007843; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bzub;
sid:2007843; rev:2;)

#by Darren Spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Metafisher/Bzub/Cimuz/Tanspy Reporting User Activity"; flow:established,to_server; uricontent:"ver="; nocase;
uricontent:"&lg="; nocase; uricontent:"&phid="; nocase; uricontent:"&r="; pcre:"/phid=[A-F0-9]{64}/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009349;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bzub; sid:2009349; rev:3;)

#by William Salusky of AOL, modified to use httpinspect
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Cashout Proxy Bot reg_DST"; flow:to_server,established; uricontent:".php?"; uricontent:"lang="; uricontent:"&pal=";
uricontent:"&bay="; uricontent:"&gold="; uricontent:"&id="; uricontent:"&param="; uricontent: "&socksport="; uricontent:"&httpport="; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008248; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Cashout_Proxy; sid:2008248; rev:2;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Cashpoint.com Related checkin User-Agent (inetinst)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
inetinst|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007808; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Cashpoint.com;
sid:2007808; rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Cashpoint.com Related checkin User-Agent (okcpmgr)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
okcpmgr|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007810; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Cashpoint.com;
sid:2007810; rev:3;)

#by Darren Spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN DownloaderExchanger/Cbeplay Variant Checkin"; flow:to_server,established; content:"POST "; depth:5; nocase;
content:"|0d 0a 0d 0a|os="; nocase; content:"&ver="; nocase; distance:0; content:"&idx="; nocase; distance:0; content:"&user="; nocase; distance:0; content:"&ioctl="; nocase;
distance:0; content:"&data="; distance:0; nocase; classtype:trojan-activity; reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?
Name=TrojanDownloader%3aWin32%2fCbeplay.B; reference:url,www.secureworks.com/research/threats/ppi/; reference:url,doc.emergingthreats.net/2010217;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Cbeplay; sid:2010217; rev:3;)

#by Jeffrey Brown at synacktip
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Ceckno Reporting to Controller"; flow:established,to_server; dsize:<30; content:"\:2|7c|"; depth:10; content:"|7c|";
distance:0; content:"|7c|"; distance:0; pcre:"/^\d+\x3a\d\x7c\d+\x7c[0-9a-z]+\x7c\d+/i"; flowbits:set,ET.cekno.initial; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008177; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Cekno; sid:2008177; rev:4;)

#by Jeffrey Brown at synacktip
#
#alert tcp $EXTERNAL_NET 1024: -> $HOME_NET any (msg:"ET TROJAN Ceckno Keepalive from Controller"; flow:established,from_server; dsize:1; content:"1"; flowbits:isset,ET.cekno.initial;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008178; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Cekno; sid:2008178; rev:3;)

#by Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32/Chekafe.A or Related Infection Checkin"; flow:established,to_server; uricontent:"isInst=";
uricontent:"lockcode="; uricontent:"PcType="; uricontent:"AvName="; uricontent:"ProCount="; classtype:trojan-activity;
reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=TrojanDownloader%3AWin32/Chekafe.A; reference:url,doc.emergingthreats.net/2011272;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Chekafe; sid:2011272; rev:2;)

#by dn1nj4
#
alert tcp $EXTERNAL_NET 8000 -> $HOME_NET any (msg:"ET TROJAN TR/Chinky.G Download Command"; flow:to_client,established; content:"|3a 2e|dl|20|http|3a 2f 2f|"; depth:12; content:".exe";
distance:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010973; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Chinky; sid:2010973;
rev:2;)

#by Jeffrey Brown
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Cinmus.Checkin 1"; flow:to_server,established; content:"GET "; depth:4; uricontent:"?version="; nocase;
uricontent:"lversion="; nocase; uricontent:"&mac="; nocase; uricontent:"&fid="; nocase; uricontent:"&vpc="; nocase; uricontent:"&run="; nocase; uricontent:"&from="; classtype: trojan-
activity; reference:url,doc.emergingthreats.net/2008623; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Cinmus; sid:2008623; rev:2;)

#by Jeffrey Brown
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Cinmus.Checkin 2"; flow:to_server,established; content:"GET "; depth:4; uricontent:"?fid="; nocase;
uricontent:"&kid="; nocase; uricontent:"&cnt="; nocase; uricontent:"&mac="; nocase; uricontent:"&kw="; nocase; uricontent:"&from="; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008624; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Cinmus; sid:2008624; rev:2;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Citi-bank.ru Related Trojan Checkin"; flow:established,to_server; uricontent:".php?hid=NT"; nocase;
uricontent:"&wp="; nocase; uricontent:"&sp="; nocase; uricontent:"&eep="; nocase; uricontent:"&edp="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008153;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Citi-bank.ru; sid:2008153; rev:2;)

#by Marcus at unsober, re 68926f2883af13d6001126aae4345dab
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Rootkit.Win32.Clbd.cz Checkin"; flow:established,to_server; content:"POST "; depth:5; uricontent:".php";
content:"gd="; content:"=="; within:20; content:"&affid="; content:"="; within:5; content:"&subid="; content:"=="; within:5; content:"&prov="; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008442; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Clbd.cz; sid:2008442; rev:3;)

#by darren spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Clod/Sereki Communication with C&C"; flow:established,to_server; uricontent:".php?id="; nocase; uricontent:"&cnt=";
nocase; pcre:"/\.php\?id=\d+_[0-9a-f]{8}-[0-9a-f]+-[0-9a-f]{8}&cnt=/U"; classtype:trojan-activity; reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?
Name=Backdoor%3aWin32%2fSereki.A; reference:url,www.threatexpert.com/report.aspx?md5=bbb6ac2181dbbe15efd13c294cb991fa; reference:url,www.threatexpert.com/report.aspx?
md5=3c39bfc78fcf3fe805c7472296bf6319; reference:url,doc.emergingthreats.net/2010289; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Clod; sid:2010289;
rev:2;)

#by darren spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Clod/Sereki Checkin with C&C (noalert)"; flow:established,to_server; content:"GET "; depth:4;
uricontent:"/chck.dat"; nocase; content:!"|0d 0a|User-Agent|3a|"; nocase; content:!"|0d 0a|Referer|3a|"; nocase; flowbits:set,ET.clod1; flowbits:noalert; classtype:trojan-activity;
reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Backdoor%3aWin32%2fSereki.A; reference:url,www.threatexpert.com/report.aspx?
md5=bbb6ac2181dbbe15efd13c294cb991fa; reference:url,www.threatexpert.com/report.aspx?md5=3c39bfc78fcf3fe805c7472296bf6319; reference:url,doc.emergingthreats.net/2010290;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Clod; sid:2010290; rev:4;)

#by darren spruell
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Clod/Sereki Checkin Response"; flow:established,from_server; dsize:<350; content:"|0d 0a 0d 0a|!chckOK!"; nocase;
flowbits:isset,ET.clod1; classtype:trojan-activity; reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Backdoor%3aWin32%2fSereki.A;
reference:url,www.threatexpert.com/report.aspx?md5=bbb6ac2181dbbe15efd13c294cb991fa; reference:url,www.threatexpert.com/report.aspx?md5=3c39bfc78fcf3fe805c7472296bf6319;
reference:url,doc.emergingthreats.net/2010291; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Clod; sid:2010291; rev:2;)

#by jeffrey brown
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN Codesoft PW Stealer Email Report Outbound"; flow:established,to_server; content:"|0d 0a|Subject|3a| Codesoft PW Stealer";
content:"******STEAM PASS STEALER*******"; distance:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008310; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_CodeSoft; sid:2008310; rev:2;)

#by Kevin Ross
#
#alert tcp $HOME_NET any -> 67.15.94.80 $HTTP_PORTS (msg:"ET TROJAN Possible Downadup/Conficker-A Worm Activity"; flow:to_server,established; uricontent:"/GeoIP.dat.gz";
classtype:trojan-activity; reference:url,www.microsoft.com/security/portal/Entry.aspx?Name=Worm%3aWin32%2fConficker.A; reference:url,www.f-secure.com/v-descs/worm_w32_downadup_a.shtml;
reference:url,doc.emergingthreats.net/bin/view/Main/2008802; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/TROJAN/TROJAN_Conficker; sid:2008802; rev:5;)

#By RPG and Jack Pepper, modified by thierry chich and darren spruell
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downadup/Conficker A or B Worm reporting"; flow:to_server,established; uricontent:"/search?q="; pcre:"/^\/search\?
q=[0-9]{1,3}(&aq=7(\?[0-9a-f]{8}))?$/U"; pcre:"/\x0d\x0aHost\: \d+\.\d+\.\d+\.\d+\x0d\x0a/"; classtype:trojan-activity; reference:url,www.f-secure.com/weblog/archives/00001584.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2009024; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Conficker; sid:2009024; rev:12;)

#By RPG and Jack Pepper, modified by thierry chich and darren spruell
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downadup/Conficker A Worm reporting"; flow:to_server,established; uricontent:"/search?q="; uricontent:"&aq=";
pcre:"/\/search\?q\=\d+&aq=\d/mi"; classtype:trojan-activity; reference:url,www.f-secure.com/weblog/archives/00001584.html; reference:url,doc.emergingthreats.net/bin/view/Main/2009114;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/TROJAN/TROJAN_Conficker; sid:2009114; rev:3;)

#by Tillman Werner
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"ET TROJAN Conficker.a Shellcode"; flow:established,to_server; content:"|e8 ff ff ff ff c1|^|8d|N|10 80|1|c4|Af|81|9EPu|f5 ae c6 9d
a0|O|85 ea|O|84 c8|O|84 d8|O|c4|O|9c cc|IrX|c4 c4 c4|,|ed c4 c4 c4 94|&<O8|92|\;|d3|WG|02 c3|,|dc c4 c4 c4 f7 16 96 96|O|08 a2 03 c5 bc ea 95|\;|b3 c0 96 96 95 92 96|\;|f3|\;|24|i| 95
92|QO|8f f8|O|88 cf bc c7 0f f7|2I|d0|w|c7 95 e4|O|d6 c7 17 f7 04 05 04 c3 f6 c6 86|D|fe c4 b1|1|ff 01 b0 c2 82 ff b5 dc b6 1b|O|95 e0 c7 17 cb|s|d0 b6|O|85 d8 c7 07|O|c0|T|c7 07 9a 9d
07 a4|fN|b2 e2|Dh|0c b1 b6 a8 a9 ab aa c4|]|e7 99 1d ac b0 b0 b4 fe eb eb|"; classtype:trojan-activity; reference:url,www.honeynet.org/node/388;
reference:url,doc.emergingthreats.net/2009200; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/TROJAN/TROJAN_Conficker; sid:2009200; rev:6;)

#by Tillman Werner
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"ET TROJAN Conficker.b Shellcode"; flow:established,to_server; content:"|e8 ff ff ff ff c2|_|8d|O|10 80|1|c4|Af|81|9MSu|f5|8|ae c6 9d
a0|O|85 ea|O|84 c8|O|84 d8|O|c4|O|9c cc|Ise|c4 c4 c4|,|ed c4 c4 c4 94|&<O8|92|\;|d3|WG|02 c3|,|dc c4 c4 c4 f7 16 96 96|O|08 a2 03 c5 bc ea 95|\;|b3 c0 96 96 95 92 96|\;|f3|\;|24 |i|95
92|QO|8f f8|O|88 cf bc c7 0f f7|2I|d0|w|c7 95 e4|O|d6 c7 17 cb c4 04 cb|{|04 05 04 c3 f6 c6 86|D|fe c4 b1|1|ff 01 b0 c2 82 ff b5 dc b6 1f|O|95 e0 c7 17 cb|s|d0 b6|O|85 d8 c7
07|O|c0|T|c7 07 9a 9d 07 a4|fN|b2 e2|Dh|0c b1 b6 a8 a9 ab aa c4|]|e7 99 1d ac b0 b0 b4 fe eb eb|"; classtype:trojan-activity; reference:url,www.honeynet.org/node/388;
reference:url,doc.emergingthreats.net/2009201; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/TROJAN/TROJAN_Conficker; sid:2009201; rev:6;)

#Disabling in favor of the preproc and SO rules that are now available
#
#alert udp $HOME_NET [!1720,!1722,!2427,!5060,1024:] -> $EXTERNAL_NET [!1720,!1722,!2427,!5060,1024:] (msg:"ET TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet
(bit value 1)"; dsize:>19; byte_test:1, &, 1, 19; threshold: type both, track by_src, count 95, seconds 50; classtype:trojan-activity; reference:url,mtc.sri.com/Conficker/addendumC/;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/TROJAN/TROJAN_Conficker; reference:url,doc.emergingthreats.net/2009205; sid:2009205; rev:4;)

#Disabling in favor of the preproc and SO rules that are now available
#
#alert udp $HOME_NET [!1720,!1722,!2427,!5060,1024:] -> $EXTERNAL_NET [!1720,!1722,!2427,!5060,1024:] (msg:"ET TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet
(bit value 4)"; dsize:>19; byte_test:1, &, 4, 19; threshold: type both, track by_src, count 95, seconds 40; classtype:trojan-activity; reference:url,mtc.sri.com/Conficker/addendumC/;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/TROJAN/TROJAN_Conficker; reference:url,doc.emergingthreats.net/2009206; sid:2009206; rev:4;)

#Disabling in favor of the preproc and SO rules that are now available
#
#alert udp $HOME_NET [!1720,!1722,!2427,!5060,1024:] -> $EXTERNAL_NET [!1720,!1722,!2427,!5060,1024:] (msg:"ET TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet
(bit value 5)"; dsize:>19; byte_test:1, &, 5, 19; threshold: type both, track by_src, count 95, seconds 40; classtype:trojan-activity; reference:url,mtc.sri.com/Conficker/addendumC/;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/TROJAN/TROJAN_Conficker; reference:url,doc.emergingthreats.net/2009207; sid:2009207; rev:4;)

#Disabling in favor of the preproc and SO rules that are now available
#
#alert udp $HOME_NET [!1720,!1722,!2427,!5060,1024:] -> $EXTERNAL_NET [!1720,!1722,!2427,!5060,1024:] (msg:"ET TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet
(bit value 16)"; dsize:>19; byte_test:1, &, 16, 19; threshold: type both, track by_src, count 95, seconds 40; classtype:trojan-activity; reference:url,mtc.sri.com/Conficker/addendumC/;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/TROJAN/TROJAN_Conficker; reference:url,doc.emergingthreats.net/2009208; sid:2009208; rev:4;)

#by Daniel Clemens
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Conficker/KernelBot/MS08-067 related Trojan Checkin"; flow:established,to_server; content:"GET "; depth:4;
uricontent:"/kernel/zz.htm?"; uricontent:"Ver="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008737; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Conficker; sid:2008737; rev:7;)

#by David Wharton
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Suspicious Accept-Language HTTP Header, zh-cn, likely Kernelbot/Conficker Trojan Related";
flow:established,to_server; content:"|0d 0a|Accept-Language|3A| zh|2D|cn"; flowbits:set,ET.ms08067_header; flowbits:noalert; classtype:not-suspicious;
reference:url,doc.emergingthreats.net/bin/view/Main/2008738; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Conficker; sid:2008738; rev:5;)

#by David Wharton
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Conficker/MS08-067 Worm Traffic Outbound"; flowbits:isset,ET.ms08067_header; flow:established,to_server;
content:"If-None-Match|3A| |22|60794|2D|12b3|2D|e4169440|22|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008739;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Conficker; sid:2008739; rev:6;)

#by Philipp Bescht
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN contacy.info Trojan Checkin (User agent clk_jdfhid)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
clk_jdfhid|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008399; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Contacy.info;
sid:2008399; rev:4;)

#by Joe Stewart of Secureworks
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Coreflood/AFcore Trojan Infection"; flow:to_server; content:"POST|20|/c/a"; byte_test:1,<,64,0,relative;
content:"HTTP/1.0|0d0a|Host|3a20|"; within:21; classtype:trojan-activity; reference:url,www.secureworks.com/research/threats/coreflood; reference:url,doc.emergingthreats.net/2008434;
```

```
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Coreflood; sid:2008434; rev:3;)

#modified version for new variants, matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Coreflood/AFcore Trojan Infection (2)"; flow:to_server; content:"POST "; depth:5; content:"HTTP/1.0|0d 0a|Host|3a
20|"; content:"|0d 0a 0d 0a|r="; content:"&i="; distance:0; content:"&v="; distance:0; content:"&os="; distance:0; content:"&s="; distance:0; content:"&h="; distance:0; content:"&d=";
distance:0; content:"&panic"; distance:0; content:"&ie="; distance:0; content:"&input="; distance:0; content:"&c="; distance:0; classtype:trojan-activity;
reference:url,www.secureworks.com/research/threats/coreflood; reference:url,doc.emergingthreats.net/2008443; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Coreflood; sid:2008443; rev:3;)

#Submitted 2008-06-26 by Darren Spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN CoreFlooder.Q Data Posting"; flow:established,to_server; content:"POST "; depth:5; uricontent:"/upload"; nocase;
uricontent:"file="; nocase; uricontent:"&id="; nocase; threshold: type limit, track by_src, seconds 3600, count 1; classtype:trojan-activity;
reference:url,www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ%5FCOREFLOOD%2EQ; reference:url,doc.emergingthreats.net/2008352; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/TROJAN/VIRUS_Coreflood; sid:2008352; rev:4;)

#Submitted 2008-06-26 by Darren Spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN CoreFlooder.Q C&C Checkin"; flow:established,to_server; content:"POST "; depth:5; uricontent:"/a?"; nocase;
content:"|0d 0a 0d 0a|wg="; nocase; content:"&cn="; nocase; content:"&i="; nocase; content:"&panic="; nocase; threshold: type limit, track by_src, seconds 3600, count 1;
classtype:trojan-activity; reference:url,www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ%5FCOREFLOOD%2EQ; reference:url,doc.emergingthreats.net/2008353;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/TROJAN/VIRUS_Coreflood; sid:2008353; rev:4;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN CoreFlooder C&C Checkin (2)"; flow:established,to_server; content:"POST "; depth:5; uricontent:"/index.php"; nocase;
content:"|0d 0a 0d 0a|r="; content:"&i="; distance:0; content:"&v="; distance:0; content:"&os="; distance:0; content:"&panic="; distance:0; content:"&input="; distance:0;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009287; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/TROJAN/VIRUS_Coreflood; sid:2009287; rev:1;)

#by matt jonkman, Proxy.Corpes.j 0fe727c2779b6891697db8f768b6d34b
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Proxy.Corpes.j Infection Report"; flow:established,to_server; uricontent:".php?tma="; uricontent:"&mode=";
pcre:"/mode=\d+D[0-9A-F]{150}/U"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008144; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Corpes; sid:2008144; rev:3;)

#by dn1nj4
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Cosmu Process Dump Report"; flow:established,to_server; content:"] Dumping processes {|0d 0a|"; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/2011234; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Cosmu; sid:2011234; rev:2;)

#by Jeffrey Brown, re 35546d9972aed2a5fec2c4e1136730a3
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Crypt.nc Checkin"; flow:to_server,established; uricontent:".php?l="; uricontent:"&d="; uricontent:"&ver=";
uricontent:"&rvz1="; uricontent:"&rvz2="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008567; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Crypt; sid:2008567; rev:2;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Crypt.CFI.Gen Checkin"; flow:established,to_server; content:"POST "; depth:5; content:"|0d 0a|User-Agent|3a| BIE|0d
0a|"; content:"|0d 0a 0d 0a|cname="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009204; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Crypt; sid:2009204; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN DMSpammer HTTP Post Checkin"; flow:established,to_server; content:"POST "; depth:5; uricontent:"/stat";
uricontent:".php"; content:"|0d 0a|User-Agent|3a| Mozilla/4.0 (compatible|3b| Synapse)|0d 0a|"; content:"|0d 0a 0d 0a|x|9c|"; distance:0; pcre:"/\/stat\d+\.php/U"; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/2008271; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_DMSpammer; sid:2008271; rev:4;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN DNS Changer HTTP Post Checkin"; flow:established,to_server; content:"POST "; depth:5; content:"|0d 0a 0d 0a|x=";
content:!"|0d 0a|User-Agent|3a| "; pcre:"/x=[0-9a-zA-Z]{50}/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008263; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_DNS_Changer; sid:2008263; rev:4;)

#By pedromarinho and matt jonkman.
#Downloader.Agent.bnm and dnschange.bnm, etc
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN DNS Changer.bnm/Downloader.bnm CnC Channel Start"; flow:established,to_server; dsize:8; content:"|0b 01 00 00 00 00 00
00|"; classtype:trojan-activity; flowbits:noalert; flowbits:set,ET.dlbnm1; reference:url,doc.emergingthreats.net/2008805; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_DNS_Changer; sid:2008805; rev:3;)

#By pedromarinho and matt jonkman.
#Downloader.Agent.bnm and dnschange.bnm, etc
#
#alert tcp $EXTERNAL_NET 1024: -> $HOME_NET any (msg:"ET TROJAN DNS Changer.bnm/Downloader.bnm CnC Channel Start Response"; flow:established,from_server; dsize:4; content:"|0b 01|";
depth:2; content:"|00|"; distance:1; within:1; classtype:trojan-activity; flowbits:isset,ET.dlbnm1; reference:url,doc.emergingthreats.net/2008806;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_DNS_Changer; sid:2008806; rev:3;)

#By pedromarinho and matt jonkman.
#Downloader.Agent.bnm and dnschange.bnm, etc
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN DNS Changer.bnm/Downloader.bnm Second CnC Channel Start"; flow:established,to_server; dsize:32; content:"|00 00 00 00 c0
a8 01 1e 67 00 00 00 00|"; depth:13; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008807; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_DNS_Changer; sid:2008807; rev:4;)

#By pedromarinho and matt jonkman.
#Downloader.Agent.bnm and dnschange.bnm, etc
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN DNS Changer.bnm/Downloader.bnm Second CnC Channel Traffic"; flow:established,to_server; dsize:32; content:"|55 d8 09 00 c0
a8 01 1e 67 00 00 00 00|"; depth:13; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008808; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_DNS_Changer; sid:2008808; rev:4;)

#by matt jonkman, re 94ff9b9a3b40c3f21e4fac3a7712b6a6
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN DNSChanger.AT or related Infection Checkin Post"; flow:established,to_server; content:"POST /cgi-bin/generator
HTTP/1.0|0d 0a|Content-Length|3a| "; depth:50; content:"|0d 0a 0d 0a|"; within:10; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008940;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_DNS_Changer; sid:2008940; rev:4;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Daemonize.ft HTTP Checkin"; flow:established,to_server; uricontent:".php?v="; nocase; uricontent:"&rnd="; nocase;
uricontent:"&u=00"; nocase; uricontent:"&s="; nocase; uricontent:"&id="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008086;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Daemonize; sid:2008086; rev:2;)

#by darren spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Daonol C&C Communication"; flow:established,to_server; uricontent:"/x/?0"; nocase; content:"|0d 0a|SS|3a|"; nocase;
content:"|0d 0a|Xost|3a|"; nocase; pcre:"/\/x\/\?0\w{35}$/U"; classtype:trojan-activity; reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?
Name=Win32%2fDaonol; reference:url,blog.fireeye.com/research/2009/10/gumblar-not-gumby.html; reference:url,www.iss.net/threats/gumblar.html;
reference:url,blog.scansafe.com/journal/2009/10/15/gumblar-website-botnet-awakes.html; reference:url,doc.emergingthreats.net/2010164; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Daonol; sid:2010164; rev:3;)

#Matt Jonkman
#This thing send out an email to it's owner with stats and such. This ought to catch it..
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN Banker.Delf Infection - Sending Initial Email to Owner"; flow:established,to_server; content:"X-Library|3a| Indy 9"; nocase;
content:"Maquina.."; nocase; content:"Vers|e3|o do Windows"; nocase; content:"Microsoft Windows"; nocase; content:"Mac Address.."; nocase; classtype:trojan-activity;
reference:url,www.avira.com/en/threats/section/details/id_vir/1836/tr_banker.delf.df735649.html; reference:url,doc.emergingthreats.net/2002976;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2002976; rev:8;)

#another variant
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN Banker.Delf Infection variant 2 - Sending Initial Email to Owner"; flow:established,to_server; content:"X-Library|3a| Indy
9"; nocase; content:"Nome Computador|3a| "; nocase; content:"Data|3a| "; nocase; content:"Windows|3a| Microsoft Windows "; nocase; classtype:trojan-activity;
reference:url,www.avira.com/en/threats/section/details/id_vir/1836/tr_banker.delf.df735649.html; reference:url,doc.emergingthreats.net/2002978;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2002978; rev:5;)

#Yet another
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN Banker.Delf Infection variant 3 - Sending Initial Email to Owner"; flow:established,to_server; content:"X-Library|3a| Indy
9"; nocase; content:"Subject|3a| INFECT - "; nocase; content:"Data|3a| "; nocase; content:"Windows|3a| Microsoft Windows "; nocase; classtype:trojan-activity;
reference:url,www.avira.com/en/threats/section/details/id_vir/1836/tr_banker.delf.df735649.html; reference:url,doc.emergingthreats.net/2002980;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2002980; rev:4;)

#Yet another
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN Banker.Delf Infection variant 4 - Sending Initial Email to Owner"; flow:established,to_server; content:"X-Library|3a| Indy
9"; nocase; content:"Maquina"; nocase; content:"IP"; nocase; content:"Hora"; nocase; content:"Data"; nocase; content:"Microsoft Windows "; nocase; classtype:trojan-activity;
reference:url,www.avira.com/en/threats/section/details/id_vir/1836/tr_banker.delf.df735649.html; reference:url,doc.emergingthreats.net/2002981;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2002981; rev:4;)

#from sandnet data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banker.Delf User-Agent (Varlok_11000)"; flow:established,to_server; content:"User-Agent|3a| Varlok_"; nocase;
classtype:trojan-activity; reference:url,www.avira.com/en/threats/section/details/id_vir/1836/tr_banker.delf.df735649.html; reference:url,doc.emergingthreats.net/2003931;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2003931; rev:4;)

#from sandnet data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banker.Delf User-Agent (Ms)"; flow:established,to_server; content:"User-Agent|3a| Ms|0d 0a|"; classtype:trojan-
activity; reference:url,www.avira.com/en/threats/section/details/id_vir/1836/tr_banker.delf.df735649.html; reference:url,doc.emergingthreats.net/2003933;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2003933; rev:6;)

#from sandnet data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banker.Delf User-Agent (hhh)"; flow:established,to_server; content:"User-Agent|3a| hhh"; classtype:trojan-activity;
reference:url,www.avira.com/en/threats/section/details/id_vir/1836/tr_banker.delf.df735649.html; reference:url,doc.emergingthreats.net/2004442;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2004442; rev:4;)

#from sandnet data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banker.Delf User-Agent (Mz)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| Mz|0d 0a|";
classtype:trojan-activity; reference:url,www.avira.com/en/threats/section/details/id_vir/1836/tr_banker.delf.df735649.html; reference:url,doc.emergingthreats.net/2007594;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2007594; rev:6;)

#from sandnet data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banker.Delf User-Agent (MzApp)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| MzApp|0d 0a|";
classtype:trojan-activity; reference:url,www.avira.com/en/threats/section/details/id_vir/1836/tr_banker.delf.df735649.html; reference:url,doc.emergingthreats.net/2007594;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2009988; rev:2;)

#from sandnet data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Banker.Delf User-Agent (WINDOWS_LOADS)"; flow:established,to_server; content:"User-Agent|3a| WINDOWS_LOADS";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007699; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2007699; rev:4;)

#yet another c&c method, by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Delf HTTP Checkin (1)"; flow:established,to_server; uricontent:"/mydown.asp?"; nocase; uricontent:"reg="; nocase;
uricontent:"&ver="; nocase; uricontent:"&tgid="; nocase; uricontent:"&address="; nocase; uricontent:"&mydo="; nocase; uricontent:"&flag="; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2007838; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2007838; rev:4;)

#delf keylog upload, kinda flimsy but works
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 21 (msg:"ET TROJAN Delf Keylog FTP Upload"; flow:established,to_server; content:"STOR "; depth:5; content:" Keylogger ["; nocase; distance:5;
within:50; content:"].txt|0d 0a|"; nocase; distance:5; within:40; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007858; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2007858; rev:2;)

#delf keylog upload, kinda flimsy but works
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Delf HTTP Post Checkin (1)"; flow:established,to_server; content:"POST "; depth:5; uricontent:".php"; nocase;
content:"|0d 0a|Content-type|3a| image/gif|0d 0a 0d 0a|x|da|"; content:!"|0d 0a|User-Agent|3a| "; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007867;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2007867; rev:3;)

#by Victor Julien
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Delf Download via HTTP"; flow:established,to_server; content:"GET "; depth:4; uricontent:"/mdfexcute/";
content:"Windows 98)"; depth:200; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007911; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2007911; rev:2;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Delf/Hupigon C&C Channel Version Report"; flow:established,to_server; dsize:<25; content:"VERSON|3a|"; depth:7;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007930; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2007930; rev:4;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Delf Checkin via HTTP (up)"; flow:established,to_server; uricontent:"/up.html?"; nocase; uricontent:"set="; nocase;
uricontent:"&pid="; nocase; uricontent:"&MAC="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007939; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2007939; rev:2;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Delf Checkin via HTTP (5)"; flow:established,to_server; content:"POST "; depth:5; uricontent:".php"; nocase;
content:"|0d 0a|email="; nocase; content:"&computador="; nocase; distance:0; content:"&nomfile="; nocase; distance:0; content:"&user="; nocase; distance:0; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008044; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2008044; rev:2;)

#by matt jonkman
#re sample 41c62970ea34413c4011b220724bf029
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Delf CnC Channel Packet 1"; flowbits:isnotset,ET.unk.1; flow:established,to_server; dsize:<200; content:"|8e 00 d0 00|";
depth:4; flowbits:set,ET.unk.1; flowbits:noalert; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008006; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2008006; rev:6;)

#by matt jonkman
#re sample 41c62970ea34413c4011b220724bf029
#
#alert tcp $EXTERNAL_NET 1024: -> $HOME_NET any (msg:"ET TROJAN Delf CnC Channel Packet 1 reply"; flowbits:isset,ET.unk.1; flow:established,from_server; dsize:<15; content:"|05 00 00
00|"; depth:4; flowbits:set,ET.unk.2; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008007; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2008007; rev:5;)
```

```
#by matt jonkman
#re sample 41c62970ea34413c4011b220724bf029
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Delf CnC Channel Checkin Replies"; flowbits:isset,ET.unk.2; flow:established,to_server; dsize:<20; content:"|09 00 00
00|"; depth:4; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008008; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2008008;
rev:5;)

#by matt jonkman
#re sample 41c62970ea34413c4011b220724bf029
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Delf CnC Channel Keepalive Pong"; flow:established,to_server; dsize:<40; content:"|20 00 00 00 f8 4d b2 77|"; depth:8;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008009; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2008009; rev:5;)

#by matt jonkman
#re sample 41c62970ea34413c4011b220724bf029
#
#alert tcp $EXTERNAL_NET 1024: -> $HOME_NET any (msg:"ET TROJAN Delf CnC Channel Keepalive Ping"; flow:established,from_server; dsize:22; content:"|12 00 00 00 1c 5e|"; depth:6;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008010; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2008010; rev:6;)

#by matt jonkman
#re sample 41c62970ea34413c4011b220724bf029
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Delf Checkin via HTTP (6)"; flow:established,to_server; content:"GET "; depth:4; uricontent:".php?v="; nocase;
uricontent:"&u="; nocase; uricontent:"&t="; nocase; uricontent:"&p="; nocase; uricontent:"&=w"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008071;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2008071; rev:2;)

#by matt jonkman
#re sample 41c62970ea34413c4011b220724bf029
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Delf Checkin via HTTP (7)"; flow:established,to_server; content:"POST "; depth:5; uricontent:".php?macros="; nocase;
uricontent:"&botstatus="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008090; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2008090; rev:2;)

#by matt jonkman
#re sample 41c62970ea34413c4011b220724bf029
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Delf Checkin via HTTP (8)"; flow:established,to_server; content:"POST "; depth:5; uricontent:".php"; nocase;
content:"|0d 0a|User-Agent|3a| Mozilla/3.0 (compatible|3b| Indy Library)"; content:"|0d 0a 0d 0a|name="; distance:0; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008268; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2008268; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Delf Key Checkin (Clicker.Win32.Delf.afl)"; flow:established,to_server; uricontent:".php?key=???????+???????????";
uricontent:"+Dial-up+???????+?+??????????????"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008666; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2008666; rev:2;)

#victor julien
#Ikarus: Trojan.Delf-5496,
#re 462ee0f70fae7e7f29e546069e43484e
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Trojan.Delf-5496 Checkin Error"; flow:established,to_server; dsize:350<>450; content:"Erorr File active\;sorry file erorr
plaes down file agen"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008905; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf;
sid:2008905; rev:3;)

#victor julien
#Ikarus: Trojan.Delf-5496,
#re 462ee0f70fae7e7f29e546069e43484e
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Trojan.Delf-5496 Egg Request"; flow:established,to_server; dsize:<35; content:"|7c|CreateForm|7c|FileTransfer|7c|";
depth:29; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008906; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2008906; rev:3;)

#victor julien
#Ikarus: Trojan.Delf-5496,
#re 462ee0f70fae7e7f29e546069e43484e
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Trojan.Delf-5496 File Manager Access Report"; flow:established,to_server; dsize:<35;
content:"|7c|CreateForm|7c|FileManager|7c|"; depth:30; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008907; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2008907; rev:3;)

#victor julien
#Ikarus: Trojan.Delf-5496,
#re 462ee0f70fae7e7f29e546069e43484e
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Trojan.Delf-5496 New Infection Report"; flow:established,to_server; dsize:<500; content:"|7c|OnConnect|7c|New Server|7c|";
depth:29; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008908; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2008908; rev:3;)

#by: Jeremy Conway at sudosecure.net
#ref: d253db84a6d08dbeec6426c4c4d212a6
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader.Win32.Delf followon POST Data PUSH Packet"; flow:established,to_server; content:"tip="; depth:4; nocase;
content:"&cli="; nocase; content:"&tipo="; nocase; classtype:trojan-activity; reference:url,www.threatexpert.com/threats/trojan-downloader-win32-delf.html;
reference:url,doc.emergingthreats.net/2009824; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delf; sid:2009824; rev:4;)

#by sjirkdog
#re 146244b0d5cce3d21719ad94d650a82f
#traffic was on port 2009 in sample, since it is a new year. Maybe use it as the source
#
alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET any (msg:"ET TROJAN Delfsnif/Buzus.fte Remote Response"; flow:established,from_server; dsize:9; content:"|05 00 00 00|"; depth:4;
content:"|cd|"; distance:4; within:1; classtype:trojan-activity; reference:url,www.threatexpert.com/threats/virtool-win32-delfsnif-gen.html;
reference:url,doc.emergingthreats.net/2009079; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Delfsnif; sid:2009079; rev:2;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Densmail.com Related Trojan Checkin"; flow:established,to_server; uricontent:"/cc.php"; nocase; uricontent:"v=";
nocase; uricontent:"&rnd="; nocase; pcre:"/v=\d+&rnd=\d+/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007822; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Densmail.com; sid:2007822; rev:2;)

#By Scott Melnick
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Dialer"; flow: established,to_server; uricontent:"/getnumtemp.asp?nip=0"; nocase; classtype:trojan-activity;
reference:url,isc.sans.org/diary.php?storyid=1388; reference:url,doc.emergingthreats.net/2003083; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Dialers;
sid:2003083; rev:3;)

#Matt Jonkman from snadnet data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Dialer-715 Install Checkin"; flow: established,to_server; uricontent:"/perl/invoc_oneway.pl"; nocase; uricontent:"?
id_service="; nocase; uricontent:"&nom_exe="; nocase; uricontent:"&skin="; nocase; uricontent:"&id_produit="; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2003650; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Dialers; sid:2003650; rev:3;)

#by Scott Melnick from sandnet data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Dialer-967 User-Agent"; flow:to_server,established; content:"User-Agent|3a| del|0d 0a|"; nocase; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/2006364; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Dialers; sid:2006364; rev:4;)

#matt jonkman from sandnet data, updated by darren spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Nebuler/Dialer.qn HTTP Request - Checkin"; flow:established,to_server; uricontent:".php?"; uricontent:"c=";
uricontent:"&v="; uricontent:"&b="; uricontent:"&id="; uricontent:"&cnt="; uricontent:"&q="; classtype:trojan-activity; reference:url,www.symantec.com/security_response/writeup.jsp?
docid=2006-051916-2518-99&tabid=2; reference:url,www.microsoft.com/security/portal/Entry.aspx?Name=Trojan%3aWin32%2fNebuler.gen!D; reference:url,www.threatexpert.com/report.aspx?
```

```
md5=e9f1f226ff86e72c558e9a9da32c796d; reference:url,doc.emergingthreats.net/2007743; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Dialers; sid:2007743;
rev:4;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Dialer.MC(vf) HTTP Request - Checkin"; flow:established,to_server; uricontent:".php?"; uricontent:"mode=";
uricontent:"&PartID="; uricontent:"&mac="; content:"|0d 0a|User-Agent|3a| Mozilla/3.0 (compatible|3b| Indy Library)|0d 0a|"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2007913; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Dialers; sid:2007913; rev:3;)

#by Deapesh Misra
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Dialer.Trojan Activity"; flow: to_server,established; uricontent:"/dialer_min/getnum.asp?nip"; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/2008345; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Dialers; sid:2008345; rev:2;)

#by jholguin
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Dialer.buv Sending Information Home"; flow:established,to_server; uricontent:"/exit.php?if="; nocase;
content:"&cl="; content:"&id="; content:"&ov="; content:"&site="; content:"&tk="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008430;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Dialers; sid:2008430; rev:2;)

#by Marcus at unsober
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32 Dialer Variant"; flow:established,to_server; content:"GET "; depth:4; uricontent:"icp=";
uricontent:"&id_site="; uricontent:"&dl_tracker"; uricontent:"&connection_type="; uricontent:"&asked_mdl_id="; uricontent:"&dialer="; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008441; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Dialers; sid:2008441; rev:3;)

#by pedro marinho
#143fd8452113d6feb651ea89bb5f3e50
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Dialer.Win32.E-Group.n Checkin"; flow:to_server,established; uricontent:"login="; nocase; uricontent:"&brokerid=";
nocase; uricontent:"&extlogin="; nocase; uricontent:"&autosize="; nocase; uricontent:"&icp="; nocase; uricontent:"&id_site="; nocase; uricontent:"&dl_tracker="; nocase;
uricontent:"&connection_type="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008490; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Dialers; sid:2008490; rev:4;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Dropper Checkin (often scripts.dlv4.com related)"; flow:established,to_server; content:"GET "; depth:4;
uricontent:"/Common/module.php?"; nocase; uricontent:"brokerid="; nocase; uricontent:"&product="; nocase; uricontent:"&customid="; nocase; uricontent:"&mediaid="; nocase;
uricontent:"&no_product_name="; nocase; uricontent:"&extlogin="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010458;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Dialers; sid:2010458; rev:5;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Dropper Checkin 2 (often scripts.dlv4.com related)"; flow:established,to_server; content:"GET "; depth:4;
uricontent:"/Common/module.php?"; nocase; uricontent:"&isautogeneratedpage="; nocase; uricontent:"&dialer="; nocase; uricontent:"&p2e="; nocase; uricontent:"&nohit="; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010932; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Dialers; sid:2010932; rev:1;)

#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Diazom Trojan User-Agent in Use (cv_v2.0.1)"; flow:established,to_server; content:"User-agent|3a| cv_v";
classtype:trojan-activity; reference:url,ww.symantec.com/enterprise/security_response/writeup.jsp?docid=2007-032316-0426-99&tabid=2; reference:url,doc.emergingthreats.net/2003598;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Diazom; sid:2003598; rev:4;)

#this is similar to 2008942, but this trojan doesn't add a host header
#by victor julien
#
alert tcp $HOME_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET TROJAN dlink router access attempt"; flow:established,to_server; content:"GET /dlink/hwiz.html HTTP/1.0|0d 0a 0d 0a|";
depth:33; content:!"|0d 0a|Host|3a| "; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008945; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Dlink_Home_Router_Access; sid:2008945; rev:4;)

#by Matt Jonkman
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Donbot Connect to CnC"; flow:established,to_server; dsize:7; content:"HALLO|0d 0a|"; depth:7; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008450; reference:url,blog.fireeye.com/research/2009/10/a-little_more_on_donbot.html;
reference:url,www.avertlabs.com/research/blog/index.php/2009/04/05/donbot-joining-the-club-of-million-dollar-botnets/; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Donbot; sid:2008450; rev:5;)

#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Donbot Report to CnC"; flow:established,to_server; content:"HASH|3a 20|"; depth:6; content:"|0d 0a|ID|3a 20|"; distance:0;
content:"|0d 0a|Session|31 20|"; distance:0; content:"|0d 0a|RBL|3a 20|"; classtype:trojan-activity; reference:url,blog.fireeye.com/research/2009/10/a-little_more_on_donbot.html;
reference:url,www.avertlabs.com/research/blog/index.php/2009/04/05/donbot-joining-the-club-of-million-dollar-botnets/; reference:url,doc.emergingthreats.net/2008451;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Buzus; sid:2008451; rev:3;)

#by: Jeremy Conway at sudosecure.net
#ref: 703432baec9fbd9ffed5fa2af0510166
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader (Win32.Doneltart) Checkin - HTTP GET"; flow:established,to_server; content:"GET "; depth:4;
uricontent:".php?open="; nocase; uricontent:"&myid="; nocase; content:!"|0d 0a|User-Agent|3a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009814;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Doneltart; sid:2009814; rev:3;)

#by Marcus at unsober
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Donkeyp2p Update Detected"; flow:established,to_server; content:"GET "; depth:4; uricontent:"donkeyp2p.php";
uricontent:"?kind="; uricontent:"&args="; uricontent:"&ver="; uricontent:"&uniq="; uricontent:"&dllver="; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008364; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Donkeyp2p; sid:2008364; rev:2;)

#by matt jonkman
#slso called Trojan.Dropper.RRM and Trojan.Win32.Inject.adt
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Dorf/Win32.Inject.adt C&C Communication Outbound"; flow:established,to_server; dsize:16; content:"1SCD|00 00|"; depth:6;
offset:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008031; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Dorf; sid:2008031; rev:3;)

#by matt jonkman
#slso called Trojan.Dropper.RRM and Trojan.Win32.Inject.adt
#
alert tcp $EXTERNAL_NET 1024: -> $HOME_NET any (msg:"ET TROJAN Dorf/Win32.Inject.adt C&C Communication Inbound"; flow:established,from_server; dsize:16; content:"1SCD|00 00|"; depth:6;
offset:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008032; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Dorf; sid:2008032; rev:3;)

#by derran spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Dosenjo/Kvadr Proxy Trojan Activity"; flow:established,to_server; uricontent:"hingDeny="; nocase; uricontent:"&id=";
nocase; pcre:"/\?ca[sc]hingDeny=[0-9A-Za-z]{16}&/U"; classtype:trojan-activity; reference:url,www.f-secure.com/v-descs/trojan-proxy_w32_kvadr_gen!a.shtml;
reference:url,www.threatexpert.com/report.aspx?md5=fd2d6bb1d2a9803c49f1e175d558a934; reference:url,www.threatexpert.com/report.aspx?md5=e4664144f8e95cfec510d5efa24a35e7;
reference:url,doc.emergingthreats.net/2010334; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Dosenjo; sid:2010334; rev:2;)

#Matt Jonkman, thanks to the Clam guys for the information and sample
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader-1355 Checking In"; flow:established,to_server; uricontent:"/adload.php?a1="; nocase; uricontent:"a3=";
nocase; uricontent:"&a4="; nocase; uricontent:"&a5="; nocase; content:!"User-Agent\:"; content:"Host\:"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003408;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader-1355; sid:2003408; rev:3;)

#by axn jxn
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader-5265/Torpig/Anserin/Sinowal Unique UA (MSID)"; flow:established,to_server; content:"User-Agent|3a| MSID
["; nocase; depth:320; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003590; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader-
5265; sid:2003590; rev:6;)
```

```
#by Matt Jonkman
#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader.Dluca HTTP Checkin"; flow:established,to_server; uricontent:"?id={"; nocase; uricontent:"&srv="; nocase;
uricontent:"&ver="; nocase; uricontent:"&docid="; nocase; uricontent:"&time="; nocase; uricontent:"&cstate="; nocase; uricontent:"&state="; nocase; uricontent:"&flash="; nocase;
uricontent:"&pin="; nocase; uricontent:"&OSInfo2="; nocase; uricontent:"&cinfo="; nocase; uricontent:"&smd="; nocase; uricontent:"&rts="; nocase; uricontent:"&retryattempt="; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007595; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader.Dluca; sid:2007595;
rev:4;)

#Sigs for general downloader trojans and worms. Not all get unique names
#by Matt Jonkman. Saw a downloader appending ver7 to the end of a regular UA. No spaces. very unique
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Suspicious User-Agent - Possible Trojan Downloader (ver18/ver19, etc)"; flow:established,to_server; content:"|0d
0a|User-Agent|3a| "; nocase; content:")ver"; within:250; pcre:"/User-Agent\:[^\n]+\)ver\d/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003380;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2003380; rev:7;)

#from castlecops research, http://www.castlecops.com, sig by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader.Small 5ser Agent Detected (NetScafe)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
NetScafe"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003641; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2003641; rev:5;)

#Reports of falsing here, the UA is legit within MS VB stuff. Scheduled to be deleted in a week or so. Do not recommend using this
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader.VB.TX User Agent Detected (Microsoft URL Control)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| Microsoft URL Control -"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003646; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2003646; rev:5;)

#Reports of falsing here, the UA is legit within MS VB stuff. Scheduled to be deleted in a week or so. Do not recommend using this
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Backdoor.Irc.MFV User Agent Detected (IRC-U)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| IRC-U v";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003647; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General;
sid:2003647; rev:5;)

#Reports of falsing here, the UA is legit within MS VB stuff. Scheduled to be deleted in a week or so. Do not recommend using this
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Clicker.BC User Agent Detected (linkrunner)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
linkrunner"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003648; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2003648; rev:5;)

#generic downloader and bot checkin url, found in Backdoor.Win32.Small.or
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Bot Backdoor Checkin/registration Request"; flow:established,to_server; uricontent:"/remote.php?"; nocase;
uricontent:"os="; nocase; uricontent:"&user="; nocase; uricontent:"&status="; nocase; uricontent:"&version="; nocase; uricontent:"&build="; nocase; uricontent:"&uptime="; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006366; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2006366;
rev:4;)

#by Scott Melnick and Andre
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader.Win32.Agent.bwr"; flow:established,to_server; uricontent:"?m="; nocase; uricontent:"&a="; nocase;
uricontent:"&hdd="; nocase; uricontent:"&os="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006377; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2006377; rev:3;)

#from sandnet analysis, by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Matcash or related downloader User-Agent Detected"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| x";
pcre:"/User-Agent\: x\w\wx\w\w\!x\w\wx\w\wx\w\w/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006382; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2006382; rev:7;)

#from sandnet analysis, by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader User-Agent Detected (Windows Updates Manager|3.12|...)"; flow:established,to_server; content:"|0d
0a|User-Agent|3a| Windows Updates Manager|7c|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006387; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2006387; rev:6;)

#from sandnet analysis, by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader User-Agent Detected (ld)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| ld|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006394; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2006394;
rev:5;)

#sandnet analysis, by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader.26001 Url Pattern Detected"; flow:established,to_server; uricontent:"install.php?"; nocase;
uricontent:"wall_id="; nocase; uricontent:"&maddr=0"; nocase; uricontent:"&action="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006400;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2006400; rev:3;)

#sandnet analysis, by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader.26001 Url Pattern Detected (lunch_id)"; flow:established,to_server; uricontent:".php?"; nocase;
uricontent:"aff_id="; nocase; uricontent:"lunch_id="; nocase; uricontent:"&maddr=0"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006401;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2006401; rev:3;)

#from sandnet data, by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader.Win32.Agent.cav Url Pattern Detected (ping)"; flow:established,to_server; uricontent:"/ping/"; nocase;
pcre:"/\/ping\/[0-9a-fA-F]{64}\/[0-9a-fA-F]+\/[0-9a-fA-F]+/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007284; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2007284; rev:3;)

#matt jonkman, from sandnet data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN General Downloader Checkin URL (GUID+)"; flow:established,to_server; uricontent:"&version="; nocase;
uricontent:"&configversion="; nocase; uricontent:"GUID="; nocase; uricontent:"&cmd="; nocase; uricontent:"&p="; nocase; uricontent:"&i="; nocase; uricontent:"&x="; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007577; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2007577;
rev:3;)

#matt jonkman, from sandnet data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN General Downloader or Virut C&C Ack"; flow:established,to_server; uricontent:"uid="; nocase; uricontent:"&version=";
nocase; uricontent:"&actionname="; nocase; uricontent:"&action="; nocase; uricontent:"&success="; nocase; uricontent:"&debug="; nocase; uricontent:"&nocache="; nocase; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/2007587; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2007587; rev:3;)

#Matt Jonkman, from the sandnet
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Suspicious User-Agent - Matcash related Trojan Downloader (Ismazo Advanced Loader)"; flow:established,to_server;
content:"|0d 0a|User-Agent|3a| Ismazo"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2007633; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2007633; rev:6;)

#Matt Jonkman, Trojan-Downloader.Win32.Small.hkp
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Trojan-Downloader.Win32.Small.hkp Checkin via HTTP"; flow:established,to_server; dsize:96; content:"GET /";
depth:5; pcre:"/\/[0-9a-f]{78}\sHTTP/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007755; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2007755; rev:3;)

#By Jeremy Conway - Possible root kit user agent
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN User-agent DownloadNetFile Win32.small.hsh downloader"; flow:established,to_server; content:"GET "; depth:4;
content:"|0d 0a|User-Agent|3A| DownloadNetFile|0D 0A|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007778; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2007778; rev:7;)

#By Jeremy Conway
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Browser HiJacker/Infostealer Stat file"; flow:established,to_server;
content:"|5B00|u|00|p|00|d|00|a|00|t|00|e|005D|"; nocase; content:"v|00|e|00|r|00|="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007777;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2007777; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader General Bot Checking In via HTTP Post (bot_id push)"; flow:established,to_server; content:"POST ";
depth:5; content:"|0d 0a 0d 0a|bot_id="; content:"&build_id="; distance:0; content:"&sport="; distance:0; content:"&hport="; distance:0; content:"&ping="; distance:0; content:"&speed=";
distance:0; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2007831; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General;
sid:2007831; rev:2;)

#matt jonkman, sample marked Trojan-Downloader.Win32.Small.htz by fsecure
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader General Bot Checking In - Possible Win32.Small.htz related"; flow:established,to_server; content:"POST ";
depth:5; uricontent:"?id="; nocase; content:!"|0d 0a|User-Agent|3a| "; content:"|0d 0a 0d 0a|proc=[System Process]|0d 0a|"; content:"|0d 0a|&size="; distance:0; classtype: trojan-
activity; reference:url,doc.emergingthreats.net/2007836; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2007836; rev:3;)

#Matt Jonkman, Kaspersky Trojan-Proxy.Win32.Agent.ty
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Suspicious User-Agent - Possible Trojan Downloader (WinInet)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| WinInet|0d 0a|"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2007837; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2007837; rev:3;)

#Matt Jonkman, Kaspersky Trojan-Proxy.Win32.Agent.blm
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Suspicious User-Agent - Possible Trojan Downloader (Shell)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| Shell|0d 0a|"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2007840; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2007840; rev:3;)

#Matt Jonkman, Kaspersky Trojan-Proxy.Win32.Agent.blm
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Suspicious User-Agent - Possible Trojan-Dropper.Win32.Agent.eut (Yhrbg)"; flow:established,to_server; content:"|0d
0a|User-Agent|3a| Yhrbg|0d 0a|"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2007912; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2007912; rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Suspicious User-Agent - Possible Trojan Downloader (Digital)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| Digital|0d 0a|"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2007923; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2007923; rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Suspicious User-Agent - Possible Trojan Downloader (downloaded)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| downloaded|0d 0a|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007924; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2007924; rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Suspicious User-Agent - Possible Trojan Downloader (wnames)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| wnames|0d 0a|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007925; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2007925; rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Suspicious User-Agent - Possible Trojan Downloader (cv_v5.0.0)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| cv_v"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007926; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2007926; rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader.49651 Checkin"; flow:established,to_server; uricontent:"/boot.php/boot.php?"; nocase;
uricontent:"partner="; nocase; uricontent:"&mac="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007952; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2007952; rev:2;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader.49651 Install Report"; flow:established,to_server; uricontent:"/install.php?"; nocase;
uricontent:"partner="; nocase; uricontent:"&mac="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007953; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2007953; rev:2;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader.49651 Online Report"; flow:established,to_server; uricontent:"/up.html?"; nocase; uricontent:"set=";
nocase; uricontent:"pid="; nocase; uricontent:"&mac="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007954; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2007954; rev:2;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Cygo Checkin"; flow:established,to_server; uricontent:"/count.php?"; nocase; uricontent:"type="; nocase;
uricontent:"partner="; nocase; uricontent:"&mac="; nocase; uricontent:"ver="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007955;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2007955; rev:2;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Common Downloader Trojan Checkin"; flow:established,to_server; uricontent:".php?pid="; nocase; uricontent:"mac=";
nocase; uricontent:"&amd="; nocase; uricontent:"&win64="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007975; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2007975; rev:2;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Suspicious User-Agent - Possible Trojan Downloader (https)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| https|0d 0a|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008019; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2008019; rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN General Downloader URL Pattern (/loader/setup.php)"; flow:established,to_server; uricontent:"/loader/setup.php?id=";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008076; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General;
sid:2008076; rev:2;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader.VB.CEJ HTTP Checkin"; flow:established,to_server; uricontent:"/down"; uricontent:"/down/?";
uricontent:"s="; uricontent:"&t="; uricontent:"&v="; pcre:"/\/down\d+\/down\/\?s=[A-F0-9]+\&t=\d+\/\d+\/20/U"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008087;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2008087; rev:2;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Common Downloader Access Count Tracking URL"; flow:established,to_server; uricontent:"/access_count.html?id=";
nocase; uricontent:"&MAC=0"; nocase; pcre:"/MAC=0[a-f0-9]-[a-f0-9]{2}-[a-f0-9]{2}-[a-f0-9]{2}-[a-f0-9]{2}-[a-f0-9]{2}/Ui"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008132; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2008132; rev:2;)
```

```
#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Common Downloader Install Count Tracking URL"; flow:established,to_server; uricontent:"/install_count.html?id=";
nocase; uricontent:"&MAC=0"; nocase; pcre:"/MAC=0[a-f0-9]-[a-f0-9]{2}-[a-f0-9]{2}-[a-f0-9]{2}-[a-f0-9]{2}-[a-f0-9]{2}/Ui"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008133; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2008133; rev:2;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Common Downloader Install Count Tracking URL (partner)"; flow:established,to_server; content:"GET "; depth:4;
uricontent:"/partner/counter/install.php?pid="; nocase; uricontent:"&cid="; nocase; content:!"|0d 0a|User-Agent|3a| "; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008134; reference:url,www.threatexpert.com/report.aspx?md5=ea70e0971cc490a15e53d24ad6564403; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2008134; rev:4;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Common Downloader Install Report URL"; flow:established,to_server; content:"GET "; depth:4; uricontent:"a="; nocase;
uricontent:"&k="; nocase; uricontent:"&wmid="; nocase; uricontent:"&ucid="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008182;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2008182; rev:2;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Common Downloader Install Report URL (pid - mac)"; flow:established,to_server; content:"GET "; depth:4;
uricontent:"html?"; nocase; uricontent:"set="; nocase; uricontent:"&pid="; nocase; uricontent:"&mac="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008183;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2008183; rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Common Downloader Install Report URL (wmid - ucid)"; flow:established,to_server; content:"GET "; depth:4;
uricontent:"?a="; nocase; uricontent:"&k="; nocase; uricontent:"&wmid="; nocase; uricontent:"&ucid="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008194;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2008194; rev:2;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Common Downloader Install Report URL (farfly checkin)"; flow:established,to_server; content:"GET "; depth:4;
uricontent:"/rpt"; content:!"|0d 0a|User-Agent|3a| Mozilla"; pcre:"/^\/rpt\d/U"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008233;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2008233; rev:6;)

#matt jonkman, re c611990bfb445edf0bea8a63212ad43a
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Trojan-Dropper.Win32.Small.avu HTTP Checkin"; flow:established,to_server; uricontent:"m="; uricontent:"&a=";
uricontent:"&r="; uricontent:"&os="; uricontent:"00000"; pcre:"/\/s_\d\d_\d+\?/U"; pcre:"/&os=[0-9a-z]{40}/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008412;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2008412; rev:2;)

#Jeremy at sudosecure
#ref: f43842845f8d6213dda8d8739ae8a2b9
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader UserAgent(AutoDL\/1.0)"; flow:established,to_server; content:"GET "; depth:4; content:"|0d 0a|User-
Agent|3a| AutoDL/1.0|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008458; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2008458; rev:4;)

#by jholguin
#1982f2f77701dfb0f26f51fc7c2978f2
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Downloader.pgp Checkin"; flow:established,to_server; uricontent:"?id="; uricontent:"&e="; uricontent:"&err=";
uricontent:"&c="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008492; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2008492; rev:2;)

#Sig by Daniel Clemens
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Emo/Downloader.vr Checkin"; flow:established,to_server; content:"GET "; depth:4; uricontent:".php"; uricontent:"v=";
uricontent:"&rs="; uricontent:"&n="; uricontent:"&uid="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008546; reference:url,www.malwaredomainlist.com/mdl.php?
search=emo+&colsearch=All&quantity=50; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2008546; rev:4;)

#by jeremy at sudosecure
#ref: c2a3a87735f8c5e11de82c52c94aefc7
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Generic Dropper HTTP Bot grabbing config"; flow: to_server,established; uricontent:".txt"; nocase;
content:"Pragma|3a| no-cache"; content:"|0d 0a|User-Agent|3a| "; content:"|0d 0a|"; distance:6; within:8; pcre:"/User-Agent\: \d{6}\x0d\x0a/"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008664; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2008664; rev:5;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN General Downloader URL - Post Infection"; flow:established,to_server; uricontent:"/count.jsp?id=";
uricontent:"&mac=0"; uricontent:"te="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008728; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2008728; rev:2;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Generic Downloader Checkin Url Detected"; flow:established,to_server; content:"??IP|3a|"; depth:100; content:"??
IP|3a|"; distance:0; content:"????|3a|"; distance:0; pcre:"/IP\:\d[1,3]\.\d[1,3]\.\d[1,3]\.\d[1,3]/U"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008766;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2008766; rev:3;)

#by robert grabowsky
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader Win32.Small.agoy Checkin"; flow:to_server,established; uricontent:"/?jutr="; nocase; uricontent:"&oo=";
nocase; uricontent:"&ra="; nocase; content:"Host|3A|"; nocase; pcre:"/^Host\x3A\s+[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}/mi"; classtype:trojan-activity;
reference:url,www.threatexpert.com/report.aspx?md5=e491d25d82f4928138a0d8b3a6365c39; reference:url,www.threatexpert.com/reports.aspx?find=%2Fjutr%2F;
reference:url,doc.emergingthreats.net/2008859; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2008859; rev:3;)

#by Marcus at unsober.org
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN General Trojan Downloader"; flow:established,to_server; content:"GET "; depth:4; uricontent:".php?p=";
uricontent:"&s="; uricontent:"&v="; uricontent:"uid="; uricontent:"&q="; pcre:"/\.php\?p=\d+&s=.+&v=\d+&uid=\d+&q=/U"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2009299; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2009299; rev:3;)

#by: Jeremy Conway at sudosecure.net
#ref: 06ace2b012d13f7542bf7f01955b0162
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Common Trojan HTTP GET Logging"; flow:established,to_server; content:"GET "; depth:4; uricontent:"?type="; nocase;
uricontent:"&setup_id="; nocase; uricontent:"&version="; nocase; uricontent:"&os="; nocase; uricontent:"&sp="; nocase; classtype:trojan-activity;
reference:url,www.virustotal.com/analisis/df09ec9ec4e5caa42db9d08e0f9d34b378e301a1eeb3aa1e6dbd0de1aa4a66be-1246158969; reference:url,doc.emergingthreats.net/2009451;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2009451; rev:2;)

#by: Jeremy Conway at sudosecure.net
#ref: bfb38bcac71f7b0430c3445bc2997e4b
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader Checkin - Downloads Rogue Adware "; flow:established,to_server; content:"GET "; depth:4;
uricontent:"AreaID="; nocase; uricontent:"MediaID="; nocase; uricontent:"AdNo="; nocase; uricontent:"OriginalityID="; nocase; uricontent:"Url"; nocase; uricontent:"Mac="; nocase;
uricontent:"Version="; nocase; uricontent:"ValidateCode="; nocase; uricontent:"ParentName="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009526;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2009526; rev:2;)

#by: Jeremy Conway at sudosecure.net
#ref: b19d04dca79aad2513e5f90efef3a6b4
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Generic Downloader Checkin - HTTP GET "; flow:established,to_server; content:"GET "; depth:4; uricontent:".php?";
nocase; uricontent:"machineid="; nocase; uricontent:"pubuserid="; nocase; uricontent:"checkversion="; nocase; content:!"|0d 0a|User-Agent|3a|"; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2009527; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2009527; rev:3;)

#by: Jeremy Conway at sudosecure.net
#ref: 9c93ea44074055aaf22fb56bdec375c5
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Generic Downloader - HTTP POST"; flow:established,to_server; content:"POST "; depth:5; content:"|0d 0a|Content-
Length|3a| 0|0d 0a|"; nocase; uricontent:"mac="; nocase; uricontent:"key="; uricontent:"ver="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009549;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2009549; rev:3;)

#by: Jeremy Conway at sudosecure.net
#ref: 1c97be2e53458bf2367915fc40a51333
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Suspicious User-Agent filled with System Details - GET Request"; flow:established,to_server; content:"GET ";
depth:4; content:"|0d 0a|User-Agent|3a| mac="; nocase; depth:200; content:"&hdid="; nocase; distance:17; within:6; 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; reference:url,doc.emergingthreats.net/2009541; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2009541; rev:3;)

#by: Jeremy Conway at sudosecure.net
#ref: 0f79f76f0ea1d53690ed916142f94083
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Generic Downloader Check-in"; flow:established,to_server; content:"GET "; nocase; depth:4; uricontent:"htm?mac=";
nocase; uricontent:"&os="; nocase; uricontent:"&ver="; nocase; uricontent:"&id="; pcre:"/\?mac=[0-9]*&os=[a-z]*&ver=[0-9]{8}&id=[0-9\.]*/Ui"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2009704; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2009704; rev:2;)

#by: Jeremy Conway at sudosecure.net
#ref: 59c9112d9d39c3051f0c6ae1dd499d97
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader Generic - GET"; flow:established,to_server; content:"GET "; depth:4; uricontent:".php?mode="; nocase;
uricontent:"&port="; nocase; uricontent:"&id="; nocase; uricontent:"&ltime="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009803;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2009803; rev:2;)

#by jerry
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Trojan Downloader Win32/Small.CBA download"; flow:established,to_server; uricontent:"popjs.asp?uid="; nocase;
uricontent:"&tid="; nocase; uricontent:"&l="; nocase; uricontent:"&c="; classtype:trojan-activity; reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?
Name=TrojanDownloader%3AWin32%2FSmall.CBA&ThreatID=-2147372177; reference:url,doc.emergingthreats.net/2010569; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2010569; rev:3;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 81:65535 (msg:"ET TROJAN Downloader.Win32.Small"; flow:established,to_server; content:"GET "; nocase; depth:4; content:"|0d 0a|User-Agent|3a|
MSDN SurfBear|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011269; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2011269; rev:3;)

#by: Jeremy Conway at sudosecure.net
#ref: 0ef0a8a7444bf9c0b0c05209e8b33994
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Screenblaze SCR Related Backdoor - GET"; flow:established,to_server; content:"GET "; depth:4; uricontent:".php?id=";
nocase; uricontent:"&serial="; nocase; uricontent:"ver="; nocase; content:"|0d 0a|User-Agent|3a| WinInetHTTP|0d 0a|"; nocase; classtype:trojan-activity;
reference:url,vil.nai.com/vil/content/v_156782.htm; reference:url,www.spywaredetector.net/spyware_encyclopedia/Backdoor.Prosti.htm;
reference:url,home.mcafee.com/VirusInfo/VirusProfile.aspx?key=207702#none; reference:url,www.threatexpert.com/report.aspx?md5=0bcdc9c2e2102f36f594b9e727dae3c7;
reference:url,doc.emergingthreats.net/2009804; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_ScreenBlaze; sid:2009804; rev:3;)

#Matt Jonkman, found in the sandnet
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Tear Application User-Agent Detected"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| Tear
Application|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007770; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_Tear_App; sid:2007770; rev:4;)

#from the sandnet
#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Agent.cah Checkin Request"; flow:established,to_server; uricontent:"?v="; nocase; uricontent:"&mid="; nocase;
uricontent:"&r1="; nocase; uricontent:"&tm=201"; nocase; uricontent:"&av="; nocase; uricontent:"&os=Windows"; nocase; uricontent:"&uid="; nocase; uricontent:"cht="; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/2007644; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Dropper.Agent.cah; sid:2007644; rev:4;)

#discovered by victor julien, sigs by matt jonkman, interesting one. Uses an html-like tag language on 8181
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Dropper-497 (Yumato) Initial Checkin"; flow:established,to_server; dsize:5; content:"|30 30 30 0d 0a|"; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/bin/view/Main/TrojanDropper497; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Droppers_General; sid:2007917;
rev:2;)

#discovered by victor julien, sigs by matt jonkman, interesting one. Uses an html-like tag language on 8181
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Dropper-497 (Yumato) System Stats Report"; flow:established,to_server; content:"|00 00 00 83|"; depth:4; content:"<CPU>";
content:"</CPU><"; distance:0; content:"<MEM>"; content:"</MEM><"; distance:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/TrojanDropper497;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Droppers_General; sid:2007918; rev:2;)

#discovered by victor julien, sigs by matt jonkman, interesting one. Uses an html-like tag language on 8181
#
alert tcp $EXTERNAL_NET 1024: -> $HOME_NET any (msg:"ET TROJAN Dropper-497 Yumato Reply from server"; flow:established,from_server; content:"YUMATO|0d 0a|1234"; depth:12;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/TrojanDropper497; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Droppers_General; sid:2007919; rev:2;)

#discovered by victor julien, sigs by matt jonkman, interesting one. Uses an html-like tag language on 8181
#
alert tcp $EXTERNAL_NET 1024: -> $HOME_NET any (msg:"ET TROJAN Dropper-497 (Yumato) Status Reply from server"; flow:established,from_server; dsize:4; content:"|32 31 0d 0a|"; depth:4;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/TrojanDropper497; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Droppers_General; sid:2007920; rev:3;)

#matt jonkman, Dropper.Win32.VB.on
#Might be able to http_client_body these matches - but can't tell without pcap....
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Dropper.Win32.VB.on Keylog/System Info Report via HTTP"; flow:established,to_server;
content:"post=============================="; content:"=====|0d 0a|Resource Name "; distance:0; content:"|0d 0a|User Name/Value "; distance:0; content:"************STEAM
PASSWORDS**********"; distance:0; content:"Number of procesor|3a|"; distance:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Droppers_General; sid:2007987; rev:4;)

#matt jonkman Dropper Win32.Small.bfq
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Dropper mdodo.com Related Trojan"; flow:established,to_server; content:"GET "; depth:4; content:"|0d 0a|User-
Agent|3a| Mdodo"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008195; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Droppers_General;
sid:2008195; rev:3;)

#matt jonkman Dropper Win32.Small.bfq
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Dropper 6dzone.com Related Trojan"; flow:established,to_server; content:"GET "; depth:4; content:"|0d 0a|User-
Agent|3a| 6dzone|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008196; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Droppers_General; sid:2008196; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Unknown Dropper Checkin (2)"; flow:established,to_server; content:"POST / HTTP/1.1|0d 0a|"; depth:17; content:!"|0d
0a|User-Agent|3a| "; nocase; content:"|0d 0a 0d 0a|updater_version="; nocase; content:"&updater_lang="; distance:0; nocase; content:"&action_type=log"; distance:0; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010830; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Droppers_General; sid:2010830;
rev:3;)
```

```
#by Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Generic Downloader checkin (3)"; flow:established,to_server; uricontent:".php?"; uricontent:"c_pcode=";
uricontent:"c_pid="; uricontent:"c_kind="; uricontent:"c_mac="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010888; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Droppers_General; sid:2010888; rev:3;)

#Submitted by Tom Fischer, 2006-01-08, updated 4/22/06
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Dumador Reporting User Activity"; flow:established,to_server; uricontent:".php?p="; nocase; uricontent:"?
machineid="; nocase; uricontent:"&connection="; nocase; uricontent:"&iplan="; nocase; classtype:trojan-activity; reference:url,www.norman.com/Virus/Virus_descriptions/24279/;
reference:url,doc.emergingthreats.net/2002763; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Dumador; sid:2002763; rev:4;)

#Submitted 4-6-07 Mark Warren
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Trojan.Duntek establishing remote connection"; flow:established,to_server; uricontent:"rfe.php?"; nocase;
uricontent:"cmp=dun_tekfirst"; nocase; uricontent:"guid="; nocase; classtype:trojan-activity; reference:url,www.symantec.com/security_response/writeup.jsp?docid=2006-102514-0554-99;
reference:url,doc.emergingthreats.net/2003537; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Duntek; sid:2003537; rev:3;)

#By Don Jackson of SecureWorks
#Crafted for the lowest common denominator; should work in most 1.x and later engines, PCRE used for C&C traffic.
#Mostly for spotting it's use on your network. Only one DDoS rule. Be careful of the number/rate of alerts; these do not use thresholding.
#DNS left in hex to avoid advertising the domains to the bad guys via google
#these first few are for specific domains, to be removed in the not too distant future
#
alert tcp $HOME_NET any -> any 53 (msg:"ET TROJAN E-Jihad 3.0 DNS Activity TCP (1)"; flow:established,to_server; content:"|08616c2d6a696e616e036e65740000010001|"; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/bin/view/Main/EJihadHackTool; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_E-Jihad; sid:2007673; rev:6;)

#By Don Jackson of SecureWorks
#Crafted for the lowest common denominator; should work in most 1.x and later engines, PCRE used for C&C traffic.
#Mostly for spotting it's use on your network. Only one DDoS rule. Be careful of the number/rate of alerts; these do not use thresholding.
#DNS left in hex to avoid advertising the domains to the bad guys via google
#these first few are for specific domains, to be removed in the not too distant future
#
alert tcp $HOME_NET any -> any 53 (msg:"ET TROJAN E-Jihad 3.0 DNS Activity TCP (2)"; flow:established,to_server; content:"|0861312d6a696e616e036e65740000010001|"; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/bin/view/Main/EJihadHackTool; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_E-Jihad; sid:2007674; rev:6;)

#By Don Jackson of SecureWorks
#Crafted for the lowest common denominator; should work in most 1.x and later engines, PCRE used for C&C traffic.
#Mostly for spotting it's use on your network. Only one DDoS rule. Be careful of the number/rate of alerts; these do not use thresholding.
#DNS left in hex to avoid advertising the domains to the bad guys via google
#these first few are for specific domains, to be removed in the not too distant future
#
alert tcp $HOME_NET any -> any 53 (msg:"ET TROJAN E-Jihad 3.0 DNS Activity TCP (3)"; flow:established,to_server; content:"|06617264647261046 86f737402736b0000010001|"; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/bin/view/Main/EJihadHackTool; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_E-Jihad; sid:2007675; rev:6;)

#By Don Jackson of SecureWorks
#Crafted for the lowest common denominator; should work in most 1.x and later engines, PCRE used for C&C traffic.
#Mostly for spotting it's use on your network. Only one DDoS rule. Be careful of the number/rate of alerts; these do not use thresholding.
#DNS left in hex to avoid advertising the domains to the bad guys via google
#these first few are for specific domains, to be removed in the not too distant future
#
alert tcp $HOME_NET any -> any 53 (msg:"ET TROJAN E-Jihad 3.0 DNS Activity TCP (4)"; flow:established,to_server; content:"|03777777056a6f2d7566036e65740000010001|"; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/bin/view/Main/EJihadHackTool; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_E-Jihad; sid:2007676; rev:6;)

#By Don Jackson of SecureWorks
#Crafted for the lowest common denominator; should work in most 1.x and later engines, PCRE used for C&C traffic.
#Mostly for spotting it's use on your network. Only one DDoS rule. Be careful of the number/rate of alerts; these do not use thresholding.
#DNS left in hex to avoid advertising the domains to the bad guys via google
#these first few are for specific domains, to be removed in the not too distant future
#
alert tcp $HOME_NET any -> any 53 (msg:"ET TROJAN E-Jihad 3.0 DNS Activity TCP (5)"; flow:established,to_server; content:"|037777770c6a6f66706d7579747276636603636f6d0000010001|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/EJihadHackTool; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_E-Jihad;
sid:2007677; rev:6;)

#By Don Jackson of SecureWorks
#Crafted for the lowest common denominator; should work in most 1.x and later engines, PCRE used for C&C traffic.
#Mostly for spotting it's use on your network. Only one DDoS rule. Be careful of the number/rate of alerts; these do not use thresholding.
#DNS left in hex to avoid advertising the domains to the bad guys via google
#these first few are for specific domains, to be removed in the not too distant future
#
alert udp $HOME_NET any -> any 53 (msg:"ET TROJAN E-Jihad 3.0 DNS Activity UDP (1)"; content:"|08616c2d6a696e616e036e65740000010001|"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/EJihadHackTool; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_E-Jihad; sid:2007678; rev:6;)

#By Don Jackson of SecureWorks
#Crafted for the lowest common denominator; should work in most 1.x and later engines, PCRE used for C&C traffic.
#Mostly for spotting it's use on your network. Only one DDoS rule. Be careful of the number/rate of alerts; these do not use thresholding.
#DNS left in hex to avoid advertising the domains to the bad guys via google
#these first few are for specific domains, to be removed in the not too distant future
#
alert udp $HOME_NET any -> any 53 (msg:"ET TROJAN E-Jihad 3.0 DNS Activity UDP (2)"; content:"|0861312d6a696e616e036e65740000010001|"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/EJihadHackTool; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_E-Jihad; sid:2007679; rev:6;)

#By Don Jackson of SecureWorks
#Crafted for the lowest common denominator; should work in most 1.x and later engines, PCRE used for C&C traffic.
#Mostly for spotting it's use on your network. Only one DDoS rule. Be careful of the number/rate of alerts; these do not use thresholding.
#DNS left in hex to avoid advertising the domains to the bad guys via google
#these first few are for specific domains, to be removed in the not too distant future
#
alert udp $HOME_NET any -> any 53 (msg:"ET TROJAN E-Jihad 3.0 DNS Activity UDP (3)"; content:"|06617264647261046 86f737402736b0000010001|"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/EJihadHackTool; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_E-Jihad; sid:2007680; rev:6;)

#By Don Jackson of SecureWorks
#Crafted for the lowest common denominator; should work in most 1.x and later engines, PCRE used for C&C traffic.
#Mostly for spotting it's use on your network. Only one DDoS rule. Be careful of the number/rate of alerts; these do not use thresholding.
#DNS left in hex to avoid advertising the domains to the bad guys via google
#these first few are for specific domains, to be removed in the not too distant future
#
alert udp $HOME_NET any -> any 53 (msg:"ET TROJAN E-Jihad 3.0 DNS Activity UDP (4)"; content:"|03777777056a6f2d7566036e65740000010001|"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/EJihadHackTool; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_E-Jihad; sid:2007681; rev:6;)

#By Don Jackson of SecureWorks
#Crafted for the lowest common denominator; should work in most 1.x and later engines, PCRE used for C&C traffic.
#Mostly for spotting it's use on your network. Only one DDoS rule. Be careful of the number/rate of alerts; these do not use thresholding.
#DNS left in hex to avoid advertising the domains to the bad guys via google
#these first few are for specific domains, to be removed in the not too distant future
#
alert udp $HOME_NET any -> any 53 (msg:"ET TROJAN E-Jihad 3.0 DNS Activity UDP (5)"; content:"|037777770c6a6f66706d7579747276636603636f6d0000010001|"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/EJihadHackTool; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_E-Jihad; sid:2007682; rev:6;)

#these are more permanent, C&C related
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN E-Jihad 3.0 HTTP Activity 1"; flow:established,to_server; content:"GET "; depth:4; uricontent:"/tlog.php?logn=";
pcre:"/GET /tlog\.php?logn=[^\s]+&pss=[^\s]+\sHTTP/1\.[0|1]\x0D\x0A/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/EJihadHackTool;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_E-Jihad; sid:2007683; rev:6;)

#these are more permanent, C&C related
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN E-Jihad 3.0 HTTP Activity 2"; flow:established,to_server; content:"GET "; depth:4; uricontent:"/ntarg.php?";
pcre:"/GET /ntarg\.php?[^\s]*(notdoing=|howme=|uname=)[^\s]*\sHTTP/1\.[0|1]\x0D\x0A/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/EJihadHackTool;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_E-Jihad; sid:2007684; rev:6;)

#these are more permanent, C&C related
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN E-Jihad 3.0 HTTP Activity 3"; flow:established,to_server; content:"GET "; depth:4; uricontent:"/tnewu.php?nlogin=";
pcre:"/GET /tnewu.php?nlogin=[^\s]+&npss=[^\s]+&invitedby=[^\s]+\sHTTP/1\.[0|1]\x0D\x0A/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/EJihadHackTool;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_E-Jihad; sid:2007685; rev:6;)

#these are more permanent, C&C related
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN E-Jihad 3.0 DDoS HTTP Activity OUTBOUND"; flow:established,to_server; content:"GET "; offset:0; depth:4;
content:"|0d 0a|User-Agent|3a| Attacker|0d 0a|"; offset:14; classtype:denial-of-service; reference:url,doc.emergingthreats.net/bin/view/Main/EJihadHackTool;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_E-Jihad; sid:2007686; rev:7;)

#these are more permanent, C&C related
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET TROJAN E-Jihad 3.0 DDoS HTTP Activity INBOUND"; flow:established,to_server; content:"GET "; depth:4; content:"|0d
0a|User-Agent|3a| Attacker|0d 0a|"; offset:14; classtype:denial-of-service; reference:url,doc.emergingthreats.net/bin/view/Main/EJihadHackTool;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_E-Jihad; sid:2007687; rev:9;)

#by Daniel Clemens
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN Likely EXE Cryptor Packed Binary - Likely Malware"; flow:from_server,established; content:"|4D 5A|"; content:"|2E 70 61 63
6B 65 64|"; within: 447; classtype:trojan-activity; reference:url,bits.packetninjas.org; reference:url,doc.emergingthreats.net/2008557; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_EXE_Cryptor_Packed; sid:2008557; rev:2;)

#by Veerendra at secpod
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET TROJAN Likely eCard Malware Laden Email Inbound"; flow:established,to_server; content:"|0d 0a|Subject|3a| You have received an
eCard"; nocase; content:"e-card.zip"; nocase; classtype:trojan-activity; reference:url,www.sophos.com/blogs/gc/g/2008/10/15/you-have-not-received-an-ecard/;
reference:url,doc.emergingthreats.net/2008674; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Ecard_General; sid:2008674; rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN Egspy Infection Report Email"; flow:established,to_server; content:"FROM\: EgySpy Victim"; content:"TO|3a| EgySpy User";
distance:0; content:"SUBJECT|3a| E g y S p y KeyLogger"; distance:0; classtype:trojan-activity; reference:url,research.sunbelt-software.com/threatdisplay.aspx?
name=EgySpy&threatid=48410; reference:url,doc.emergingthreats.net/2008039; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Egyspy; sid:2008039; rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Egspy Infection Report via HTTP"; flow:established,to_server; uricontent:"/keylogkontrol/"; content:"|0d 0a|User-
Agent|3a| Mozilla/3.0 (compatible|3b| Indy Library)"; classtype:trojan-activity; reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=EgySpy&threatid=48410;
reference:url,doc.emergingthreats.net/2008047; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Egyspy; sid:2008047; rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Egspy Install Report via HTTP"; flow:established,to_server; uricontent:"/control.php?pcad="; nocase;
uricontent:"&tarih="; nocase; uricontent:"&saat="; nocase; uricontent:"&veri="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008136;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Egyspy; sid:2008136; rev:2;)

#by Matt Jonkman, from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Eldorado.BHO User-Agent Detected (netcfg)"; flow:established,to_server; content:"GET "; depth:4; content:"|0d
0a|User-Agent|3a| netcfg|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007758; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Eldorado; sid:2007758; rev:5;)

#by Matt Jonkman, from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Eldorado.BHO User-Agent Detected (MSIE 5.5)"; flow:established,to_server; content:"GET "; depth:4; content:"|0d
0a|User-Agent|3a| MSIE 5.5|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007833; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Eldorado; sid:2007833; rev:3;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Eleonore Exploit Pack activity"; flow:established,to_server; uricontent:"?spl="; uricontent:"&br=";
uricontent:"&vers="; uricontent:"&s="; pcre:"/\?spl=\d+&br=[A-Za-z]+&vers=\d\.\d&s=[a-z0-9]+[^&]$/U"; classtype:trojan-activity; reference:url,www.offensivecomputing.net/?q=node/1419;
reference:url,doc.emergingthreats.net/2010248; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Eleaonore; sid:2010248; rev:2;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Eleonore Exploit Pack activity variant May 2010"; flow:established,to_server; uricontent:".php?spl="; pcre:"/\?
spl=MS[0-9]{2}-[0-9]{3}$/U"; classtype:trojan-activity; reference:url,www.offensivecomputing.net/?q=node/1419; reference:url,doc.emergingthreats.net/2010248;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Eleaonore; sid:2011128; rev:1;)

#by Chich Thierry
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET TROJAN elitekeylogger v1.0 reporting - Inbound"; flow:established,to_server; content:"MAIL FROM|3a|<logs@logs.com>";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2002938; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_EliteKeyLogger; sid:2002938; rev:5;)

#by Chich Thierry
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN elitekeylogger v1.0 reporting - Outbound"; flow:established,to_server; content:"MAIL FROM|3a|<logs@logs.com>";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2002941; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_EliteKeyLogger; sid:2002941; rev:5;)

#marcus at unsober, update by darren spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Emo/Downloader.uxk checkin"; flow:established,to_server; content:"GET "; depth:4; uricontent:".php";
uricontent:"v="; uricontent:"&id="; uricontent:"&rs="; uricontent:"&cc="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008452;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Downloader_General; sid:2008452; rev:4;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Emogen Reporting via HTTP"; flow:established,to_server; uricontent:".asp?"; nocase; uricontent:"mac="; nocase;
uricontent:"&name="; nocase; uricontent:"&p="; nocase; uricontent:"&id="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007986;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Emogen; sid:2007986; rev:2;)

#another one. Fortinet calls it emogen, others call it a dropper
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Emogen Infection Checkin Initial Packet"; flow:established,to_server; dsize:<100; content:"|00 00 00 00 00 00|WindowsXP|00
00 00|"; flowbits:set,ET.emogen1; flowbits:noalert; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008269; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Emogen; sid:2008269; rev:3;)

#another one. Fortinet calls it emogen, others call it a dropper
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Emogen Infection Checkin CnC Keepalive"; flow:established,to_server; flowbits:isset,ET.emogen1; dsize:4; content:"test";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008270; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Emogen; sid:2008270; rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN my247eshop.com User-Agent"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| EShopee|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008243; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Eshop; sid:2008243; rev:3;)

#from sandnet, by Matt Jonkman
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN ExplorerHijack Trojan HTTP Checkin"; flow:established,to_server; uricontent:"php?i="; uricontent:"&v=";
uricontent:"&win=Windows"; uricontent:"&un="; uricontent:"&uv="; uricontent:"&s="; uricontent:"&onl="; uricontent:"&ip="; uricontent:"&f="; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2007700; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_ExplorerHijack; sid:2007700; rev:3;)

#moved over from corpsespyware
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN FSG Packed Binary via HTTP Inbound"; flow:from_server,established; content:"|4D 5A|"; content:"|50 45 00 00 4C 01
02 00 46 53 47 21|"; distance:10; classtype:trojan-activity; reference:url,www.securityfocus.com/infocus/1745; reference:url,doc.emergingthreats.net/2002773;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_FSG_Packer; sid:2002773; rev:6;)

#by Nathaniel Richmond
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Rogue A/V Win32/FakeXPA GET Request"; flow:to_server,established; uricontent:"?campaign="; uricontent:"&country=";
uricontent:"&counter="; uricontent:"&campaign="; uricontent:"&landid="; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2009209;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_FakeXPA; sid:2009209; rev:2;)

#by: Jeremy Conway at sudosecure.net
#ref: 4da33fd42d70397965a4e9866f57a936
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN FAKE/ROGUE AV HTTP Post"; flow:established,to_server; content:"POST "; depth:5; content:"mid="; content:"&wv=";
content:"&r="; content:"&tp="; content:"&exe="; content:"&ls="; content:"&uid="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009514;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Fake_AV; sid:2009514; rev:2;)

#by: Jeremy Conway at sudosecure.net
#ref: 8db2fc67da6106116d781d25289cb2ac
#9a023ed592a1a9ae2300b73b670a6754 951ab9f79e56b65e73188288f9c5c87e
#c258b4e02079e1c8c464736348e99a15
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN FAKE/ROGUE AV - Encoded (data=) HTTP POST"; flow:established,to_server; content:"POST "; depth:5; content:"|0d
0a|Cache-Control|3a 20|no-cache|0d 0a 0d 0a|data=/CjEfcLas0KCj/"; nocase; depth:400; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009553;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Fake_AV; sid:2009553; rev:2;)

#by: Jeremy Conway at sudosecure.net
#ref: bb3a670a8ac402be2c3b0d8f8043c3c3
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN FAKE/ROGUE AV/Security Application Checkin"; flow:established,to_server; content:"GET "; nocase; depth:4;
uricontent:"?url="; nocase; uricontent:"&affid="; nocase; content:"|0d 0a|User-Agent|3a| Mozilla/5.0 (compatible|3b| MSIE 6.0|3b| Windows XP)|0d 0a|"; nocase; pcre:"/\?url=[0-9]&affid=
[0-9]{5}/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009554; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Fake_AV; sid:2009554;
rev:3;)

#By Darren Spruell 2009-11-20
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Fake/Rogue AV Landing Page Encountered"; flow:established,to_server; uricontent:".php?"; nocase; uricontent:"land=";
nocase; uricontent:"affid="; nocase; pcre:"/\.php\?(land=\d+|affid=\d{5})&(land=\d+|affid=\d{5})$/Ui"; classtype:trojan-activity; reference:url,en.wikipedia.org/wiki/Scareware;
reference:url,doc.emergingthreats.net/2010347; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Fake_AV; sid:2010347; rev:3;)

#by evilghost and mike cox
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN FakeAV FakeSmoke HTTP POST check-in"; flow:established,to_server; content:"POST "; nocase; depth:5; content:!"|0d
0a|User-Agent|3a| "; nocase; content:!"|0d 0a|Referer|3a| "; nocase; content:"|0d 0a|User-Agent|3a| Microsoft Internet Explorer|0d 0a|"; nocase; uricontent:"loads2.php?r="; nocase; pcre:"/loads2\.php\?r=[0-9]{2}\.
[0-9]+/Ui"; classtype:trojan-activity; reference:url,isc.sans.org/diary.html?storyid=7768; reference:url,doc.emergingthreats.net/2010512; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Fake_AV;
sid:2010512; rev:6;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Potential FakeAV HTTP POST Check-IN (?r=)"; flow:established,to_server; content:"POST "; nocase; depth:5;
content:!"|0d 0a|Referer|3a| "; nocase; content:"|0d 0a|User-Agent|3a| Microsoft Internet Explorer|0d 0a|"; nocase; uricontent:"loads2.php?r="; nocase; pcre:"/loads2\.php\?r=[0-9]{2}\.
[0-9]+/Ui"; classtype:trojan-activity; reference:url,www.threatexpert.com/report.aspx?md5=94e13e13c6da5e32bde00bc527475bd2; reference:url,www.malwaredomainlist.com/forums/index.php?
topic=3190.420; reference:url,doc.emergingthreats.net/2010594; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Fake_AV; sid:2010594; rev:3;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Potential FakeAV HTTP GET Check-IN (/check)"; flow:established,to_server; content:"GET /check HTTP/1."; nocase;
content:!"|0d 0a|Referer|3a| "; nocase; content:"|0d 0a|User-Agent|3a| Microsoft Internet Explorer|0d 0a|"; nocase; classtype:trojan-activity;
reference:url,www.threatexpert.com/report.aspx?md5=94e13e13c6da5e32bde00bc527475bd2; reference:url,www.malwaredomainlist.com/forums/index.php?topic=3190.420;
reference:url,doc.emergingthreats.net/2010597; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Fake_AV; sid:2010597; rev:3;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN FakeAV Landing Page (aid,sid)"; flow:established,to_server; content:"GET "; nocase; depth:4; content:!"|0d
0a|Referer|3a| "; nocase; uricontent:".php?aid="; nocase; uricontent:"&sid="; nocase; pcre:"/[a-z]+\.php\?aid=\d+&sid=[a-z0-9]+$/Ui"; classtype:trojan-activity;
reference:url,www.bleepingcomputer.com/forums/lofiversion/index.php/t247125.html; reference:url,doc.emergingthreats.net/2010625; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Fake_AV; sid:2010625; rev:4;)

#by packet hack
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Likely FakeAV/Fakeinit/FraudLoad Checkin"; flow:established,to_server; content:"GET "; nocase; depth:4;
content:!"|0d 0a|Referer|3a| "; nocase; uricontent:"loads.php?code="; nocase; pcre:"/loads\.php\?code=\d+$/Ui"; classtype:trojan-activity;
reference:url,www.threatexpert.com/report.aspx?md5=f5e907a11831c757a94cde9257b3574c; reference:url,doc.emergingthreats.net/2010626; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Fake_AV; sid:2010626; rev:4;)

#by packet hack
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Likely FakeAV/Fakeinit/FraudLoad Checkin"; flow:established,to_server; content:"GET "; nocase; depth:4;
content:!"|0d 0a|Referer|3a| "; nocase; uricontent:"cgi-bin/download.pl?code="; nocase; pcre:"/download\.pl\?code=\d+$/Ui"; classtype:trojan-activity;
reference:url,www.threatexpert.com/report.aspx?md5=f5e907a11831c757a94cde9257b3574c; reference:url,doc.emergingthreats.net/2010627; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Fake_AV; sid:2010627; rev:4;)

#by packet hack
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Likely FakeAV/Fakeinit/FraudLoad Checkin"; flow:established,to_server; content:"GET "; nocase; depth:4;
content:!"|0d 0a|Referer|3a| "; nocase; uricontent:"cgi-bin/get.pl?l="; nocase; pcre:"/get\.pl\?l=\d+$/Ui"; classtype:trojan-activity; reference:url,www.threatexpert.com/report.aspx?
md5=f5e907a11831c757a94cde9257b3574c; reference:url,doc.emergingthreats.net/2010628; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Fake_AV; sid:2010628;
rev:4;)

#by Steven Adair at shadowserver
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN FakeAV Reporting - POST often to resolution|borders.php"; flow:to_server,established; content:"POST /"; depth:6;
content:"|0d 0a|Cache-Control|3a| no-cache|0d 0a 0d 0a|"; within:300; content:"|0d 0a 0d 0a|data="; distance:0; pcre:"/data=[a-zA-Z0-9\+\/]{64}/"; classtype:trojan-activity;
reference:url,www.sophos.com/security/analyses/viruses-and-spyware/trojagentmbr.html?_log_from=rss; reference:url,doc.emergingthreats.net/2010337;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Fake_AV; sid:2010337; rev:11;)

#2010-07-12 by Eoin Miller
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN FakeAV Served To Client"; flow:established,to_client; content:"HTTP/1"; depth:6; content:"Content-Disposition|3a|
attachment|3b| filename="; nocase; content:"|0D 0A|Set-Cookie|3a| ds=1|0D 0A|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011221;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Fake_AV; sid:2011221; rev:1;)

#by kevin ross
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Possible Fake-Rean Installer Activity (Malwareurl.com Top 30)"; flow:to_server;
uricontent:"|2F|installer|2F|Installer|2E|exe"; nocase; pcre:"/[1-3]\x2Finstaller\x2FInstaller\x2Eexe/Ui"; classtype:trojan-activity;
reference:url,www.sophos.com/security/analyses/viruses-and-spyware/trojfakereane.html?_log_from=rss; reference:url,doc.emergingthreats.net/2010221;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Fakerean; sid:2010221; rev:3;)

#this sig is experimental. It appears to use a base64 encoded user-agent
#it's very long, no spaces or punctuation, which is what we can key on
#please report load or fp problems
```

```
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Farfli User Agent Detected"; flow:established,to_server; uricontent:"/rpt"; content:"|0d 0a|User-Agent|3a| ";
content:!"|0d 0a|User-Agent|3a| Mozilla"; pcre:"/\x0a\x0aUser-Agent\x3a [a-z0-9]{92}/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007646;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Farfli; sid:2007646; rev:5;)

#by Jeffrey Brown
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Farfli HTTP Checkin Activity"; flow: to_server,established; uricontent:"/getmac.asp"; nocase; content:"x="; nocase;
content:"&y="; nocase; content:"&z="; pcre:"/x=[a-f0-9]{2}-[a-f0-9]{2}-[a-f0-9]{2}-[a-f0-9]{2}-[a-f0-9]{2}-[a-f0-9]{2}-/Ui"; classtype:trojan-activity;
reference:url,www.virustotal.com/analisis/3b532a7bf7850483882024652f6c8a8b; reference:url,doc.emergingthreats.net/2009215; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Farfli; sid:2009215; rev:3;)

#by: Jeremy Conway at sudosecure.net
#ref: a93af8f350689c700ee3fde7442a956e
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Fasec/FakeAV Alert/Keylogger/Dropper/DNSChanger Possible Rootkit - HTTP GET"; flow:established,to_server;
content:"GET "; depth:4; uricontent:"Command="; nocase; uricontent:"snNO="; nocase; uricontent:"Encode="; nocase; uricontent:"SFBH"; nocase; classtype:trojan-activity;
reference:url,www.avast.com/eng/win32-fasec.html; reference:url,www.threatexpert.com/threats/virus-win32-fasec.html; reference:url,doc.emergingthreats.net/2009472;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Fasec; sid:2009472; rev:2;)

#by matt jonkman, from sandnet data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Feral Checkin via HTTP"; flow:established,to_server; uricontent:"?ucid="; nocase; uricontent:"&wmid="; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007286; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Feral; sid:2007286; rev:3;)

#by pmarinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Trojan-Dropper.Win32.Flystud"; flow:to_server,established; uricontent:"loading.html?fn="; nocase;
uricontent:"&pid="; nocase; uricontent:"&mid="; nocase; uricontent:"&cid="; nocase; uricontent:"&pn="; nocase; uricontent:"&clientid="; nocase; uricontent:"channel="; nocase;
uricontent:"&stn="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011086; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Flystud;
sid:2011086; rev:3;)

#by chodelmort and eg
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Fragus Exploit Kit Landing"; flow:established,to_server; uricontent:".php?"; nocase; uricontent:"id="; nocase;
uricontent:"pid="; nocase; uricontent:"hello="; nocase; pcre:"/\.php\?(id=|pid=|hello=)\d+&(id=|pid=|hello=)\d+&(id=|pid=|hello=)\d+$/Ui"; classtype:trojan-activity;
reference:url,jsunpack.jeek.org/dec/go?report=d6034485132221810807 6f1ad8d21435de9d5b7c; reference:url,www.malwareurl.com; reference:url,doc.emergingthreats.net/2011693;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Fragus; sid:2011693; rev:2;)

#by Marcus at unsober
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN FraudLoad.aww HTTP CnC Post"; flow:established,to_server; content:"POST "; depth:5; uricontent:"/instlog/?"; nocase;
content:"|0d 0a|User-Agent|3a| Mozilla/3.0 (compatible|3b| TALWinInetHTTPClient"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008322;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Fraudload; sid:2008322; rev:5;)

#by: Jeremy Conway at sudosecure.net
#ref: 3f778132d4d30bd0db897adfdae1f74e
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN FAKE AV HTTP CnC Post"; flow:established,to_server; content:"POST "; depth:5; content:"action="; nocase;
content:"uid="; nocase; within:10; content:"cnt="; nocase; content:"lng="; nocase; content:"type="; nocase; within:10; content:"user_id="; nocase; content:"pc_id="; nocase;
content:"abbr="; nocase; content:"|0d 0a|User-Agent|3a| Mozilla/3.0 (compatible|3b| TALWinInetHTTPClient)"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009455;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Fraudload; sid:2009455; rev:3;)

#by: Jeremy Conway at sudosecure.net
#ref: 3f68543ffe8862c57bebfb8732a1e716
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Fraudload/FakeAlert/FakeVimes Downloader - POST"; flow:established,to_server; content:"POST "; nocase; depth:5;
content:"|0d 0a|User-Agent|3a| Mozilla/3.0 (compatible|3b| TALWinInetHTTPClient)|0d 0a|"; nocase; content:"|0d 0a 0d 0a|verint="; nocase; content:"&wv="; nocase; within:10;
content:"&report="; nocase; within:20; content:"&abbr="; nocase; content:"&pid="; classtype:trojan-activity; reference:url,www.pctools.com/mrc/infections/id/Trojan-
Downloader.FraudLoad/; reference:url,www.threatexpert.com/reports.aspx?find=Trojan-Downloader.FraudLoad; reference:url,doc.emergingthreats.net/2009751;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Fraudload; sid:2009751; rev:4;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Fruspam polling for IP likely infected"; flow:established,to_server; content:"GET "; nocase; depth:4;
uricontent:"/automation/n09230945.asp"; content:"|0d 0a|User-Agent|3a| Mozilla/5.0 (X11|3b| U|3b| Linux i686|3b| en-US|3b| rv|3a|1.9.0.4) Ubuntu/8.04 (hardy) Firefox/3.0.0|0d 0a 0d
0a|"; classtype:trojan-activity; reference:url,community.ca.com/blogs/securityadvisor/archive/2009/03/26/in-the-wild-win32-fruspam-using-american-greetings.aspx;
reference:url,doc.emergingthreats.net/2011072; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Fruspam; sid:2011072; rev:2;)

#by Philipp Bescht
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Fullspace.cc or Related Checkin (1)"; flow:established,to_server; uricontent:"/config.php?ver="; nocase;
uricontent:"&uid="; nocase; uricontent:"&action="; nocase; uricontent:"&ras="; nocase; uricontent:"&verfull="; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008397; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Fullspace.cc; sid:2008397; rev:2;)

#by Philipp Bescht
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Fullspace.cc or Related Checkin (2)"; flow:established,to_server; uricontent:"/register."; nocase; uricontent:"?
id="; nocase; uricontent:"&port="; nocase; uricontent:"&connect="; nocase; uricontent:"&ver="; nocase; uricontent:"ip="; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008398; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Fullspace.cc; sid:2008398; rev:2;)

#by marcus at unsober
#re: db3084220f85632b0eade6c759918ee6
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Gaboc Trojan Check-in"; flow:established,to_server; content:"GET "; depth:4; uricontent:".asp"; uricontent:"?type=";
uricontent:"&machinename="; classtype:trojan-activity; reference:url,www.threatexpert.com/report.aspx?md5=6e871b9c440d5c77b9158ebcbe3fcd4b;
reference:url,doc.emergingthreats.net/2009519; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Gaboc; sid:2009519; rev:3;)

#spyware/trojan/backdoors all reported here. sig by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Gadu-Gadu Chat Client Checkin via HTTP"; flow:established,to_server; uricontent:"/appsvc/appmsg"; nocase;
uricontent:"fmnumber="; nocase; uricontent:"&version="; nocase; uricontent:"&fmt="; nocase; uricontent:"&lastmsg="; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2007866; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Gadu-gadu.pl; sid:2007866; rev:6;)

#by Marcus at unsober
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN PWS.Gamania Checkin"; flow:established,to_server; content:"POST "; depth:5; content:"|0d 0a 0d 0a|"; content:"un=";
distance:0; content:"&pw="; distance:0; content:"&sn="; distance:0; content:"&l="; distance:0; content:"&gd1="; distance:0; content:"&pn="; distance:0; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008431; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Gamania; sid:2008431; rev:4;)

#by victor julien
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Trojan-GameThief.Win32.OnLineGames infection report"; flow:established,to_server; content:"POST "; depth:5;
content:"&hAssunto=infect-"; distance:50; within:400; content:"&hCorpo="; distance:0; within:50; content:"&hPara="; distance:0; within:50; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008984; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Gamethief; sid:2008984; rev:3;)

#by marcus at unsober
#re: ee1539a7b6b7012a68b986262f01756c
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Gamania Trojan Check-in"; flow:established,to_server; content:"GET "; depth:4; uricontent:".php"; uricontent:"?p4=";
uricontent:"&p5="; uricontent:"&hs="; pcre:"/p4=\d+&p5=\d+&hs=\d+/Ui"; classtype:trojan-activity; reference:url,home.mcafee.com/VirusInfo/VirusProfile.aspx?key=166939;
reference:url,doc.emergingthreats.net/2009531; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Garmania; sid:2009531; rev:4;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Potential Gemini Malware Download"; flow:established,to_server; content:"GET "; depth:4; uricontent:".php?
cmd=getFile&counter="; uricontent:"&p="; pcre:"/\.php\?cmd=getFile&counter=\d+&p=/U"; classtype:trojan-activity;
```

```
reference:url,www.virustotal.com/analisis/c36e206c6dfe88345815da41c1b14b4f33a9636ad94dd46ce48f5b367f1c736c-1254242791; reference:url,doc.emergingthreats.net/2010007;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Gemini; sid:2010007; rev:5;)

#by Mike Cox
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Potential Gemini/Fake AV Download URL Detected"; flow:established,to_server;
uricontent:"/Layouts/Landings/CentralLandings/"; nocase; uricontent:"/images/"; nocase; pcre:"/\x2FLayouts\x2FLandings\x2FCentralLandings\x2F\d+\x2Fimages\x2F/Ui"; classtype:trojan-
activity; reference:url,www.virustotal.com/analisis/c36e206c6dfe88345815da41c1b14b4f33a9636ad94dd46ce48f5b367f1c736c-1254242791; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Gemini; reference:url,doc.emergingthreats.net/2010450; sid:2010450; rev:2;)

#Matt Jonkman
#General signs of trojan infections....
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN GENERAL Possible Trojan Sending Initial Email to Owner - INFECTADO"; flow:established,to_server; content:"Subject|3a|
Microsoft Windows"; nocase; content:"INFECTADO"; nocase; within:20; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2002982; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_General; sid:2002982; rev:6;)

#Matt Jonkman
#General signs of trojan infections....
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN GENERAL Possible Trojan Sending Initial Email to Owner - SUCCESSO"; flow:established,to_server; content:"PC INFECTADO COM
SUCCESSO"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2002983; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_General;
sid:2002983; rev:3;)

#Matt Jonkman
#General signs of trojan infections....
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Suspicious Useragent Used by Several trojans (API-Guide test program)"; flow:established,to_server; content:"|0d
0a|User-Agent|3a| API-Guide test program|0d 0a|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007826; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_General; sid:2007826; rev:3;)

#Matt Jonkman
#General signs of trojan infections....
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader Checkin Pattern Used by Several Trojans"; flow:established,to_server; uricontent:".php?";
uricontent:"uid="; uricontent:"&gid="; uricontent:"&cid="; uricontent:"&rid="; uricontent:"&sid="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008143;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_General; sid:2008143; rev:2;)

#matt jonkman, used by many uploaders
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Pass Stealer FTP Upload"; flow:established,to_server; content:"INFECTADO|0d 0a|=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=|0d 0a|Computador"; depth:64; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008237; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_General; sid:2008237; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Generic Trojan Checkin"; flow:to_server,established; uricontent:"magic="; nocase; uricontent:"&id=";
uricontent:"&cache="; uricontent:"&tm="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008523; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_General; sid:2008523; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN General Bot HTTP CnC Pattern"; flow:established,to_server; uricontent:".php?guid_bot="; uricontent:"&ver_bot=";
uricontent:"&stat_bot="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008550; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_General;
sid:2008550; rev:2;)

#by victort julien
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Malformed Double Accept header - Likely Trojan-PWS.Win32.QQPass"; flow:established,to_server; content:"POST "; depth:5;
content:"|0d 0a|Accept|3a| Accept|3a| "; pcre:"/^Accept\x3A\sAccept\x3A[^\r\n]*\d+,\s/[A-z0-9\.]+,\s[A-z0-9\.]+/smi"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008975; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_General; sid:2008975; rev:4;)

#by joe stewart and bojan zdrjna
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Generic Trojan Checkin"; flow: to_server,established; content:"GET "; nocase; depth: 4; uricontent: ".asp?mac=";
nocase; pcre:"/mac=[a-f0-9]{2}-[a-f0-9]{2}-[a-f0-9]{2}-[a-f0-9]{2}-[a-f0-9]{2}-[a-f0-9]{2}/iU"; uricontent: "&ver="; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2009412; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_General; sid:2009412; rev:7;)

#by bojan
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Generic Trojan Checkin (2)"; flow: to_server,established; content:"GET "; nocase; depth: 4; uricontent: ".asp?mac=";
nocase; pcre:"/mac=[a-f0-9]+/iU"; uricontent: "&ver="; nocase; uricontent: "&os="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009442;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_General; sid:2009442; rev:6;)

#by: Jeremy Conway at sudosecure.net
#ref: 0e94639577df8c4b684b42d2acaa4417
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Generic Info Stealer - HTTP POST"; flow:established,to_server; content:"POST "; depth:5; content:"|0d 0a|Content-
Type|3a| multipart/form-data|3b| boundary|3d|"; nocase; content:"name=\"id\"|0d 0a|"; nocase; content:"name=\"upt\"|0d 0a|"; nocase; content:"name=\"mode\"|0d 0a|"; nocase;
content:"name=\"version\"|0d 0a|"; nocase; content:"name=\"cpu\"|0d 0a|"; nocase; content:"name=\"ram\"|0d 0a|"; nocase; content:"name=\"os\"|0d 0a|"; nocase; content:"name=\"user\"|0d
0a|"; nocase; content:"name=\"user\"|0d 0a|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009470; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_General; sid:2009470; rev:5;)

#by: Jeremy Conway at sudosecure.net
#ref: b5616a02e03205596215b4abfb9710ef
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader Infostealer - GET Checkin"; flow:established,to_server; content:"GET "; depth:4; content:"|0d 0a|User-
Agent|3a| wget 3.0|0d 0a|"; nocase; uricontent:"aid="; nocase; uricontent:"os="; nocase; uricontent:"uid="; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2009539; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_General; sid:2009539; rev:3;)

#by jerry at cybercave
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Possible Win32/Agent.QBY CnC Post"; flow:established,to_server; uricontent:"cike.php?fid="; nocase; uricontent:
"&cid="; nocase; uricontent:"&ver="; nocase; uricontent:"&tid="; nocase; uricontent:"&sn="; nocase; classtype:trojan-activity; reference:url,www.threatexpert.com/report.aspx?
uid=4f05faef-6a70-4957-8990-b316d8487f63; reference:url,doc.emergingthreats.net/2010138; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_General; sid:2010138;
rev:2;)

#2010-07-08 By Eoin Miller
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Generic Checkin - MSCommonInfoEx"; flow:established,to_server; content:"POST "; nocase; depth:5;
uricontent:"/common/MSCommonInfoEx.php"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011179; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_General; sid:2011179; rev:1;)

#by pedro marinho
#re aa894a50193470a9e50f9c0d842e1cb7
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Generic Trojan HTTP Get"; flow:established,to_server; content:"GET "; nocase; depth:4; uricontent:"in.php?affid=";
uricontent:"&url="; uricontent:"&win="; uricontent:"&sts="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011277; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_General; sid:2011277; rev:3;)

#by marcus at unsober
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Keylogger Crack by bahman"; flow:established; content:"POST "; nocase; depth:5;
content:"&message=|2b|keylogger|2b|Crack|2b|By|2b 25 32 31 25 32 31 25 32 31|...bahman"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008369;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_General_Keyloggers; sid:2008369; rev:6;)

#by Jeffrey Brown
```

```
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Keylogger Infection Report via POST"; flow:established,to_server; content:"texto=|25 30 44 25 30 41 25 30 44 25 30
41|Computer"; content:"|25 30 44 25 30 41|IP|25 32 45 25 32 45 25 32 45 25 32 45 25 32 45|"; distance:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008521;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_General_Keyloggers; sid:2008521; rev:2;)

#matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN SpamTool.Win32.Agent.gy/Grum/Tedroo Or Similar HTTP Checkin"; flow:established,to_server; uricontent:"?id="; nocase;
uricontent:"&tick="; nocase; uricontent:"&ver="; nocase; uricontent:"&smtp="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008189;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_General_Spamtools; reference:url,www.secureworks.com/research/threats/botnets2009/;
reference:url,securitylabs.websense.com/content/Blogs/2721.aspx; sid:2008189; rev:3;)

#matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Common Spambot HTTP Checkin"; flow:established,to_server; uricontent:"os="; uricontent:"&user=";
uricontent:"&status="; uricontent:"&uptime="; uricontent:"&cmd="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008261; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_General_Spamtools; sid:2008261; rev:2;)

#Matt Jonkman, found by Jacob Kitchel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Unnamed Generic.Malware http get"; flow:established,to_server; uricontent:"/ww20/script.php?id="; nocase;
content:"&config="; nocase; content:!"User-Agent|3a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003431; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Generic.Malware; sid:2003431; rev:4;)

#from castlecops research
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Generic.Malware.SFL User-Agent (Rescue/9.11)"; flow:established,to_server; content:"User-Agent|3a| Rescue/9.11";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003645; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Generic.Malware; sid:2003645;
rev:4;)

#by: Jeremy Conway at sudosecure.net
#ref: 3ef704eaa54118d277d52a1fe9bbcaa4
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Generic Backdoor Retrieve Instructions/Configs - HTTP GET"; flow:established,to_server; content:"GET "; nocase;
depth:4; uricontent:".php?aid="; nocase; uricontent:"&pid="; uricontent:"&kind="; nocase; content:!"|0d 0a|User-Agent|3a|"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2009826; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Generic.Malware; sid:2009826; rev:4;)

#by bojan
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Generic Trojan Checkin (double Content-Type headers)"; flow:to_server,established; content:"POST "; nocase; depth:5;
uricontent:".php"; nocase; content:"|0d 0a|Content-Type|3a| text/html"; nocase; content:"|0d 0a|Content-type|3a| image/gif"; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2010282; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Generic.Malware; sid:2010282; rev:3;)

#by bojan
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Generic Trojan Checkin (UA VBTagEdit)"; flow:to_server,established; content:"GET "; nocase; depth:4;
content:"HTTP/1.0|0d 0a|User-Agent|3a| VBTagEdit"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010439; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Generic.Malware; sid:2010439; rev:4;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Trojan-Downloader Win32.Genome.avan"; flow:to_server,established; content:"GET "; depth:4; uricontent:"?spaceIds=";
uricontent:"&mac="; uricontent:"&hdid="; uricontent:"&wlid="; uricontent:"&start="; uricontent:"&os="; uricontent:"&mem="; uricontent:"&alive="; uricontent:"&ver="; uricontent:"&mode=";
uricontent:"&guid="; uricontent:"&setup=1"; uricontent:"&install=&auto="; uricontent:"&serveid="; uricontent:"&area="; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2011236; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Genome; sid:2011236; rev:2;)

#by steven Adair of shadowserver.org
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Gh0st Remote Access Trojan Client Connect"; flow:to_server,established; content:"Gh0st"; depth:5; nocase; content:"|00 00 00
e0 00 00 00 78 9c 4b 63 60 60 98 03 c4 ac 40|"; within:19; dsize:<180; flowbits:set,ET.ghost; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008888;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Ghost; sid:2008888; rev:4;)

#by steven Adair of shadowserver.org
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN Gh0st Remote Access Trojan Server Response"; flowbits:isset,ET.ghost; flow:to_client,established; content:"Gh0st"; depth:5;
nocase; classtype:trojan-activity; reference:url,www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20081211; reference:url,doc.emergingthreats.net/2008889;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Ghost; sid:2008889; rev:4;)

#Jason aka dn1nj4 at shadowserver dot org
#ref: 4e224c80f62c1b3dc74d295d0633e699
#also re 53c26839720c9b3e9c6ed9f0d288d288
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Gh0st Trojan CnC"; flow:established,to_server; content:"Gh0st"; depth:5; flowbits:set,ET.gh0st_client; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/2010859; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Ghost; sid:2010859; rev:5;)

#Jason aka dn1nj4 at shadowserver dot org
#ref: 4e224c80f62c1b3dc74d295d0633e699
#also re 53c26839720c9b3e9c6ed9f0d288d288
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN Gh0st Trojan CnC Response"; flow:established,from_server; content:"Gh0st"; depth:5; flowbits:isset,ET.gh0st_client;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010860; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Ghost; sid:2010860; rev:5;)

#by Martin Holste
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN GhostNet Trojan Reporting"; flow:established,to_server; uricontent:"/microsoft/v2/update/upgrade.aspx?hostname=";
uricontent:"&ostype="; uricontent:"&macaddr="; uricontent:"&ipaddr="; uricontent:"&owner="; classtype:trojan-activity; threshold: type limit, track by_src, count 1, seconds 300;
reference:url,www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network; reference:url,doc.emergingthreats.net/2009202;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Ghostnet; sid:2009202; rev:4;)

#by michael sconzo
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Gimmiv.A.dll Infection"; flow: to_server,established; uricontent:"/test"; uricontent:".php"; uricontent:"?abc=";
uricontent:"?def="; classtype:trojan-activity; reference:url,www.microsoft.com/security/portal/Entry.aspx?name=TrojanSpy%3aWin32%2fGimmiv.A;
reference:url,doc.emergingthreats.net/2008689; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Gimiv; sid:2008689; rev:3;)

#by michael sconzo
#
alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Gimmiv Infection Ping Outbound"; icode:0; itype:8; dsize:20; content:"abcde12345fghij6789"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008726; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Gimiv; sid:2008726; rev:3;)

#by michael sconzo
#
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN Gimmiv Infection Ping Inbound"; icode:0; itype:8; dsize:20; content:"abcde12345fghij6789"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008727; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Gimiv; sid:2008727; rev:3;)

#by Darren Spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Glacial Dracon C&C Communication"; flow:established,to_server; uricontent:"?id="; nocase; uricontent:"&ve="; nocase;
uricontent:"&h="; nocase; content:"|0d 0a 0d 0a|&c[]="; nocase; content:"&t[]="; nocase; content:"&u[]="; nocase; content:"&d[]="; nocase; content:"&p[]="; nocase; classtype:trojan-
activity; reference:url,www.threatexpert.com/report.aspx?md5=912692cb4e3f960c9cb4bbc96fa17c9d; reference:url,www.threatexpert.com/report.aspx?md5=fd3d061ee86987e8f3f245c2dc0ceb46;
reference:url,doc.emergingthreats.net/2010163; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Glacial; sid:2010163; rev:2;)

#by Tom Fisher
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Goldun Reporting User Activity"; flow:established,to_server; uricontent:".php?param="; nocase; uricontent:"&socks=";
content:"|0d 0a|User-Agent|3a| Windows Updater"; nocase; classtype:trojan-activity; reference:url,www.avira.com/en/threats/TR_Spy_Goldun_de_1_details.html;
reference:url,doc.emergingthreats.net/2002775; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Goldun; sid:2002775; rev:6;)
```

```
#by Tom Fisher
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Goldun Reporting User Activity 2"; flow:established,to_server; uricontent:".php?phid="; nocase; uricontent:"&ver=";
nocase; uricontent:"&nn="; nocase; content:"|0d 0a|User-Agent|3a| z|0d 0a|"; classtype:trojan-activity; reference:url,www.avira.com/en/threats/TR_Spy_Goldun_de_1_details.html;
reference:url,doc.emergingthreats.net/2002780; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Goldun; sid:2002780; rev:5;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Goldun Reporting Install"; flow:established,to_server; uricontent:".php?codec="; pcre:"/codec=\d+D\d+D\d+/U";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007965; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Goldun; sid:2007965; rev:2;)

#by dxp and Darren Spruell. Compilation of former sids 2003509-2003511 and 2002854
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Gozi check-in / update"; flow:established,to_server; uricontent:"?user_id="; nocase; uricontent:"&version_id=";
nocase; uricontent:"&crc="; nocase; classtype:trojan-activity; reference:url,www.secureworks.com/research/threats/gozi; reference:url,doc.emergingthreats.net/2009410;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Gozi; sid:2009410; rev:3;)

#Joe Stewart from Lurhq
#
alert tcp any any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Possible Bobax trojan infection"; flow:established,to_server; content:"GET "; depth:4; uricontent:"/reg|3f|u=";
uricontent:"|26|v="; classtype: trojan-activity; reference:url,www.lurhq.com/bobax.html; reference:url,doc.emergingthreats.net/2001901; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_HTTP_Botnets; sid:2001901; rev:6;)

#Hacker Defender Root Kit
#By Chris Norton 2/22/05
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN HackerDefender Root Kit Remote Connection Attempt Detected"; flow: established,to_server; content:"|01 9a 8c 66 af c0 4a 11
9e 3f 40 88 12 2c 3a 4a 84 65 38 b0 b4 08 0b af db ce 02 94 34 5f 22|"; rawbytes; tag: session, 20, packets; classtype: trojan-activity;
reference:url,securityresponse.symantec.com/avcenter/venc/data/backdoor.hackdefender.html; reference:url,doc.emergingthreats.net/2001743; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_HackerDefender; sid:2001743; rev:8;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN HackerDefender.HE Root Kit Control Connection"; flow: established,to_server; content:"|d0 84 ec 77 cf ec 60 e9|"; depth:8;
classtype:trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/backdoor.hackdefender.html; reference:url,doc.emergingthreats.net/2003244;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_HackerDefender; sid:2003244; rev:3;)

#Matt Jonkman
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN HackerDefender.HE Root Kit Control Connection Reply"; flow: established,from_server; content:"|d0 84 ec 77 cf ec 60 e9|";
depth:8; classtype:trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/backdoor.hackdefender.html; reference:url,doc.emergingthreats.net/2003245;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_HackerDefender; sid:2003245; rev:3;)

#Trojan HaxDoor
#Submitted by Tom Fischer, 2006-01-24, modified 2/2/06 on info from chris, reference update from darren spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Haxdoor Reporting User Activity"; flow:established,to_server; uricontent:".php?"; nocase; uricontent:"lang=";
nocase; uricontent:"&socksport="; nocase; uricontent:"&httpport="; nocase; uricontent:"&ver="; nocase; classtype:trojan-activity;
reference:url,www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=BKDR_HAXDOOR.DI; reference:url,doc.emergingthreats.net/2002790; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_HaxDoor; reference:url,www.symantec.com/security_response/writeup.jsp?docid=2003-113016-1420-99&tabid=2; reference:url,www.threatexpert.com/report.aspx?
md5=e787c4437ff67061983cd08458f71c94; reference:url,www.threatexpert.com/report.aspx?md5=d86b9eaf9682d60cb8b928dc6ac40954; reference:url,www.threatexpert.com/report.aspx?
md5=1777f0ffa890ebfcc7587957f2d08dca; sid:2002790; rev:7;)

#Trojan HaxDoor
#Submitted by Tom Fischer, 2006-01-24, modified 2/2/06 on info from chris, reference update from darren spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Haxdoor Reporting User Activity 2"; flow:established,to_server; uricontent:".php?param="; nocase;
uricontent:"&socksport="; nocase; uricontent:"&httpport="; nocase; uricontent:"&uptime"; nocase; uricontent:"&uid="; nocase; uricontent:"&ver="; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2002929; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_HaxDoor;
reference:url,www.symantec.com/security_response/writeup.jsp?docid=2003-113016-1420-99&tabid=2; reference:url,www.threatexpert.com/report.aspx?md5=e787c4437ff67061983cd08458f71c94;
reference:url,www.threatexpert.com/report.aspx?md5=d86b9eaf9682d60cb8b928dc6ac40954; reference:url,www.threatexpert.com/report.aspx?md5=1777f0ffa890ebfcc7587957f2d08dca; sid:2002929;
rev:4;)

#by evilghost
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Exploit kit download payload likely Hiloti Gozi FakeAV etc"; flow:to_server,established; content:"GET "; nocase;
depth:4; content:!"|0d 0a|Referer|3a| "; nocase; uricontent:"/eH"; pcre:"/\/[a-z0-9]+\.[a-z0-9]{2,4}\/eH[a-z0-9]{60,}$/Ui"; classtype:trojan-activity;
reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Trojan%3AWin32%2FHiloti.gen%21D; reference:url,doc.emergingthreats.net/2011103;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hiltoi; sid:2011103; rev:7;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Exploit kit attack activity likely hostile"; flow:to_server,established; content:"GET "; nocase; depth:4;
content:!"|0d 0a|Referer|3a| "; nocase; uricontent:"/oH"; pcre:"/\/[a-z0-9]+\.[a-z0-9]{2,4}\/oH[a-z0-9]{60,}$/Ui"; classtype:trojan-activity;
reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Trojan%3AWin32%2FHiloti.gen%21D; reference:url,doc.emergingthreats.net/2011104;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hiltoi; sid:2011104; rev:7;)

#matt jonkman
#Disabled for now, getting many false positives
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Hitpop Checkin"; flow:established,to_server; uricontent:"/stat.htm?id="; nocase; uricontent:"&agt="; nocase;
uricontent:"&r=http"; nocase; uricontent:"&OS="; nocase; uricontent:"&ntime="; nocase; uricontent:"&rtime="; nocase; classtype:trojan-activity; reference:url,atlas-
public.ec2.arbor.net/docs/Hitpop_DDoS_Malware_Analysis_PUBLIC.pdf; reference:url,doc.emergingthreats.net/2008275; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hitpop; sid:2008275; rev:3;)

#by jeremy at sudosecure
#ref: 0189096db51adaf5598ef9a8eaeeff34
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Hitpop.AG/Pophot.az HTTP Checkin"; flow:to_server,established; content:"GET "; nocase; depth:4; uricontent:".asp";
nocase; uricontent:"|3F|ver="; nocase; uricontent:"|26|tgid="; nocase; uricontent:"|26|address="; nocase; pcre:"/address\=([0-9A-F][0-9A-F]-){5}([0-9A-F][0-9A-F])/i"; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/2008317; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hitpop; sid:2008317; rev:4;)

#by Don Jackson of Secureworks
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN HotLan.C Spambot C&C download command"; flow:established,from_server; content:"|3B|URL|3A|http|3A 2F 2F|";
pcre:"/\x0D\x0A\x0D\x0ASLP\x3A\d+\x3BMOD\x3A[\S\x3B]+\x3BURL\x3Ahttp\x3A\x2F{2}[^\x3B]+\x3BSRV\x3Aupd\x3B/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008471;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hotlan; sid:2008471; rev:4;)

#by Don Jackson of Secureworks
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN HotLan.C Spambot Trojan Activity"; flow:to_server,established; content:"GET|20|"; offset:0; depth:4;
content:"|3F|mod|3D|"; offset:5; depth:40; pcre:"/^GET\s+[^\x0A\x0D]+\x3Fmod\x3D\w*\x26id\x3D[^\x26\s]+\x5F\w+\x26up\x3D[^\x26]+\x26mid\x3D[^\x26\s]+/"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008473; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hotlan; sid:2008473; rev:4;)

#Matt Jonkman
#
alert tcp $EXTERNAL_NET !$HTTP_PORTS -> $HOME_NET any (msg:"ET VIRUS Hotword Trojan in Transit"; flow: established,from_server; content:"|63 6f 6d 66 69 64 65 6e 74 69 61 6c 20 64 6f 63
75 6d 65 6e 74 20 28 57 6f 72 64 29 20 66 72 6f 6d 20 44 69 67 69 44 6f 63 00 43 4d 20 25 73 20|"; classtype: trojan-activity;
reference:url,securityresponse.symantec.com/avcenter/venc/data/trojan.hotword.html; reference:url,doc.emergingthreats.net/2001959; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hotword; sid:2001959; rev:7;)

#Matt Jonkman
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET VIRUS Hotword Trojan inbound via http"; flow: established,from_server; content:"|63 6f 6d 66 69 64 65 6e 74 69 61 6c 20 64
6f 63 75 6d 65 6e 74 20 28 57 6f 72 64 29 20 66 72 6f 6d 20 44 69 67 69 44 6f 63 00 43 4d 20 25 73 20|"; classtype: trojan-activity;
reference:url,securityresponse.symantec.com/avcenter/venc/data/trojan.hotword.html; reference:url,doc.emergingthreats.net/2001960; reference:url,www.emergingthreats.net/cgi-
```

```
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hotword; sid:2001960; rev:6;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 21 (msg:"ET VIRUS Hotword Trojan - Possible File Upload CHJO"; flow: to_server,established; content:"STOR __"; content:"-CHJO.DRV"; nocase;
within: 100; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/trojan.hotword.html; reference:url,doc.emergingthreats.net/2001961;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hotword; sid:2001961; rev:9;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 21 (msg:"ET VIRUS Hotword Trojan - Possible File Upload CFXP"; flow: to_server,established; content:"STOR __"; content:"-CFXP.DRV"; nocase;
within: 100; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/trojan.hotword.html; reference:url,doc.emergingthreats.net/2001962;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hotword; sid:2001962; rev:9;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 21 (msg:"ET VIRUS Hotword Trojan - Possible FTP File Request pspv.exe"; flow: to_server,established; content:"SIZE pspv.exe"; classtype: trojan-
activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/trojan.hotword.html; reference:url,doc.emergingthreats.net/2001963; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hotword; sid:2001963; rev:9;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 21 (msg:"ET VIRUS Hotword Trojan - Possible FTP File Request .tea"; flow: to_server,established; content:"LIST "; content:".tea"; nocase;
within: 50; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/trojan.hotword.html; reference:url,doc.emergingthreats.net/2001964;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hotword; sid:2001964; rev:9;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 21 (msg:"ET VIRUS Hotword Trojan - Possible FTP File Status Upload ___"; flow: to_server,established; content:"|53 54 4f 52 20 5f 5f 5f 0d 0a|";
classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/trojan.hotword.html; reference:url,doc.emergingthreats.net/2001965;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hotword; sid:2001965; rev:9;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 21 (msg:"ET VIRUS Hotword Trojan - Possible FTP File Status Check ___"; flow: to_server,established; content:"|53 49 5a 45 20 5f 5f 5f 0d 0a|";
classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/trojan.hotword.html; reference:url,doc.emergingthreats.net/2001966;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hotword; sid:2001966; rev:9;)

#from castlecops research, http://www.castlecops.com, sig by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Hupigon User Agent Detected (SykO)"; flow:established,to_server; content:"User-Agent|3a| SykO"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003649; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hupington; sid:2003649; rev:7;)

#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Hupigon User Agent Detected (IE_7.0)"; flow:established,to_server; content:"User-Agent|3a| IE_7.0"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003932; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hupington; sid:2003932; rev:7;)

#from sandnet
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Hupigon URL Infection Checkin Detected"; flow:established,to_server; uricontent:"?mac="; nocase; uricontent:"&ver=";
nocase; uricontent:"&user="; nocase; uricontent:"&md5="; nocase; uricontent:"&pc="; nocase; pcre:"/mac=[a-f0-9]{2}-[a-f0-9]{2}-[a-f0-9]{2}-[a-f0-9]{2}-[a-f0-9]{2}-[a-f0-9]{2}/Ui";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007592; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hupington; sid:2007592; rev:5;)

#from sandnet
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Hupigon User Agent Detected (RAV1.23)"; flow:established,to_server; content:"User-Agent|3a| RAV"; nocase;
pcre:"/User-Agent\x3a RAV\d\.\d\d/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007661; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hupington; sid:2007661; rev:4;)

#from sandnet
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Hupigon User Agent Detected (??)"; flow:established,to_server; content:"User-Agent|3a| |3f 3f 0d 0a|"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007689; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hupington; sid:2007689; rev:4;)

#Backdoor.Win32.Hupigon.abb
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Hupigon CnC init (variant abb)"; flow:established,to_server; dsize:4; flowbits:isnotset,ET.hupa.init; flowbits:noalert;
content:"|00 00 00 00|"; flowbits:set,ET.hupa.init; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008041; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hupington; sid:2008041; rev:4;)

#Backdoor.Win32.Hupigon.abb
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Hupigon CnC Data Post (variant abb)"; flow:established,to_server; dsize:>200; flowbits:isset,ET.hupa.init;
content:"Windows "; content:"Service Pack "; distance:0; content:"HACK|00 00|"; distance:100; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008042;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hupington; sid:2008042; rev:3;)

#Backdoor.Win32.Hupigon.abb
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Hupigon User Agent Detected (VIP2007)"; flow:established,to_server; content:"User-Agent|3a| VIP20"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008156; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hupington; sid:2008156; rev:3;)

#new hupigon variant cnc, at least thats what some of the AVs call it. 1801d4ffb772174c655a5b223fb4d781
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Hupigon CnC Communication (variant bysj)"; flow:established,to_server; dsize:5; content:"HTTP|00|"; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/2008258; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hupington; sid:2008258; rev:3;)

#by Pedro Marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 3128 (msg:"ET TROJAN Likely Hupigon Post to Controller"; flow:established,to_server; content:"POST /+"; depth:7; flowbits:noalert;
flowbits:set,ET.Hupinit1; classtype:trojan-activity; reference:url,www.f-secure.com/v-descs/backdoor_w32_hupigon.shtml; reference:url,doc.emergingthreats.net/2008389;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hupington; sid:2008389; rev:2;)

#by Pedro Marinho
#
alert tcp $EXTERNAL_NET 3128 -> $HOME_NET any (msg:"ET TROJAN Hupigon Response from Controller (YES - ~~@@)"; flow:established,from_server; flowbits:isset,ET.Hupinit1; content:"HTTP/1.0
200 OK|0d 0a 0d 0a|YES|0d 0a 7e 7e|"; depth:26; content:"@@|0d 0a 0d 0a|"; within:150; classtype:trojan-activity; reference:url,www.f-secure.com/v-descs/backdoor_w32_hupigon.shtml;
reference:url,doc.emergingthreats.net/2008390; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hupington; sid:2008390; rev:2;)

#by jeremy at sudosecure
#ref: a127ef8d46e52b3df09c1c9430de6a27
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Hupigon.AZG Checkin"; flow:established,to_server; content:"GET "; depth:4; nocase; content:"|0d 0a|User-Agent|3a|
Mozilla/3.0 (compatible|3b| Indy Library)|0d 0a|"; within:300; nocase; uricontent:"eve="; nocase; uricontent:"username="; nocase; uricontent:"anma="; nocase; uricontent:"ver="; nocase;
classtype:trojan-activity; reference:url,www.pandasecurity.com/homeusers/security-info/about-malware/encyclopedia/overview.aspx?idvirus=143511&sind=0;
reference:url,vil.nai.com/vil/content/v_145056.htm; reference:url,doc.emergingthreats.net/2008515; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hupington;
sid:2008515; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Hupigon.dkxh Checkin to CnC"; flow:established,to_server; content:"OK|2e 01|200"; depth:20; offset:13; content:"Windows ";
distance:4; within:30; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008540; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hupington;
sid:2008540; rev:3;)

#by darren spruell
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Hupigon System Stats Report (I-variant)"; flow:established,to_server; content:"|00 00 00|"; depth:3; content:"<CPUI>";
content:"</CPUI><"; distance:0; within:27; content:"<MEMI>"; content:"</MEMI><"; distance:0; within:27; pcre:"/^\x00\x00\x00[\x72-\x74]/"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/TrojanDropper497; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hupington; sid:2009052; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 3128:9000 (msg:"ET TROJAN Possible Hupigon Connect"; flow:established,from_server; flowbits:set,ET.Hupinit2; dsize:<28; content:"HTTP/1.0 200 ";
depth:13; classtype:trojan-activity; flowbits:noalert; reference:url,doc.emergingthreats.net/2009290; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hupington; sid:2009290; rev:1;)

#matt jonkman
#
alert tcp $EXTERNAL_NET 3128:9000 -> $HOME_NET any (msg:"ET TROJAN Hupigon CnC Client Status"; flow:established,to_server; flowbits:isset,ET.Hupinit2; dsize:<6; content:"|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009291; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hupington; sid:2009291; rev:1;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 3128:9000 (msg:"ET TROJAN Hupigon CnC Server Response"; flow:established,from_server; flowbits:isset,ET.Hupinit2; dsize:3; content:"|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009292; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hupington; sid:2009292; rev:1;)

#by shirkdog
#
alert tcp $EXTERNAL_NET 1024: -> $HOME_NET any (msg:"ET TROJAN Win32.Hupigon Control Server Response"; flow:from_server,established; dsize:16; content:"|03 00 00 00 00 00 00 00 c4 ec 48
f5 5e 00 85 80|"; depth:16; threshold: type both, count 2, seconds 120, track by_src; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009350;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hupington; sid:2009350; rev:4;)

#by: Jeremy Conway at sudosecure.net
#ref: d96eaa91b6af24f4ed1616a817e5a819
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN KillAV/Dropper/Mdrop/Hupigon - HTTP GET"; flow:established,to_server; content:"GET "; nocase; depth:4;
uricontent:".asp?mac="; nocase; uricontent:"&xxx="; nocase; content:"|0d 0a|User-Agent|3a| baidu|0d 0a|"; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2009811; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Hupington; sid:2009811; rev:4;)

#By Joe Stewart, Based on valuable work by Tom Fisher
#
alert icmp any any -> any any (msg:"ET TROJAN ICMP Banking Trojan sending encrypted stolen data"; dsize:>64; itype:8; icode:0; content:"|08|"; depth:1; byte_test:4,>,64,1,little;
byte_test:4,<,1500,1,little; content:"|0000|"; distance:4; within:1495; classtype:trojan-activity; reference:url,www.websensesecuritylabs.com/alerts/alert.php?AlertID=570;
reference:url,doc.emergingthreats.net/2003073; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_ICMP_Tunnel; sid:2003073; rev:4;)

#IRC Trojan Reporting
#By Erik Fichtner
#Bleeding-Remix :: irc / ircbot detection state machine
#compiled from various sources.
#thanks to: Joe Stewart of LURHO, Joel Esler, Tomfi.
### Client login process. flowbits needs an OR.
### Client needs to tell the server who they are, join
### join a group, and someone needs to say something to
### someone else.
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET CHAT IRC USER command"; flow: to_server,established; content:"USER|20|"; nocase; offset: 0; content:"|203a|"; within: 40;
content:"|0a|"; within: 40; flowbits:noalert; flowbits: set,irc.start; classtype: misc-activity; reference:url,doc.emergingthreats.net/2002023;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; sid:2002023; rev:12;)

#IRC Trojan Reporting
#By Erik Fichtner
#Bleeding-Remix :: irc / ircbot detection state machine
#compiled from various sources.
#thanks to: Joe Stewart of LURHO, Joel Esler, Tomfi.
### Client login process. flowbits needs an OR.
### Client needs to tell the server who they are, join
### join a group, and someone needs to say something to
### someone else.
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET CHAT IRC NICK command"; flow: to_server,established; content:"NICK|20|"; nocase; depth:50; content:"|0a|"; within: 40;
flowbits:noalert; flowbits: set,irc.start; classtype: misc-activity; reference:url,doc.emergingthreats.net/2002024; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; sid:2002024; rev:13;)

#IRC Trojan Reporting
#By Erik Fichtner
#Bleeding-Remix :: irc / ircbot detection state machine
#compiled from various sources.
#thanks to: Joe Stewart of LURHO, Joel Esler, Tomfi.
### Client login process. flowbits needs an OR.
### Client needs to tell the server who they are, join
### join a group, and someone needs to say something to
### someone else.
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET CHAT IRC JOIN command"; flow:to_server,established; content:"JOIN|2023|"; nocase; depth:50; content:"|0a|"; within:40;
flowbits:set,irc.start; flowbits:set,is_proto_irc; flowbits:noalert; classtype:misc-activity; reference:url,doc.emergingthreats.net/2002025; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; sid:2002025; rev:14;)

#Another start, psyBNC servers don't always use a join, info from Reg Quinton
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN psyBNC IRC Server Connection"; flow:from_server,established; content:"psyBNC@lam3rz"; depth:33; nocase;
flowbits:set,irc.start; flowbits:set,is_proto_irc; classtype: misc-activity; reference:url,en.wikipedia.org/wiki/PsyBNC; reference:url,doc.emergingthreats.net/2003302;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; sid:2003302; rev:7;)

#Updated by Reg Quinton
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET CHAT IRC PRIVMSG command"; flowbits:isset,irc.start; flow:established; content:"PRIVMSG|20|"; depth:8; flowbits:set,is_proto_irc;
flowbits:noalert; classtype: misc-activity; reference:url,doc.emergingthreats.net/2002026; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2002026; rev:15;)

### Alternate path to is_proto_irc, Catch PING/PONG.
#
alert tcp any any -> any any (msg:"ET CHAT IRC PING command"; flowbits:isnotset,is_proto_irc; flow: from_server,established; content:"PING|20|"; nocase; offset: 0; flowbits:
set,irc.ping; flowbits:noalert; classtype: misc-activity; reference:url,doc.emergingthreats.net/2002027; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; sid:2002027; rev:6;)

### Alternate path to is_proto_irc, Catch PING/PONG.
#
alert tcp any any -> any any (msg:"ET CHAT IRC PONG response"; flowbits:isnotset,is_proto_irc; flowbits:isset,irc.ping; flowbits:noalert; flow: from_client,established;
content:"PONG|20|"; nocase; offset: 0; flowbits: set,is_proto_irc; classtype: misc-activity; reference:url,doc.emergingthreats.net/2002028; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; sid:2002028; rev:6;)

#Bot potty
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN BOT - channel topic scan/exploit command"; flowbits:isset,is_proto_irc; flow:to_client,established; content:"|3a|";
offset:0; content:"|20|332|20|"; within: 50; content:"|2023|"; within: 20; content:"|203a|"; nocase; within: 40; tag: host,300,seconds,dst; pcre:"/(ntscan [0-9]{1,4} [0-9]
{1,4}|dcom\.self|scan\.(start|stop)|scan ([0-9]{1,3}\.[0-9]{1,3})|(advscan|asc|xscan|xploit|adv\.start)
(webdav|netbios|ntpass|dcom(2|135|445|1025)|mssql|lsass|optix|upnp|dcass|beagle[12]|mydoom|netdevil|DameWare|kuang2|sub7|iis5ssl|wkssvc|wks1|mysql|wkssvcOth|wkssvcENG|arkeia|arcserve|wi
ns|veritas|netbackup|asn))/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2002029; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; sid:2002029; rev:10;)

#Bot potty
#
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN BOT - potential scan/exploit command"; flowbits:isset,is_proto_irc; flow:established; content:"PRIVMSG|20|"; depth:8;
nocase; content:"|3a|"; within:30; pcre:"/(ntscan [0-9]{1,4} [0-9]{1,4}|dcom\.self|scan\.(start|stop)|scan ([0-9]{1,3}\.[0-9]{1,3})|(advscan|exploited|asc|xscan|xploit|adv\.start)
(webdav|netbios|ntpass|dcom(2|135|445|1025)|mssql|lsass|optix|upnp|dcass|beagle[12]|mydoom|netdevil|DameWare|kuang2|sub7|iis5ssl|wkssvc|wks1|mysql|wkssvcOth|wkssvcENG|arkeia|arcserve|wi
ns|veritas|netbackup|asn))/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2002030; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; sid:2002030; rev:14;)

#Bot potty
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN BOT - potential update/download via http command"; flowbits:isset,is_proto_irc; flow:established,to_client; content:"
http|3a|//"; pcre:"/\.(upda|getfile|dl\dx|dl|download|execute)\w*\s+http\x3a\x2f\x2f/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2002031;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; sid:2002031; rev:18;)

#Bot potty
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN BOT - potential update/download via ftp command"; flowbits:isset,is_proto_irc; flow:established,to_client;
content:"ftp|3a|//"; pcre:"/\.(upda|getfile|dl\dx|dl|download|execute)\w*\s+ftp\x3a\x2f\x2f/i"; classtype: trojan-activity; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; reference:url,doc.emergingthreats.net/2011162; sid:2011162; rev:3;)

#Bot potty
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN BOT - potential DDoS command (1)"; flowbits:isset,is_proto_irc; flow:established,to_client; content:"floodnet ";
pcre:"/floodnet ([0-9]{1,3}\.){3}[0-9]{1,3}|(tcp|syn|udp|ack|ping|icmp)(flood)? ([0-9]{1,3}\.){3}[0-9]{1,3}/i"; classtype: trojan-activity;
reference:url,doc.emergingthreats.net/2002032; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; sid:2002032; rev:21;)

#Bot potty
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN BOT - potential response"; flowbits:isset,is_proto_irc; flow:established; content:"PRIVMSG|20|"; nocase; depth:8;
content:"|3a|"; within:30; pcre:"/((T?FTP)\x3a File transfer|(random|sequential) Port Scan|Random (Spreading|Scanner)|Exploiting IP|Exploiting\.\.|flooding\x3a|flood stopped|sending
packets)|Random Method started|FINDFILE|Scan stopped|No scan thread found|thread\(s\) stopped|\x3aExec /i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2002033;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; sid:2002033; rev:15;)

#Bot potty
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN BOT - potential misc bot commands"; flowbits:isset,is_proto_irc; flow: established; content:"PRIVMSG|20|"; depth:8; nocase;
content:"|3a|"; within:30; tag: host,300,seconds,src; pcre:"/((\.aim\w*|ascanall|\x3agetshit200)\s+\w+)|
((@kill|@get_os_version|@get_computer_name|@get_bot_version|@update|@restart|@reboot|@shutdown)\s)/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2002384;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; sid:2002384; rev:14;)

#Bot potty
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN BOT - channel topic misc bot commands"; flowbits:isset,is_proto_irc; flow: established; content:"|3a|"; offset: 0;
content:"|20|332|20|"; within: 50; content:"|2023|"; within: 20; content:"|203a|"; tag: host,300,seconds,src; pcre:"/(\.aim\w*|ascanall)\s+\w+/i"; classtype: trojan-activity;
reference:url,doc.emergingthreats.net/2002386; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; sid:2002386; rev:10;)

#Bot potty
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN BOT - potential DDoS command (2)"; flowbits:isset,is_proto_irc; flow: established; tag: host,300,seconds,dst;
content:"ddos"; nocase; pcre:"/ddos\.(phat(icmp|syn|wonk)|stop|(syn|udp|http)flood|targa3|(syn|ack|random) ([0-9]{1,3}\.){3}[0-9]{1,3})/i"; classtype: trojan-activity;
reference:url,doc.emergingthreats.net/2003132; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; sid:2003132; rev:5;)

#Added commands of another nasty bot
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN BOT - potential reptile commands"; flowbits:isset,is_proto_irc; flow:established; content:"PRIVMSG|20|"; nocase; depth:8;
content:"|3a|"; within:30; pcre:"/\.
((testdlls|threads|nsp|speed|uptime|installed|secure|sec|unsecure|unsec|process|ps|rand|exploitftpd|eftpd|flusharp|farp|flushdns|fdns|resolve|dns|pstore|pst|sysinfo|si|netinfo|ni|drivei
nfo|di|currentip)\s*[\r\n]|(iestart|ies|login|l|mirccmd|system|file\s+(cat|exists|e|del|rm|rmdir|move|copy|attrib)|down|dl\dx|update|reg\s+(query|delete|write))\s+\w+|
(banner|ban|advscan|asc|scanall|sa|ntscan|nts)\s*[\n\r])/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2002363; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; sid:2002363; rev:12;)

#Added commands of another nasty bot
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN BOT - channel topic reptile commands"; flowbits:isset,is_proto_irc; flow:established; content:"|3a|"; offset: 0;
content:"|20|332|20|"; within: 50; content:"|2023|"; within: 20; content:"|203a|"; pcre:"/\.
((testdlls|threads|netstatp|nsp|speed|uptime|installed|secure|sec|unsecure|unsec|process|ps|rand|exploitftpd|eftpd|flusharp|farp|flushdns|fdns|resolve|dns|pstore|pst|sysinfo|si|netinfo|
ni|driveinfo|di|stats|currentip)\s*[\r\n]|(iestart|ies|login|l|mirccmd|system|file\s+(cat|exists|e|del|rm|rmdir|move|copy|attrib)|down|dl\x|update|reg\s+(query|delete|write))\s+\w+|
(banner|ban|advscan|asc|scanall|sa|ntscan|nts)\s*[\n\r])/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2002385; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; sid:2002385; rev:11;)

#agobot, sdbot stuff, from JB
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN Agobot-SDBot Commands"; flowbits:isset,is_proto_irc; flow:established; content:"PRIVMSG|20|"; depth:8; nocase;
pcre:"/((cvar\.set)|(http\.(execute|update))|((aol)spam\.(setlist|settemplate|start|stop|setuser|setpass))|sniffer\.
(addstring|delstring)|pingstop|udpstop|scan(all|stats|del|stop)|clone(stop|start)|c_(raw|mode|nick|join|part|privmsg|action))/i"; classtype: trojan-activity;
reference:url,doc.emergingthreats.net/2003157; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; sid:2003157; rev:6;)

#pBot commands, Matt Jonkman, updated by Reg Quinton
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN pBot (PHP bot) Commands"; flowbits:isset,is_proto_irc; flow:established; content:"PRIVMSG|20|"; nocase; depth:8;
pcre:"/PRIVMSG\s+\S+\s+\x3a\s*(\.user |\.logout|\.die|\.restart|\.mail |\.dns |\.download |\.exec |\.find |\.cmd |\.php |\.tcpflood |\.udpflood |\.raw |\.rndnick|\.pscan |\.ud\.server
)/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2003208; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; sid:2003208;
rev:10;)

#These are by Reg Quinton for perl bots. Uses the above irc state machines:
#$Id: emerging-virus.rules,v 1.3910 2010/07/30 02:04:53 jonkman Exp $
#I am building these from perlbots I've captured over the last few months
#as I chase PHP injection attacks. In each case what you have is a "PRIVMSG"
#response with content that looks like ":\002...text\002"
#I rely on flowbits isproto_irc to catch the leading "PRIVMSG .*:"
#[11:29am dominic] cat ~/php-injection/* | sed -n 's/.*:\\002/:\\002/p' |\
#sed 's/002[ :].*/002/' | sort | uniq -c | grep 002\\[
#2 :\002[Atk33]\002
#2 :\002[Exploiting]\002
#2 :\002[Finished]\002
#8 :\002[GOOGLE]\002
#1 :\002[GOOGLER]\002
#11 :\002[HTTP]\002
#4 :\002[HTTP-DDOS]\002
#1 :\002[HTTP DDoSing]\002
#1 :\002[PKS-SCAN| @@ ERROR @@ ]\002
#1 :\002[PKS-SCAN|EXPLOTANDO CON CURL]\002
#1 :\002[PKS-SCAN|EXPLOTANDO CON FETCH]\002
#1 :\002[PKS-SCAN|EXPLOTANDO CON GET]\002
#1 :\002[PKS-SCAN|EXPLOTANDO CON LYNX]\002
#1 :\002[PKS-SCAN|EXPLOTANDO CON WGET]\002
#1 :\002[PKS-SCAN| SPREANDING ]\002
#2 :\002[Results]\002
#2 :\002[RSH]\002
#19 :\002[SCAN]\002
#10 :\002[TCP]\002
#4 :\002[TCP-DDOS]\002
#2 :\002[TCP DDoSing]\002
#13 :\002[UDP]\002
#4 :\002[UDP-DDOS]\002
#1 :\002[UDP DDoSing]\002
#2 :\002[v6]\002
#1 :\002[v6|Exploiting]\002
#1 :\002[v6|VULN]\002
#6 :\002[VERSION]\002
#Ones that look like ':\002[sometext]\002'
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN perlb0t/w0rmb0t Response (Case 1)"; flow:established; flowbits:isset,is_proto_irc; content:"|3A 02 5B|"; content:"|5B 02|";
within: 32; pcre:"/\x3A\x02\x5B(Atk33|Exploiting|Finished|GOOGLE.*|HTTP.{0,8}|PKS-SCAN.{0,20}|Results|RSH|SCAN|TCP.{0,8}|UDP.{0,8}|v6.{0,12}|VERSION)\x5D\x02/i"; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/2006910; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; sid:2006910; rev:6;)

#[11:31am dominic] cat ~/php-injection/* | sed -n 's/.*:\\002/:\\002/p' \
#| sed 's/002[ :].*/002/' | sort | uniq -c | grep 002.003
#2 :\002\0034<------------------------------------------------>\003\002");
#2 :\002\0034<------------------------------------------------>\003\002");
#1 :\002\0034[BackConnect]\003\002
#2 :\002\0034[help]\003\002
#1 :\002\0034[HTTP]\003\002
#1 :\002\0034[HTTP DDoSing]\003\002
#1 :\002\0034PerlBot :By SPEED (Security Net Information) LoaDED bY @adms");
#3 :\002\0034[SCAN]\003\002
#2 :\002\0034[TCP DDoSing]\003\002
#1 :\002\0034[UDP]\003\002
#1 :\002\0034[UDP DDoSing]\003\002
#1 :\002\0034[VERSION]\003\002
#Ones that look like \002\0034[sometext]\003\002
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN perlb0t/w0rmb0t Response (Case 2)"; flow:established; flowbits:isset,is_proto_irc; content:"|3A 02 03|4|5B|"; content:"|03
02|"; within: 32; pcre:"/\x3A\x02\x034\x5B(BackConnect|help|HTTP.*|SCAN|TCP.*|UDP.*|VERSION)\x5D\x03\x02/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006911;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; sid:2006911; rev:6;)

#[11:34am dominic] cat ~/php-injection/* | sed -n 's/.*:\\002/:\\002/p' \
#| sed 's/002[ :].*/002/' | sort | uniq -c | grep -v '002\\003' | grep -v '002\['
#1 :\002
#2 :\002Alvo dos Pacotes\002
#1 :\002Conectando-se em\002
#1 :\002M&#233;dia de envio\002
#1 :\002Tempo\002
#2 :\002Tempo de Pacotes\002
#1 :\002Total bytes\002
#2 :\002Total de Pacotes\002
#1 :\002Total pacotes\002
#Ones that look like \002sometext\002
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN perlb0t/w0rmb0t Response (Case 3)"; flow:established; flowbits:isset,is_proto_irc; content:"|3A 02|"; content:"|02|";
within: 32; pcre:"/\x3A\x02(Alvo dos Pacotes|Conectando-se em|M.dia de envio|Tempo.*|Total .*)\x02/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2006912;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; sid:2006912; rev:8;)

#$Id: emerging-virus.rules,v 1.3910 2010/07/30 02:04:53 jonkman Exp $
#[8:03am dominic] telnet 59.124.158.12 65500
#Trying 59.124.158.12...
#Connected to 59-124-158-12.HINET-IP.hinet.net (59.124.158.12).
#Escape character is '^]'.
#:irc.Indonesia.B0tN3t.org NOTICE AUTH :*** Looking up your hostname...
#:irc.Indonesia.B0tN3t.org NOTICE AUTH :*** Found your hostname
#Reg Quinton <reggers@ist.uwaterloo.ca>; 9-Nov-2007
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN B0tN3t IRCbotnet"; flow:from_server,established; content:"|3a|"; offset:0; depth:1; content:"B0tN3t"; within:32; nocase;
flowbits:set,irc.start; flowbits:set,is_proto_irc; classtype:misc-activity; reference:url,en.wikipedia.org/wiki/Botnet; reference:url,doc.emergingthreats.net/2007672;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; sid:2007672; rev:5;)

#by Greg Bowser
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Username in IRC (XP-..)"; flow:established,to_server; flowbits:isset,is_proto_irc; content:"USER XP-";
pcre:"/USER XP-[A-z0-9]{4,8} \* 0 \:.*/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008123; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots; sid:2008123; rev:4;)

#by Greg Bowser
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Nick in IRC (USA +..)"; flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008124; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2008124; rev:2;)

#by Reg Quinton
#Kaiten is a compiled code DDOS IRCbotnet for Unix/Linux systems. You will
#find the string "Kaiten wagoraku" in the code ..(or in the strings if you
#have a compiled version). It's been around since at least 2006, source can
#be found at many sites.
#See also
#http://isc.sans.org/diary.html?storyid=1127
#http://handlers.dshield.org/pbueno/Steve_malware6.pdf
#http://www.stacksegment.net/wiki/index.php/Linux_Malware_Analysis
#http://ktp.e-isa.com/Viruses/Linux.DDos-Kaiten.htm
#Reg Quinton; 2007/08/30
#Botnet begins by contacting an IRC server (there's some randomization to
#pick one) and saying (with short nick,ident,user strings..):
#Send(sock,"NICK %s\nUSER %s localhost localhost :%s\n",nick,ident,user);
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Kaiten IRCbotnet login"; flow:to_server,established; content:"NICK|20|"; offset:0; depth:5; content:"USER|20|"; within:32;
content:"localhost|20|localhost|20 3A|"; within:32; pcre:"/NICK\x20\S+\x0AUSER\x20\S+localhost\x20localhost\x20\x3A/"; flowbits:set,irc.start; classtype:trojan-activity;
reference:url,en.wikipedia.org/wiki/IRC_bot; reference:url,doc.emergingthreats.net/2007621; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Kaiten;
sid:2007621; rev:4;)

#various distinctive responses to commmands implemented by Kaiten client
#
alert tcp $HOME_NET any -> any any (msg:"ET TROJAN Kaiten IRCbotnet Response"; flow:established; flowbits:isset,irc.start; content:"NOTICE|20|"; content:"|20 3A|"; within:32;
pcre:"/\x20\x3A(Receiving\x20file.\x0A|Saved\x20as\x20|Spoofs\x3A\x20|Kaiten\x20wa\x20goraku|Current\x20status\x20is\x3a\x20|Removed\x20all\x20spoofs|Packeting\x20|Panning\x20|Tsunami\x
20heading\x20for\x20|Unknowing\x20|Killing\x20pid\x20)/"; classtype:trojan-activity; reference:url,en.wikipedia.org/wiki/IRC_bot; reference:url,doc.emergingthreats.net/2007622;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Kaiten; sid:2007622; rev:4;)

#various commmands implemented by Kaiten client, they don't use a : delimiter
#as others do, it's "[:<server> ]PRIVMSG !<clients> <command> <args>". I'm
#skipping the server part. I wish there were flowbits that noted that we have
#an IRC channel going. I don't want to watch everything.
#
alert tcp any any -> $HOME_NET any (msg:"ET TROJAN Kaiten IRCbotnet Commands"; flow:from_server,established; content:"PRIVMSG|20 21|";
pcre:"/PRIVMSG\x20\x21\S+\x20(TSUNAMI\x20|PAN\x20|UDP\x20|UNKNOWN\x20|GETSPOOFS|SPOOFS\x20)/i"; classtype:trojan-activity; reference:url,en.wikipedia.org/wiki/IRC_bot;
reference:url,doc.emergingthreats.net/2007623; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Kaiten; sid:2007623; rev:5;)

#$Id: emerging-virus.rules,v 1.3910 2010/07/30 02:04:53 jonkman Exp $
#Pitbull is an IRCbot implemented in Perl since 2007/09/13, code seems to have
#authors who speak spanish or portugese. Small sample here
#http://www.directadmin.com/forum/showthread.php?p=113720
#Google had a cached version, you might browse around to find others.
#Versions I captured are a little different from one another (s/space/etx/).
#Code *says* it supports these commands (but versions differ):
#!bot @portscan <ip>
#!bot @nmap <ip> <beginport> <endport>
#!bot @back <ip><port>
#!bot @udpflood <ip> <packet size> <time>
#!bot @tcpflood <ip> <port> <packet size> <time>
#!bot @httpflood <site> <time>
#!bot @linuxhelp
#!bot @rfi <vuln> <dork>
```

```
#!bot @system
#!bot @milw0rm
#!bot @logcleaner
#!bot @sendmail <subject> <sender> <recipient> <message>
#!bot @join <#channel>
#!bot @part <#channel>
#!bot @help
#!bot cd tmp for example
#!bot !eval <code= for example :@nickname>
#Reg Quinton; 26-Sept-2007
#seems to be a common prefix in responses with the few I've seen.
#
alert tcp $HOME_NET any -> any any (msg:"ET TROJAN Pitbull IRCbotnet Response"; flow:established; flowbits:isset,irc.start; content:"PRIVMSG|20|"; content:"|3A|"; within:32;
content:"4"; within:5; content:"12"; within:5; content:"|3a|"; within:5; pcre:"/\x3a.4\x7c.12.\x3a.4/"; classtype:trojan-activity; reference:url,en.wikipedia.org/wiki/IRC_bot;
reference:url,doc.emergingthreats.net/2007624; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Pitbull; sid:2007624; rev:4;)

#various commmands implemented by Pitbull client as provided above
#
alert tcp any any -> $HOME_NET any (msg:"ET TROJAN Pitbull IRCbotnet Commands"; flow:from_server,established; content:"PRIVMSG|20|";
pcre:"/PRIVMSG.*@(portscan|nmap|back|udpflood|tcpflood|httpflood|linuxhelp|rfi|system|milw0rm|logcleaner|sendmail|join|part|help)/i";  classtype:trojan-activity;
reference:url,en.wikipedia.org/wiki/IRC_bot; reference:url,doc.emergingthreats.net/2007625; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Pitbull;
sid:2007625; rev:6;)

#distinctive string in page fetch to google, yahoo, lycos, milw0rm, etc.
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Pitbull IRCbotnet Fetch"; flow:to_server,established; content:"Accept|3a20|*/*|0d0a|User-
Agent|3a20|Mozilla/5.0|0d0a0d0a|"; depth:300; classtype:trojan-activity; reference:url,en.wikipedia.org/wiki/IRC_bot; reference:url,doc.emergingthreats.net/2007626;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Pitbull; sid:2007626; rev:3;)

#update by darren spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Illusion Bot (Lussilon) Checkin"; flow:established,to_server; content:"POST "; nocase; depth:5; uricontent:"?
act=online&"; nocase; uricontent:"s4="; nocase; uricontent:"&s5="; nocase; uricontent:"&nickname="; content:"|0d 0a 0d 0a|msg_out="; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2007829; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Illusion_Bot; sid:2007829; rev:6;)

#IE Ilookup Trojan
#Submitted by Joseph Gama, for IE Ilookup Trojan
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN IE Ilookup Trojan"; flow: from_server,established; content:"#@~^/gAAAA==@#@&@#@&7lMP|3a|HVK^P{P[W1Ehn";
content:"#@~^GAIAAA==@#@&\\CMPsX/DD,xPvEU+kmC2"; classtype: misc-activity; reference:url,62.131.86.111/analysis.htm; reference:url,doc.emergingthreats.net/2001066;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Ilookup; sid:2001066; rev:8;)

#by Darren Spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN TROJ_INJECT.NI Update Request"; flow:established,to_server; dsize:7; content:"F222222"; classtype:trojan-activity;
reference:url,www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_INJECT.NI&VSect=T; reference:url,doc.emergingthreats.net/2009077; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Infect; sid:2009077; rev:3;)

#by Matt Jonkman
#A large number of trojans report an infection by sending a blank email to a gmail or other free provider
#They're pretty bland, other than they almost always use the Indy Mail lib. So the mail is slightly unique
#This sig should catch them outbound
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN Possible Infection Report Mail - Indy Mail lib and No Message Body - Priority 1"; flow:established,to_server; content:"|0d
0a|X-Priority|3a| 1|0d 0a|X-Library|3a| Indy "; content:"|0d 0a 0d 0a 2e 0d 0a|"; within:30; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007611;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Infection_Emails; sid:2007611; rev:8;)

#by Matt Jonkman
#A large number of trojans report an infection by sending a blank email to a gmail or other free provider
#They're pretty bland, other than they almost always use the Indy Mail lib. So the mail is slightly unique
#This sig should catch them outbound
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN Possible Infection Report Mail - Indy Mail lib and No Message Body - Priority 3"; flow:established,to_server; content:"|0d
0a|X-Priority|3a| 3|0d 0a|X-Library|3a| Indy "; content:"|0d 0a 0d 0a 2e 0d 0a|"; within:30; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007612;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Infection_Emails; sid:2007612; rev:8;)

#by Matt Jonkman
#A large number of trojans report an infection by sending a blank email to a gmail or other free provider
#They're pretty bland, other than they almost always use the Indy Mail lib. So the mail is slightly unique
#This sig should catch them outbound
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN Possible Infection Report Mail - Indy Mail lib and MAC Message Body - Priority 1"; flow:established,to_server; content:"|0d
0a|X-Priority|3a| 1|0d 0a|X-Library|3a| Indy "; content:"|0d 0a|MAC......."; nocase; within:20; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007613;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Infection_Emails; sid:2007613; rev:7;)

#by Matt Jonkman
#A large number of trojans report an infection by sending a blank email to a gmail or other free provider
#They're pretty bland, other than they almost always use the Indy Mail lib. So the mail is slightly unique
#This sig should catch them outbound
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN Possible Infection Report Mail - Indy Mail lib and MAC Message Body - Priority 3"; flow:established,to_server; content:"|0d
0a|X-Priority|3a| 3|0d 0a|X-Library|3a| Indy "; content:"|0d 0a|MAC......."; nocase; within:20; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007614;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Infection_Emails; sid:2007614; rev:7;)

#by Matt Jonkman
#A large number of trojans report an infection by sending a blank email to a gmail or other free provider
#They're pretty bland, other than they almost always use the Indy Mail lib. So the mail is slightly unique
#This sig should catch them outbound
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN Possible Infection Report Mail - Indy Mail lib and Nome do Computador in Body"; flow:established,to_server; content:"|0d
0a|X-Library|3a| Indy "; content:"Nome do Computador......."; nocase; distance:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007950;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Infection_Emails; sid:2007950; rev:4;)

#from castlecops research, http://www.castlecops.com, sig by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Inject.BV Trojan User Agent Detected (faserx)"; flow:established,to_server; content:"User-Agent|3a| faser"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003637; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Inject; sid:2003637; rev:4;)

#by Marcus of Unsober
#ref: 0ad5f61380dba645bd1eaa965a78a8d1
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET DELETED Injecter Checkin"; flow:established,to_server; content:"GET "; depth:4; uricontent:"mod="; uricontent:"&id=";
uricontent:"&up="; content:"|0d 0a|User-Agent|3a| Mozilla/4.0 (compatible|3b| MSIE 6.0|3b| Windows NT 5.1|3b| SV1)"; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008349; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Injector; sid:2008349; rev:5;)

#by Marcus of Unsober
#ref: 0ad5f61380dba645bd1eaa965a78a8d1
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Insidebar.co.kr Related Infection Checkin"; flow:established,to_server; content:"POST "; nocase; depth:5;
content:"|0d 0a 0d 0a|e=inside&s="; content:"&ver="; distance:0; content:"&p="; distance:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008760;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Insidebar; sid:2008760; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1030 (msg:"ET TROJAN Ipbill.com Related Dialer Trojan Checkin"; flow:established,to_server; dsize:7; content:"|0a|"; offset:6;
pcre:"/\d\d\d\d\d\d\x0a/"; classtype:trojan-activity; flowbits:set,ET.ipbill1; reference:url,doc.emergingthreats.net/2008730; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Ipbill.com; sid:2008730; rev:3;)
```

```
#matt jonkman
#
alert tcp $EXTERNAL_NET 1030 -> $HOME_NET any (msg:"ET TROJAN Ipbill.com Related Dialer Trojan Server Response"; flow:established,from_server; dsize:<20; content:"|0a 5b 27|"; offset:2;
depth:5; content:"|27 5d 0a|"; distance:0; classtype:trojan-activity; flowbits:isset,ET.ipbill1; reference:url,doc.emergingthreats.net/2008731;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Ipbill.com; sid:2008731; rev:3;)

#new CNC channel, sample has no AV detection, collected 5/14
#sigs by Jeffrey Brown
#Register the first comm w/ 7c, 1 byte packet
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Juicopotomous to Controller"; flow:established,to_server; dsize:1; content:"|7c|"; flowbits:set,ET.unknown.setup;
flowbits:noalert; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008245; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Juicopotomous;
sid:2008245; rev:5;)

#new CNC channel, sample has no AV detection, collected 5/14
#sigs by Jeffrey Brown
#Register the first comm w/ 7c, 1 byte packet
#
alert tcp $EXTERNAL_NET 1024: -> $HOME_NET any (msg:"ET TROJAN Juicopotomous ack from Controller"; flowbits:isset,ET.unknown.setup; flow:established,from_server; dsize:<50; content:"|7d
27|"; depth:2; flowbits:set,ET.unknown.replied; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008246; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Juicopotomous; sid:2008246; rev:4;)

#new CNC channel, sample has no AV detection, collected 5/14
#sigs by Jeffrey Brown
#Register the first comm w/ 7c, 1 byte packet
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Juicopotomous ack to Controller"; flowbits:isset,ET.unknown.replied; flow:established,to_server; dsize:<50; content:"|7e
27|"; depth:2; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008247; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Juicopotomous;
sid:2008247; rev:5;)

#new CNC channel, sample has no AV detection, collected 5/14
#sigs by Jeffrey Brown
#Register the first comm w/ 7c, 1 byte packet
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Kangkio User-Agent (lsosss)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| lsosss|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008767; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Kangkio; sid:2008767; rev:3;)

#by Jeremy Conway
#ref: 13bce3215f758d69a6574f7018ed8c32
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Keylogger PRO GOLD Post"; flow:established,to_server; content:"to="; content:"&from="; within:200;
content:"&subject="; within:200; content:"&message="; within:200; content:"Discribtion"; within:14; content:"KEYLOGG+PRO+GOLD+VERSION"; content:"IPHostName"; content:"IPAddress";
content:"YahooMessenger+Passwords"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008642; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Keylogger_Pro; sid:2008642; rev:2;)

#by marcus at unsober.org
#re:532e39fdcd20fa7cc52e34b664a0e8f5
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Keylogger Pro Update Check"; flow:established,to_server; content:"POST "; depth:5; content:"<root><clnt>"; content:"
</clnt><code>CheckUpdate</code>"; nocase; pcre:"/<root><clnt>\d{8}-\d{4}-\d{4}-\d{4}-[0-9A-F]{12}</clnt><code>CheckUpdate</code>/"; classtype:trojan-activity;
reference:url,vil.nai.com/vil/content/v_130975.htm; reference:url,doc.emergingthreats.net/2009533; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Keylogger_Pro; sid:2009533; rev:2;)

#by Marcus at unsober
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Keylogger.ane Checkin"; flow:established,to_server; content:"Secret Client|00 00 00|"; depth:18; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/2008449; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Keyloggers; sid:2008449; rev:2;)

#by Matt Jonkman, re 4a9362b44caaa807b3f383df60306bf9
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Keypack.co.kr Related Trojan User-Agent Detected"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
keypack"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008339; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Keypack.co.kr;
sid:2008339; rev:3;)

#by Marcus of unsober
#re f94837651cf2decefb4b754c718046df
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN KLog Nick Keylogger Checkin"; flow:established,to_server; content:"POST "; nocase; depth:5; uricontent:".php";
content:"|0d 0a|User-Agent|3a| Mozilla/3.0 (compatible|3b| Indy Library)"; content:"Nick+Key+Ativado"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008338;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Klog; sid:2008338; rev:5;)

#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Klom.A Connecting to Controller"; flow:established,to_server; uricontent:"/s_13_0?m="; nocase; uricontent:"r=";
nocase; uricontent:"&a="; nocase; uricontent:"&os="; nocase; classtype:trojan-activity; reference:url,www.bitdefender.com/VIRUS-1000126-en--Trojan.Klom.A.html;
reference:url,doc.emergingthreats.net/2003538; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Klom; sid:2003538; rev:3;)

#by William Salusky at AOL
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Knockbot Proxy Checkin"; flow:to_server,established; uricontent:".php?win="; uricontent:"&id="; uricontent:"&lip=";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008249; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Knockbot; sid:2008249; rev:2;)

#by evilghost and darren spruell
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Knockbot Proxy Response From Controller"; flow:established,from_server; content:"|0d 0a 0d
0a|command|7c|file|7c|http"; depth:250; nocase; content:"|7c|"; within:150; classtype:trojan-activity; reference:url,www.malwaredomainlist.com/mdl.php?search=knock.php;
reference:url,doc.emergingthreats.net/2010787; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Unknown; sid:2010787; rev:4;)

#by evilghost and darren spruell
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Knockbot Proxy Response From Controller (empty command)"; flow:established,from_server; content:"|0d 0a 0d
0a|command|7c|"; nocase; depth:250; classtype:trojan-activity; reference:url,www.malwaredomainlist.com/mdl.php?search=knock.php; reference:url,doc.emergingthreats.net/2010788;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Unknown; sid:2010788; rev:4;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN W32.Koblu"; flow:established,to_server; content:"GET "; depth:4; uricontent:"sid="; nocase; uricontent:"&sa=";
nocase; uricontent: "&p="; uricontent:"&q=cards&rf="; uricontent:"&enc="; uricontent:"&enk=&xsc=&xsp=&xsm="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010230;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Koblu; sid:2010230; rev:4;)

#by Victor Julien
#Ikarus: Worm.Win32.Koobface.C,
#re e3e392688b15f1077daec4dfc1ca7530
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Worm.Win32.Koobface.C User-Agent"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| Mozilla/5.01";
content:"Gecko/2005"; within:50; content:"Firefox/3"; distance:5; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008848; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Koobface; sid:2008848; rev:4;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Koobface Trojan HTTP Post Checkin"; flow:established,to_server; content:"POST "; nocase; depth:5; content:"|0d 0a 0d
0a|f=0&a="; content:"&v="; within:6; content:"&c="; within:5; content:"&s="; within:4; content:"&l=&ck="; within:10; content:"&c_fb="; within:10; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008864; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Koobface; sid:2008864; rev:4;)

#by Chris Green
#
```

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Koobface BLACKLABEL"; flow:established,from_server; content: "#BLACKLABEL|0d 0a|EXIT"; classtype:trojan-activity;
reference:url,blog.threatexpert.com/2008/12/koobface-leaves-victims-black-spot.html; reference:url,doc.emergingthreats.net/2009407; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Koobface; sid:2009407; rev:2;)

#by Darren Spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Koobface HTTP Request (2)"; flow:established,to_server; uricontent:"?action="; nocase; uricontent:"&v="; nocase;
pcre:"/\?action=\w+gen&v=\d+/U"; classtype:trojan-activity; reference:url,ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html;
reference:url,doc.emergingthreats.net/2010150; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Koobface; sid:2010150; rev:4;)

#by jerry at cybercave
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Koobface C&C availability check"; flow:established,to_server; content:"POST "; nocase; depth:5;
uricontent:"/achcheck.php"; nocase; flowbits:set,ET.koobfacecheck; flowbits:noalert; classtype:trojan-activity;
reference:url,us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_20heart_20of_20koobface_final_1_.pdf; reference:url,doc.emergingthreats.net/2010151;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Koobface; sid:2010151; rev:4;)

#by jerry at cybercave
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Koobface C&C availability check successful"; flowbits:isset,ET.koobfacecheck; flow:established,from_server;
content:"|0d 0a 0d 0a|ACH_OK"; nocase; classtype:trojan-activity;
reference:url,us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_20heart_20of_20koobface_final_1_.pdf; reference:url,doc.emergingthreats.net/2010152;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Koobface; sid:2010152; rev:3;)

#by jerry at cybercave
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Koobface fetch C&C command detected"; flow:established, to_server; uricontent:".php"; nocase; content:"f=0&a=";
content:"&v="; content:"&c="; content:"&s="; content:"&l="; content:"&ck="; content:"&c_fb="; content:"&c_ms="; content:"&c_hi="; content:"&c_be="; content:"&c_fr="; content:"&c_yb=";
content:"&c_tg="; content:"&c_nl="; content:"&c_fu="; classtype:trojan-activity;
reference:url,us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_20heart_20of_20koobface_final_1_.pdf; reference:url,doc.emergingthreats.net/2010153;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Koobface; sid:2010153; rev:3;)

#by Steven Adair at shadowserver
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Likely Koobface Beaconing (getexe)"; flow:to_server,established; content:"GET "; nocase; depth:4; uricontent:"?
getexe="; uricontent:".exe"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010700; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Koobface; sid:2010700; rev:3;)

#by pedro Marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32/Korklic.A"; flow:to_server,established; content:"GET "; nocase; depth:4; uricontent:"mode=boot&MyValue=";
uricontent:"&code="; pcre:"/MyValue=[a-f0-9]{2}\:[a-f0-9]{2}\:[a-f0-9]{2}\:[a-f0-9]{2}\:[a-f0-9]{2}\:/Ui"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2009003;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Korklic; sid:2009003; rev:4;)

#trojan using this domain and UA
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Kpang.com Related Trojan User-Agent (kpangupdate)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
kpangupdate|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007779; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Kpang.com;
sid:2007779; rev:4;)

#trojan using this domain and UA
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Kpang.com Related Trojan User-Agent (alertup)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
alertup|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007849; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Kpang.com;
sid:2007849; rev:3;)

#by matt jonkman, from sandnet hits
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Krunchy/BZub HTTP Checkin/Update"; flow:established,to_server; uricontent:".php?action="; uricontent:"&guid=%";
content:"GET "; nocase; depth:4; content:!"|0d 0a|User-Agent|3a| "; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007775; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Krunchy; sid:2007775; rev:5;)

#by matt jonkman, from sandnet hits
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Krunchy/BZub HTTP POST Update"; flow:established,to_server; content:"|0d 0a 0d 0a|action="; content:"|25 35
46|script"; distance:0; content:"POST "; nocase; depth:5; content:!"|0d 0a|User-Agent|3a| "; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007776;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Krunchy; sid:2007776; rev:5;)

#By matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Lager Trojan Initial Checkin"; flow:established,to_server; uricontent:"/cp/rule.php?"; nocase;
uricontent:"fstt="; nocase; uricontent:"&b="; nocase; uricontent:"name="; classtype:trojan-activity; reference:url,www.viruslist.com/en/viruses/encyclopedia?virusid=87732;
reference:url,doc.emergingthreats.net/2003187; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Lager.Win32; sid:2003187; rev:3;)

#By matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Lager Trojan Reporting"; flow:established,to_server; uricontent:"/cp/rule.php?"; nocase; uricontent:"v=";
nocase; uricontent:"&b="; nocase; uricontent:"name="; classtype:trojan-activity; reference:url,www.viruslist.com/en/viruses/encyclopedia?virusid=87732;
reference:url,doc.emergingthreats.net/2003188; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Lager.Win32; sid:2003188; rev:3;)

#By matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Lager Trojan Reporting (gcu)"; flow:established,to_server; uricontent:"/cp/rule.php?"; nocase;
pcre:"/\/cp\/rule\.php\?gcu=\d+/Ui"; classtype:trojan-activity; reference:url,www.viruslist.com/en/viruses/encyclopedia?virusid=87732; reference:url,doc.emergingthreats.net/2003189;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Lager.Win32; sid:2003189; rev:3;)

#By matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Lager Trojan Reporting Spam"; flow:established,to_server; content:"POST "; nocase; depth:5;
uricontent:"/sp/post.php"; nocase; content:"data="; depth:400; classtype:trojan-activity; reference:url,www.viruslist.com/en/viruses/encyclopedia?virusid=87732;
reference:url,doc.emergingthreats.net/2003190; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Lager.Win32; sid:2003190; rev:6;)

#from anonymous
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET 1025:5000 (msg:"ET TROJAN Possible Web-based DDoS-command being issued"; flow: established,from_server; content: "Server|3a| nginx/0.";
offset: 17; depth: 19; content: "Content-Type|3a| text/html"; content:"|3a|80|3b|255.255.255.255"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003296;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Lager.Win32; sid:2003296; rev:4;)

#by Shirkdog
#re 8888fcb5020d1295f4343f601263306a
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Backdoor Lanfiltrator Checkin"; flow:established,to_server; uricontent:"/ralog.cgi"; uricontent:"&ip=";
uricontent:"&servertype=lanfiltrator"; classtype:trojan-activity; reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=Backdoor.Win32.LanFiltrator.3b&threatid=51642;
reference:url,doc.emergingthreats.net/2009078; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Lanfiltrator; sid:2009078; rev:2;)

#by matt jonkman
#
#alert tcp $EXTERNAL_NET 1024: -> $HOME_NET any (msg:"ET TROJAN Lethic Spambot CnC Initial Connect"; flow:established,from_server; flowbits:isnotset,ET.lethic.init;
flowbits:set,ET.lethic.init; flowbits:noalert; dsize:5; content:"|00 00 00 00 06|"; classtype:trojan-activity; reference:url,www.m86security.com/trace/spambotitem.asp?article=1205;
reference:url,doc.emergingthreats.net/2010646; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Lethic; sid:2010646; rev:3;)

#by matt jonkman
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Lethic Spambot CnC Initial Connect Bot Response"; flow:established,to_server; flowbits:isset,ET.lethic.init; dsize:5;
content:"|00 00 00 00 06|"; flowbits:set,ET.lethic.established; classtype:trojan-activity; reference:url,www.m86security.com/trace/spambotitem.asp?article=1205;
reference:url,doc.emergingthreats.net/2010647; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Lethic; sid:2010647; rev:3;)
```

```
#by matt jonkman
#
#alert tcp $EXTERNAL_NET 1024: -> $HOME_NET any (msg:"ET TROJAN Lethic Spambot CnC Connect Command"; flowbits:isset,ET.lethic.established; flow:established,from_server; dsize:11;
content:"|02|"; offset:4; depth:5; classtype:trojan-activity; reference:url,www.m86security.com/trace/spambotitem.asp?article=1205; reference:url,doc.emergingthreats.net/2010648;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Lethic; sid:2010648; rev:3;)

#by matt jonkman
#
#alert tcp $EXTERNAL_NET 1024: -> $HOME_NET any (msg:"ET TROJAN Lethic Spambot CnC Connect Command (port 25 specifically)"; flowbits:isset,ET.lethic.established;
flow:established,from_server; dsize:11; content:"|02|"; offset:4; depth:5; content:"|00 19|"; offset:9; classtype:trojan-activity;
reference:url,www.m86security.com/trace/spambotitem.asp?article=1205; reference:url,doc.emergingthreats.net/2010649; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Lethic; sid:2010649; rev:3;)

#by matt jonkman
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Lethic Spambot CnC Bot Command Confirmation"; flow:established,to_server; flowbits:isset,ET.lethic.established; dsize:6;
content:"|21 01|"; offset:4; classtype:trojan-activity; reference:url,www.m86security.com/trace/spambotitem.asp?article=1205; reference:url,doc.emergingthreats.net/2010650;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Lethic; sid:2010650; rev:3;)

#by matt jonkman
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Lethic Spambot CnC Bot Transaction Relay"; flow:established,to_server; flowbits:isset,ET.lethic.established;
content:"|03|"; offset:4; depth:5; classtype:trojan-activity; reference:url,www.m86security.com/trace/spambotitem.asp?article=1205; reference:url,doc.emergingthreats.net/2010651;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Lethic; sid:2010651; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Ligats/DR.Ilomo Agent Post"; flow:established,to_server; content:"POST /"; nocase; depth:6; content:"|0d 0a 0d
0a|o="; content:"&s=000"; distance:1; within:8; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008740; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Ligats; sid:2008740; rev:4;)

#New delf cnc. Also being called Trojan.PWS.Gamania.origin, Trojan-PSW.Win32.OnLineGames.aenl,
#Trojan-PSW.Win32.OnLineGames.aenl, Win32.Looked.P(v)
#re 7bbec6c1d7d727e70854184b1c1c5088
#
alert tcp $EXTERNAL_NET 81:90 -> $HOME_NET any (msg:"ET TROJAN Looked.P/Gamania/Delf #109/! Style CnC Checkin Response from Server"; flow:established,from_server; dsize:6; content:"#1";
depth:2; content:"/!"; offset:4; pcre:"/^\x23\d\d\d\x2f\x21/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/Win32Looked;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Looked; sid:2008220; rev:5;)

#New delf cnc. Also being called Trojan.PWS.Gamania.origin, Trojan-PSW.Win32.OnLineGames.aenl,
#Trojan-PSW.Win32.OnLineGames.aenl, Win32.Looked.P(v)
#re 7bbec6c1d7d727e70854184b1c1c5088
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 81:90 (msg:"ET TROJAN Looked.P/Gamania/Delf #108/! Style CnC Checkin"; flow:established,to_server; dsize:6; content:"#1"; depth:2; content:"/!";
distance:2; within:2; pcre:"/^\x23\d\d\d\x2f\x21/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/Win32Looked;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Looked; sid:2008219; rev:6;)

#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Lop.gfr/Swizzor HTTP Update/Checkin"; flow:established,to_server; content:"POST "; nocase; depth:5;
uricontent:"/tba/"; nocase; content:"|0d 0a|guid="; content:"&version="; content:"&clientid="; content:"&time="; content:"&idle="; content:"&ticksBoot="; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2007774; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Lop; sid:2007774; rev:6;)

#Deepash Misra
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Lop.gfr/Swizzor HTTP Update/Checkin (usually host-domain-lookup.com related)"; flow:established,to_server;
uricontent:"/upd/check?"; nocase; uricontent:"&fxp="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008333; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Lop; sid:2008333; rev:2;)

#by Marcus of unsober
#ref: 6eddfbc8886805b1eeb0d934b08cefff
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Swizzor Checkin"; flow:established,to_server; content:"GET "; nocase; depth:4; uricontent:"c="; uricontent:"&wv=";
uricontent:"&wd="; uricontent:"&ie="; content:"|0d 0a|User-Agent|3a| NSISDL/1.2 (Mozilla)"; classtype:successful-recon-limited; reference:url,doc.emergingthreats.net/2008347;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Lop; sid:2008347; rev:5;)

#by Deapesh Misra
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Swizzor Checkin (kgen_up)"; flow:to_server,established; uricontent:"kgen_up.int"; uricontent:"fxp="; pcre:"/fxp=[a-
z0-9]{60}/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008379; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Lop; sid:2008379;
rev:3;)

#by Rob Grabowsky
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Lop_com or variant Checkin (9kgen_up)"; flow:established,to_server; content:"GET "; nocase; depth:4;
uricontent:"/9kgen_up.int?"; nocase; classtype:trojan-activity; reference:url,www.threatexpert.com/reports.aspx?find=9kgen_up.int; reference:url,doc.emergingthreats.net/2008943;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Lop; sid:2008943; rev:3;)

#by: Jeremy Conway at sudosecure.net
#ref: 05f72061bb956336ee397e739d04242b
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Swizzor Family GET"; flow:established,to_server; content:"GET "; nocase; depth:4; uricontent:"szclientid=";
uricontent:"szmac="; uricontent:"szusername="; uricontent:"szver="; uricontent:"mode="; uricontent:"value="; uricontent:"systype="; uricontent:"rid="; uricontent:"szname=";
uricontent:"szpaname="; uricontent:"palen="; uricontent:"szpapaname="; uricontent:"chksum="; classtype:trojan-activity; reference:url,www.threatexpert.com/report.aspx?
md5=ed06e3cd6f57fc260194bf9fa224181e; reference:url,doc.emergingthreats.net/2009441; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Lop; sid:2009441; rev:3;)

#by: Jeremy Conway at sudosecure.net
#ref: 7f417525009a554c82d1329a26c60a90
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Swizzor-based Downloader - Invalid User-Agent (Mozilla/4.0 (compatible MSIE 7.0 na .NET CLR 2.0.50727 .NET CLR
3.0.4506.2152 .NET CLR 3.5.30729))"; flow:established,to_server; content:"GET "; nocase; depth:4; content:"|0d0a|User-Agent|3a| Mozilla/4.0 (compatible|3b| MSIE 7.0|3b| na|3b| .NET CLR
2.0.50727|3b| .NET CLR 3.0.4506.2152|3b| .NET CLR 3.5.30729)|0d0a|"; within:500; classtype:trojan-activity; reference:url,www.cyber-ta.org/releases/malware-analysis/public/2009-07-12-
public/ARCHIVE/1247423556.chatter; reference:url,doc.emergingthreats.net/2009810; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Lop; sid:2009810; rev:4;)

#by Marcus of unsober
#re 5f0920312f5a044d07b6425e2b6887f9
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Lost Door Checkin"; flow:established,to_server; content:"GET "; depth:4; uricontent:"subject=Lost|20|door|20|";
uricontent:"by|20|OussamiO"; content:"|0d 0a|User-Agent|3a| Mozilla/4.0 (compatible|3b| MSIE 6.0|3b| Windows NT 5.1|3b| SV1)"; classtype:trojan-activity; nocase;
reference:url,doc.emergingthreats.net/2008340; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Lost_Door; sid:2008340; rev:4;)

#by: Jeremy Conway at sudosecure.net
#ref: 073098e919581aff1456abed109a1eb4
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Luder.B User-Agent (Mozilla/4.0 (SPGK)) - GET"; flow:established,to_server; content:"GET "; nocase; depth:4;
content:"|0d 0a|User-Agent|3a| Mozilla/4.0 (SPGK)|0d 0a|"; nocase; within:300; classtype:trojan-activity; reference:url,home.mcafee.com/VirusInfo/VirusProfile.aspx?key=212955#none;
reference:url,www.threatexpert.com/threats/virus-win32-luder-b.html; reference:url,doc.emergingthreats.net/2009805; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Luder; sid:2009805; rev:4;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Lydra.hj HTTP Checkin"; flow:established,to_server; uricontent:"/NewsFolder/News00"; uricontent:".ASP?id=";
pcre:"/\/NewsFolder\/News00\d\d\.ASP\?id=/U"; pcre:"/Host\: \d+\.\d+\.\d+\.\d+/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008130;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Lydra; sid:2008130; rev:2;)

#by Matt Jonkman, MBR Virus related
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN MBR Trojan (Sinowal/Mebroot/) Phoning Home"; flow:established,to_server; content:"POST "; nocase; depth:5;
uricontent:"/ld/mat"; nocase; uricontent:".php"; nocase; content:"|0d 0a|id="; distance:30; content:"&hit="; distance:5; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2007747; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_MBR; sid:2007747; rev:4;)

#by Victor Julien
#Ikarus: AdWare.Win32.MWGuide,
#re a98bb554bf012dd25d94b764bc4a0678
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN AdWare.Win32.MWGuide checkin"; flow:established,to_server; uricontent:"/sidebar_load.php?maddr=";
uricontent:"ipaddr="; uricontent:"aff_id="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008839; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_MWGuide; sid:2008839; rev:3;)

#by Victor Julien
#Ikarus: AdWare.Win32.MWGuide,
#re a98bb554bf012dd25d94b764bc4a0678
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN AdWare.Win32.MWGuide keepalive"; flow:established,to_server; uricontent:"/alive.php?aff_id="; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/2008840; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_MWGuide; sid:2008840; rev:3;)

#info from Bojan at ISC and Russell Fulton
#sig by Russell and Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Mac Trojan HTTP Checkin (accept-language violation)"; flow:established,to_server; content:"GET "; depth:4; content:"
HTTP/1.1|0d 0a|Accept-Language|3a| "; pcre:"/Accept-Language\: [a-zA-Z0-9]{20}/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007650;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Mac_Trojan; sid:2007650; rev:4;)

#by victor julien
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Mac User-Agent Typo - Likely Hostile/Trojan Infection"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
Mozilla/5.0 (Macintosh|3b|"; content:"(KHTML, like Geco,"; within:100; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008954;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Mac_UA_Typo; sid:2008954; rev:3;)

#by victor julien
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET TROJAN Mac User-Agent Typo INBOUND - Likely Hostile"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
Mozilla/5.0 (Macintosh|3b|"; content:"(KHTML, like Geco,"; within:100; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008955;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Mac_UA_Typo; sid:2008955; rev:3;)

#by Chuck Conn at the World Bank
#
alert udp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Palevo/BFBot/Mariposa client join attempt"; dsize:7; content:"|61|"; depth:1; flowbits:noalert;
flowbits:set,ET.MariposaJoin; classtype:trojan-activity; reference:url,defintel.com/docs/Mariposa_Analysis.pdf; reference:url,defintel.blogspot.com/2009/09/half-of-fortune-100-
companies.html; reference:url,doc.emergingthreats.net/2010100; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Mariposa;
reference:url,blogs.pcmag.com/securitywatch/2009/09/botnet_reported_loose_in_fortu.php; reference:url,www.symantec.com/business/security_response/writeup.jsp?docid=2009-093006-0442-
99&tabid=2; reference:url,www.symantec.com/connect/blogs/mariposa-butterfly; sid:2010100; rev:5;)

#by Chuck Conn at the World Bank
#
alert udp $EXTERNAL_NET 1024: -> $HOME_NET 1024: (msg:"ET TROJAN Palevo/BFBot/Mariposa server join acknowledgement"; dsize:8; content:"|40|"; depth:1; flowbits:isset,ET.MariposaJoin;
classtype:trojan-activity; reference:url,defintel.com/docs/Mariposa_Analysis.pdf; reference:url,defintel.blogspot.com/2009/09/half-of-fortune-100-companies.html;
reference:url,doc.emergingthreats.net/2010101; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Mariposa;
reference:url,blogs.pcmag.com/securitywatch/2009/09/botnet_reported_loose_in_fortu.php; reference:url,www.symantec.com/business/security_response/writeup.jsp?docid=2009-093006-0442-
99&tabid=2; reference:url,www.symantec.com/connect/blogs/mariposa-butterfly; sid:2010101; rev:5;)

#these are mcboo.com and bundlext.com related. David Yawsa registrant
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Mcboo.com/Bundlext.com related Trojan Checkin URL"; flow:established,to_server; uricontent:"/ack.php?version=";
uricontent:"&uid="; uricontent:"&status="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008758; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Mcboo.com; sid:2008758; rev:2;)

#by Matt Jonkman, significant update from Don Jackson of Secureworks
#
alert udp $HOME_NET any -> $EXTERNAL_NET 6990:6999 (msg:"ET TROJAN Medbod UDP Phone Home Packet"; dsize:<50; content:"ebex"; nocase; pcre:"/\x06\x00?$/"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2007949; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Medbod; sid:2007949; rev:6;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN MEREDROP/micr0s0fts.cn Related Checkin"; flow:established,to_server; content:"POST "; nocase; depth:5;
uricontent:"/update.asp"; content:"|0d 0a 0d 0a|ver="; content:"|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00|"; distance:8; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008891; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Meredrop; sid:2008891; rev:3;)

#by David Bianco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Metajuan trojan checkin"; flow:established,to_server; uricontent:"trafc-2/rfe"; nocase; classtype: trojan-activity;
reference:url,www.symantec.com/security_response/writeup.jsp?docid=2007-030112-0714-99; reference:url,doc.emergingthreats.net/2007811; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Metajuan; sid:2007811; rev:3;)

#by Scott Melnick
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Downloader.MisleadApp Fake Security Product Install"; flow:established,to_server; content:"GET "; nocase; depth:4;
uricontent:"hash?http"; nocase; pcre:"/\/(ucleaner|udefender|ufixer)\.com\/demo\.php\?/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007566;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_MisleadApp; sid:2007566; rev:5;)

#Added 2005-10-04 in response to ISC diary
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Mitglieder Proxy Bot Checking In"; flow:established,to_server; uricontent:"/scr5.php"; nocase; pcre:"/\/scr5\.php\?
p=\d+&id=\d+/Ui"; classtype:trojan-activity; reference:url,isc.sans.org/diary.php?storyid=722; reference:url,doc.emergingthreats.net/2002387; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Mitglieder; sid:2002387; rev:6;)

#by Marcus of unsober
#ref: 7d5651c19e316480971eb5406727f720
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Mitglieder Checkin"; flow:established,to_server; content:"GET "; nocase; depth:4; uricontent:"p=";
uricontent:"&id="; content:"|0d 0a|User-Agent|3a| personal"; classtype:trojan-activity; nocase; reference:url,doc.emergingthreats.net/2008346; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Mitglieder; sid:2008346; rev:5;)

#by David Wharton
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32/Monkif Downloader Checkin"; flow:to_server,established; uricontent:"/cgi/"; uricontent:".php?"; nocase;
uricontent:"x640<x"; classtype:trojan-activity; reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=TrojanDownloader%3aWin32%2fMonkif.C;
reference:url,doc.emergingthreats.net/2009126; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Monkif; sid:2009126; rev:6;)

#by David Wharton
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Monkif/DlKroha Trojan Activity HTTP Outbound"; flow:to_server,established; uricontent:"/cgi/"; uricontent:".php?";
uricontent:"x4x4x"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009752; reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?
Name=TrojanDownloader%3aWin32%2fMonkif.C; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Monkif; sid:2009752; rev:3;)

#by: Jeremy Conway at sudosecure.net
#ref: 07fe977eb92b9ecc4b40f182604223fb
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Trojan.MyDNS DNSChanger - HTTP POST"; flow:established,to_server; content:"POST "; nocase; depth:5; content:"|0d
0a|Cache-Control|3a 20|no-cache|0d 0a 0d 0a|r="; nocase; content:"&f="; nocase; content:"&p="; nocase; content:"&u="; nocase; content:"&i="; nocase; content:"&g="; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009813; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_MyDNS; sid:2009813; rev:3;)

#from Matt Richard with Verisign Security Services / iDefense
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 80 (msg:"ET TROJAN NPRC Malicious POST Request Possible DOJ or DOT Malware"; flow:to_server; content:"POST "; nocase; depth:5;
content:"ACCEPT|3A|"; nocase; within:300; content:"POST|2C|"; nocase; within:100; classtype:trojan-activity; reference:url,www.websense.com/securitylabs/alerts/alert.php?AlertID=835;
reference:url,doc.emergingthreats.net/2007748; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_NPRC; sid:2007748; rev:5;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Nanspy Bot Checkin"; flow:established,to_server; content:"HEAD "; nocase; depth:5; uricontent:"/bbcount.php?
action="; uricontent:"&uid="; uricontent:"&locale="; uricontent:"&build="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010158;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Nanspy; sid:2010158; rev:3;)

#by Markus Lude
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Navipromo related update"; flow:established,to_client; content:"|0d 0a|Server|3a| lighttpd|0d 0a 0d 0a|<HTML>
<CFG>_SYSTEM_DIR_"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009694; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Navipromo;
sid:2009694; rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Nbar.co.kr Related Trojan Checkin"; flow:established,to_server; uricontent:"?nid_mac=";
uricontent:"&nid_os_ver=Windows"; uricontent:"&nid_ie_ver="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008592; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Nbar.co.kr; sid:2008592; rev:2;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Neonaby.com Related Trojan User-Agent (neonabyupdate)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
neonabyupdate|0d 0a|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007825; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Neonaby.com; sid:2007825; rev:3;)

#by Darren Spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Trojan.Win32.Inject.esi Outbound Communication"; flow:established,to_server; content:"GET "; depth:4;
isdataat:62,relative; content:"|0d 0a|Accept-Language|3a| en-en"; nocase; pcre:"/\/[A-Za-z0-9]{2,16}\/[A-Za-z0-9]{2,16}\d{5}\/\d{1,5}\/\d{2}[A-Za-z0-9]{2,16}\/[A-Za-z0-9]
{2,16}\d{3}\//sm"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009125; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Netnam;
sid:2009125; rev:9;)

#by Philipp Bescht
#ref: 965583b539fb59b643c7bdd83e269a7e
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 2227 (msg:"ET TROJAN Trojan-PSW.Win32.Nilage.crg Checkin"; flow:established,to_server; dsize:32; content:"|00 c0 a8 01 f4 6f 00 00 00|";
depth:12; content:"|00 00 00 05 01 28 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008481; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Nilage; sid:2008481; rev:3;)

#by dn1nj4
#
alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Nine Ball Infection Ping Outbound"; icode:0; itype:8; dsize:32; content:"EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011185; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_NineBall; sid:2011185; rev:2;)

#by dn1nj4
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Nine Ball Infection ya.ru Post"; flow:established,to_server; content:"POST /"; depth:6; uricontent:"/gate/";
uricontent:".php"; content:"|0d 0a 0d 0a|"; content:"ya.ru/"; distance:67; within:6; classtype:trojan-activity; reference:url,www.martinsecurity.net/page/3;
reference:url,doc.emergingthreats.net/2011186; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_NineBall; sid:2011186; rev:3;)

#by dn1nj4
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Nine Ball Infection Posting Data"; flow:established,to_server; content:"POST /"; depth:6; content:"/gate/";
distance:0; content:".php"; distance:0; content:"|0d 0a 0d 0a|"; distance:0; content:"AAAAAAAACI"; distance:67; within:10; classtype:trojan-activity;
reference:url,www.martinsecurity.net/page/3; reference:url,doc.emergingthreats.net/2011187; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_NineBall;
sid:2011187; rev:3;)

#by dn1nj4
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Nine Ball User-Agent Detected (NQX315)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| NQX315|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011188; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_NineBall; sid:2011188; rev:3;)

#by Jeremy Conway at sudosecure.net
#ref: 62c1608a16a6857228adfce266779ea6
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN NoBo Downloader Dropper GET"; flow:established,to_server; content:"GET "; nocase; depth:4; content:"User-Agent|3a|
NoBo"; classtype:trojan-activity; reference:url,www.spynomore.com/trojan-nobo-v1-3.htm; reference:url,doc.emergingthreats.net/2009443; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Nobo; sid:2009443; rev:4;)

#by Matt Jonkman
#Advisory by Websense, www.websense.com/securitylabs/alerts/alert.php?AlertID=743
#This one is from what appears to be a typo in the get string right after the initial infection
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Nukebot related infection - Unique HTTP get request"; flow:established,to_server; content:".dll|0d
0a|e|20|HTTP/1.1"; rawbytes; content:!"User-Agent|3a|"; nocase; classtype:trojan-activity; reference:url,www.websense.com/securitylabs/alerts/alert.php?AlertID=743;
reference:url,doc.emergingthreats.net/2003432; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Nukebot; sid:2003432; rev:4;)

#by Matt Jonkman
#Advisory by Websense, www.websense.com/securitylabs/alerts/alert.php?AlertID=743
#This one is from what appears to be a typo in the get string right after the initial infection
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Nukebot Checkin"; flow:established,to_server; content:"POST "; rawbytes; depth:5; uricontent:"/script.php?";
content:!"User-Agent|3a|"; nocase; pcre:"/\/script\.php?\d{8}/Ui"; content:"Kernel|3a|"; classtype:trojan-activity; reference:url,www.websense.com/securitylabs/alerts/alert.php?
AlertID=743; reference:url,doc.emergingthreats.net/2003433; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Nukebot; sid:2003433; rev:4;)

#by Matt Jonkman, from sandnet
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Nulprot Checkin Response"; flow:established,from_server;  content:"HTTP/1.0 200 OK|0d 0a|Encryption|3a| on|0d
0a|Content-Length\: "; offset:0; depth:49;  classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007669; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Nulprot; sid:2007669; rev:8;)

#ref: 6b4ef50e3e21205685cea919ebf93476
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Obitel trojan calling home"; flow:established,to_server; uricontent:"/gate.php?hash="; content:"/gate.php?hash=";
content:" HTTP/1."; distance:8; within:16; classtype:trojan-activity; reference:url,www.abuse.ch/?p=143; reference:url,doc.emergingthreats.net/2008405;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Obitel; sid:2008405; rev:3;)

#by darren spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Obitel Downloader Request"; flow: established,to_server; uricontent:".php?id="; content:"|0d 0a|User-Agent|3a| ie|0d
0a|"; pcre:"/\.php\?id=[0-9a-f]{8}$/U"; classtype:trojan-activity; reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?
Name=TrojanDownloader%3aWin32%2fObitel.gen!A; reference:url,threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_AGENT.ASLV&VSect=T;
reference:url,doc.emergingthreats.net/2010244; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Obitel; sid:2010244; rev:3;)

##by darren spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Oficla Downloader Activity Observed"; flow:established,to_server; content:"GET "; nocase; depth:4; uricontent:".php?
id="; nocase; uricontent:"&v="; nocase; uricontent:"&tm="; nocase; uricontent:"&b="; nocase; pcre:"/\x2Ephp\x3Fid\x3D\d*\x26v\x3D\d*\x26tm\x3D\d*\x26b\x3D\d*/iU"; classtype:trojan-
activity; reference:url,www.threatexpert.com/report.aspx?md5=38e1d644e2a16041b5ec1a02826df280; reference:url,www.threatexpert.com/report.aspx?md5=1db0c8d48a76662496af7faf581b1cf0;
reference:url,doc.emergingthreats.net/2009776; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Oficla; sid:2009776; rev:3;)

#by evilghost and darren spruell and mike cox and crew
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Oficla Checkin (1)"; flow:established,to_server; content:"GET "; nocase; depth:4; content:!"|0d 0a|Referer|3a| ";
nocase; content:!"|0d 0a|Accept-Encoding|3a| "; nocase; uricontent:".php?"; nocase; uricontent:"v="; nocase; uricontent:"&id="; nocase; uricontent:"&b="; nocase; uricontent:"&tm=";
nocase; classtype:trojan-activity; reference:url,www.threatexpert.com/report.aspx?md5=f71d48a86776f8c0da4d7a46257ff97c; reference:url,doc.emergingthreats.net/2010743;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Oficla; sid:2010743; rev:5;)

#by evilghost
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Oficla Russian Malware Bundle C&C instruction response with runurl"; flow:established,to_client; content:"|0d 0a 0d
0a|[info]runurl|3a|"; content:"|7c|taskid|3a|"; within:100; content:"|7c|delay|3a|"; within:30; content:"|7c|upd|3a|"; within:20; content:"[/info]"; distance:0; classtype:trojan-
activity; reference:url,malwarelab.org/2009/11/russian-malware-bundle/; reference:url,doc.emergingthreats.net/2010723; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Unknown; sid:2010723; rev:3;)

#by evilghost
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Oficla Russian Malware Bundle C&C instruction response"; flow:established,to_client; content:"|0d 0a 0d 0a|
[info]kill|3a|"; content:"|7c|delay|3a|"; within:50; content:"|7c|upd|3a|"; within:20; content:"[/info]"; distance:0; classtype:trojan-activity;
reference:url,malwarelab.org/2009/11/russian-malware-bundle/; reference:url,doc.emergingthreats.net/2010724; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Unknown; sid:2010724; rev:3;)

#by evilghost
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Oficla Russian Malware Bundle C&C instruction response (2)"; flow:established,to_client; content:"|0d 0a 0d 0a|
[info]delay|3a|"; content:"|7c|upd|3a|"; within:20; content:"[/info]"; distance:0; classtype:trojan-activity; reference:url,malwarelab.org/2009/11/russian-malware-bundle/;
reference:url,doc.emergingthreats.net/2010744; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Unknown; sid:2010744; rev:3;)

#by victor julien
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN onmuz.com Infection Activity"; flow:established,to_server; uricontent:"pid=patchup_notpid_update^on";
uricontent:"/logonmuz"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008973; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Onmuz.com;
sid:2008973; rev:3;)

#by darren spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Opachki Link Hijacker Traffic Redirection"; flow:established,to_server; uricontent:"/?do=rphp"; nocase;
uricontent:"&sub="; nocase; uricontent:"&b="; nocase; uricontent:"&q="; nocase; uricontent:"&orig="; nocase; classtype:trojan-activity;
reference:url,www.secureworks.com/research/threats/opachki/?threat=opachki; reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?
Name=Trojan%3aWin32%2fOpachki.A; reference:url,www.symantec.com/security_response/writeup.jsp?docid=2009-092213-3317-99&tabid=2; reference:url,doc.emergingthreats.net/2010224;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Opachki; sid:2010224; rev:2;)

#by darren spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Opachki Link Hijacker HTTP Header Injection"; flow:established,to_server; uricontent:".php?l="; nocase;
uricontent:"&u="; nocase; content:"|0d 0a|Accept-Encoding|3a|"; nocase; content:"|0d 0a|Referer|3a| "; nocase; pcre:"/\x0d\x0aAccept-Encoding\x3a\s+([a-z])\1{3,}/i"; classtype:trojan-
activity; reference:url,www.secureworks.com/research/threats/opachki/?threat=opachki; reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?
Name=Trojan%3aWin32%2fOpachki.A; reference:url,www.symantec.com/security_response/writeup.jsp?docid=2009-092213-3317-99&tabid=2; reference:url,doc.emergingthreats.net/2010283;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Opachki; sid:2010283; rev:3;)

#matt jonkman, re 9fcea128aeff455ff8f6c9558dd150fd
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN Optix Pro Trojan/Keylogger Reporting Installation via Email"; flow:established,to_server; content:"|0d 0a|X-Priority|3a| 3|0d
0a|X-Library|3a| Indy "; content:"|0d 0a 0d 0a|Optix Pro v"; distance:4; within:25; classtype:trojan-activity; reference:url,en.wikipedia.org/wiki/Optix_Pro;
reference:url,doc.emergingthreats.net/2008212; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Optix; sid:2008212; rev:4;)

#matt jonkman, re 9fcea128aeff455ff8f6c9558dd150fd
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Optix Pro Trojan/Keylogger Reporting Installation via HTTP-Email Post"; flow:established,to_server; content:"POST ";
nocase; depth:5; content:"|0d 0a 0d 0a|to="; content:"Optix Pro v"; distance:0; within:250; content:" Server Online"; within:40; classtype:trojan-activity;
reference:url,en.wikipedia.org/wiki/Optix_Pro; reference:url,doc.emergingthreats.net/2008218; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Optix;
sid:2008218; rev:4;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Otwycal User-Agent (Downing)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Downing|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008159; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Otwycal; sid:2008159; rev:4;)

#also called VB-EMU:VB-Backdoor-PEK-based!Ma
#
alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Overtoolbar.net Backdoor ICMP Checkin Request"; dsize:9; icode:0; itype:8; content:"Echo This"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2009130; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Overtoolbar.net; sid:2009130; rev:3;)

#also called VB-EMU:VB-Backdoor-PEK-based!Ma
#
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN Overtoolbar.net Backdoor ICMP Checkin Response"; dsize:9; icode:0; itype:0; content:"Echo This"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2009131; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Overtoolbar.net; sid:2009131; rev:3;)

#by Russ McRee of expedia.com
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN - Trojan.Proxy.PPAgent.t (updatea)"; flow:to_server,established; uricontent:"/updatea.php?p="; nocase;
pcre:"/updatea.php?p=\d+/Ui"; classtype:trojan-activity; flowbits:set,BT.ppagent.updatea; flowbits:noalert; reference:url,original.avira.com/en/threats/vdf_history.html?id_vdf=2738;
reference:url,doc.emergingthreats.net/2003115; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PPAgent; sid:2003115; rev:3;)

#by Russ McRee of expedia.com
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN - Trojan.Proxy.PPAgent.t (updateb)"; flowbits:isset,BT.ppagent.updatea; flow:to_server,established;
uricontent:"/updateb.php?p="; nocase; pcre:"/updateb.php?p=\d+/Ui"; classtype:trojan-activity; flowbits:unset,BT.ppagent.updatea;
reference:url,original.avira.com/en/threats/vdf_history.html?id_vdf=2738; reference:url,doc.emergingthreats.net/2003116; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PPAgent; sid:2003116; rev:3;)

#by Lance James and Michael Ligh, referenced in paper at http://www.securescience.net/FILES/securescience/10378/pubMalwareCaseStudy.pdf
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 80 (msg:"ET TROJAN Prg Trojan v0.1-v0.3 Data Upload"; flow:to_server,established; content:"POST "; nocase; depth:5; uricontent:"php?";
content:"Content-Type|3a20|binary"; depth:512; content:"LLAH"; within:512; classtype:trojan-activity;
reference:url,www.securescience.net/FILES/securescience/10378/pubMalwareCaseStudy.pdf; reference:url,doc.emergingthreats.net/2003182; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PRG; sid:2003182; rev:7;)

#by Lance James and Michael Ligh, referenced in paper at http://www.securescience.net/FILES/securescience/10378/pubMalwareCaseStudy.pdf
#
alert tcp $EXTERNAL_NET 80 -> $HOME_NET any (msg:"ET TROJAN Prg Trojan Server Reply"; flow:to_client,established; content:"HTTP"; depth:4; content:"|0d0a|Hall|3a|"; depth:512;
classtype:trojan-activity; reference:url,www.securescience.net/FILES/securescience/10378/pubMalwareCaseStudy.pdf; reference:url,doc.emergingthreats.net/2003183;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PRG; sid:2003183; rev:5;)

#by Lance James and Michael Ligh, referenced in paper at http://www.securescience.net/FILES/securescience/10378/pubMalwareCaseStudy.pdf
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN Prg Trojan v0.1 Binary In Transit"; flow:to_client,established; content:"MZ"; content:"|1D B9 F2 75 62 85 5A 4F 15 48 52 1D
50 90 41 89 37 9F FF 94 CE A6 3E 63 35 AB 29 6B 30 43 2F 45 46 B0 E1 C2 11 7F 0C 55 0F C7|"; depth:128; classtype:trojan-activity;
reference:url,www.securescience.net/FILES/securescience/10378/pubMalwareCaseStudy.pdf; reference:url,doc.emergingthreats.net/2003184; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PRG; sid:2003184; rev:5;)

#by Lance James and Michael Ligh, referenced in paper at http://www.securescience.net/FILES/securescience/10378/pubMalwareCaseStudy.pdf
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN Prg Trojan v0.2 Binary In Transit"; flow:to_client,established; content:"MZ"; content:"|13 B9 F2 75 62 85 5A 4F 15 48 19 1D
10 4F 0D 5B 04 5B 04 60 CE 5F 00 67 F5 AE 25 6B 20 41 23 B3|"; depth:128; classtype:trojan-activity;
reference:url,www.securescience.net/FILES/securescience/10378/pubMalwareCaseStudy.pdf; reference:url,doc.emergingthreats.net/2003185; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PRG; sid:2003185; rev:5;)

#by Lance James and Michael Ligh, referenced in paper at http://www.securescience.net/FILES/securescience/10378/pubMalwareCaseStudy.pdf
#
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN Prg Trojan v0.3 Binary In Transit"; flow:to_client,established; content:"MZ"; content:"| 5E 7D 66 7D 28 40 19 88 5F 8C 13 50
15 59 08 58 3C 97 00 9B 33 A5 F9 AF 39 68 F0 9F 27 AF E9 A8 25 B7 18 B6 15 7F 0E B6 1A|"; depth:128; classtype:trojan-activity;
reference:url,www.securescience.net/FILES/securescience/10378/pubMalwareCaseStudy.pdf; reference:url,doc.emergingthreats.net/2003186; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PRG; sid:2003186; rev:5;)

#by Jeremy Conway
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Prg Trojan HTTP POST v1"; flow:established,to_server; content:"POST "; nocase; depth:5; uricontent:".php?2=";
uricontent:"&n="; uricontent:"&v="; uricontent:"&i="; uricontent:"&sp="; uricontent:"&lcp="; classtype:trojan-activity;
reference:url,www.securescience.net/FILES/securescience/10378/pubMalwareCaseStudy.pdf; reference:url,doc.emergingthreats.net/2007688; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PRG; sid:2007688; rev:7;)

#by Jeremy Conway
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Prg Trojan HTTP POST version 2"; flow:established,to_server; content:"POST "; nocase; depth:5; uricontent:".php?1=";
uricontent:"&i="; pcre:"/\.php\?1=[a-z0-9]+_[a-z0-9_]+&i=/Ui"; classtype:trojan-activity; reference:url,www.securescience.net/FILES/securescience/10378/pubMalwareCaseStudy.pdf;
reference:url,doc.emergingthreats.net/2007724; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PRG; sid:2007724; rev:8;)

#by steven adair from shadowserevr
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN PRG/wnspoem/Zeus InfoStealer Trojan Config Download"; flow:established; uricontent:"/cfg.bin"; nocase; content:"GET
"; depth: 4; nocase; content:"no-cache|0d 0a 0d 0a|"; nocase; within:300; pcre:"/\/cfg\.bin$/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008100;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PRG; sid:2008100; rev:5;)

#by Jeremy at sudosecure
#ref 5b59da8ec99f65e02bcd0e48e14c43a8
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Banker Infostealer/PRG POST on High Port"; flow:to_server,established; content:"POST "; depth:5; content:"|2E|php|3F|2=";
nocase; content:"|26|n="; nocase; content:"|26|v="; nocase; content:"|26|i="; nocase; content:"|26|sp="; nocase; content:"|26|lcp="; nocase; classtype:trojan-activity;
reference:url,www.securescience.net/FILES/securescience/10378/pubMalwareCaseStudy.pdf; reference:url,doc.emergingthreats.net/2008326; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PRG; sid:2008326; rev:4;)

#by Tom Fischer
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN PWS-LDPinch Reporting User Activity"; flow:established,to_server; uricontent:".php?ut="; nocase; uricontent:"&idr=";
nocase; uricontent:"&lang="; nocase; uricontent:"&ver="; nocase; uricontent:"&winver="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2002812;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PWS-LDPinch; sid:2002812; rev:3;)

#New by Matt Jonkman, re 0a7b2d160c90af079dbe560b38c89d3f in sandnet
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN PWS-LDPinch posting data"; flow:established,to_server; dsize:>400; content:"POST "; depth:5; content:"|0d 0a 0d
0a|a="; nocase; content:"&b="; nocase; within:10; content:"&d="; nocase; within:20; content:".bin&"; nocase; within:30; content:"u="; nocase; within:10; content:"&c="; nocase;
within:20; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006385; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PWS-LDPinch; sid:2006385;
rev:3;)

#New by Matt Jonkman, re 0a7b2d160c90af079dbe560b38c89d3f in sandnet
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN PWS-LDPinch posting data (2)"; flow:established,to_server; dsize:>400; content:"POST / HTTP/1.1"; depth:15;
content:"|0d 0a 0d 0a|a="; nocase; content:"&b="; nocase; distance:0; content:"&c="; nocase; distance:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007756;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PWS-LDPinch; sid:2007756; rev:3;)

#more pinch
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN LDPinch Checkin (2)"; flow:established,to_server; content:"POST "; nocase; depth:5; uricontent:".php"; nocase;
content:"|0d 0a 0d 0a|a="; content:"&b="; nocase; distance:0; content:"&d="; nocase; distance:0; content:"&c="; distance:0; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2007828; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PWS-LDPinch; sid:2007828; rev:7;)

#more pinch
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN LDPinch Checkin (3)"; flow:established,to_server; content:"a="; offset:0; depth:2; content:"&b=Passes from";
distance:0; content:"&c="; distance:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007862; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PWS-LDPinch; sid:2007862; rev:8;)

#more pinch
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN LDPinch Checkin (4)"; flow:established,to_server; content:"a="; offset:0; depth:2; content:"&b=Pinch"; nocase;
distance:0; content:"&c="; distance:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008061; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PWS-LDPinch; sid:2008061; rev:3;)

#more pinch
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN LDPinch Checkin (8)"; flow:established,to_server; uricontent:"/view.php"; nocase; content:"a="; content:"&b=Passes";
distance:0; content:"&d=Pass"; distance:0; content:"&c="; distance:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008091;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PWS-LDPinch; sid:2008091; rev:2;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN LDPinch SMTP Password Report"; flow:established,to_server; content:"Subject|3a| Passes from "; depth:21; content:"|0d
0a|Content-Disposition|3a| attachment\; filename=\"report.bin\""; distance:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008034;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PWS-LDPinch; sid:2008034; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN LDPinch Checkin (9)"; flow:established,to_server; dsize:>1000; content:"POST "; depth:5; uricontent:"/gate.php";
nocase; content:"|0d 0a 0d 0a|a=&b=&d=&c="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008213; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PWS-LDPinch; sid:2008213; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 82 (msg:"ET TROJAN LDPinch Checkin on Port 82"; flow:established,to_server; content:".php"; nocase; content:"a="; content:"&b=Pinch";
distance:0; content:"&d="; distance:0; content:"&c="; distance:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008354; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PWS-LDPinch; sid:2008354; rev:3;)

#Marcus at unsober
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 82 (msg:"ET TROJAN LD Pinch Checkin (HTTP POST on port 82)"; flow:established,to_server; content:"POST "; depth:5; content:".php"; content:"a=";
content:"&b="; content:"&d="; content:"&c="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008366; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PWS-LDPinch; sid:2008366; rev:2;)

#re 415908b65e87d91daa94704ef7e2788b, by jholguin (tb-security)
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN LDPinch SMTP Password Report with mail client The Bat!"; flow:established,to_server; content:"X-Mailer|3a| The Bat!";
content:"|0d 0a|Content-Disposition|3a| attachment|3b|"; content:!"|0d 0a|Subject|3a| Undeliverable|3a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008411;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PWS-LDPinch; sid:2008411; rev:5;)

#by Jeremy at sudosecure
#ref: 04406e913a0070eac26df3627a7a05c1
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN LDPinch Checkin Flowbit set"; flow:established,to_server; content:"POST "; depth:5; uricontent:"/gate.php"; nocase;
content:"application|2F|x-www-form-urlencoded|0D 0A|"; flowbits:set,ET.PINCH; flowbits:noalert; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008468;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PWS-LDPinch; sid:2008468; rev:3;)

#by Jeremy at sudosecure
#ref: 04406e913a0070eac26df3627a7a05c1
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN LDPinch Checkin v2"; flowbits:isset,ET.PINCH; flow:established,to_server; content:"a="; nocase; content:"b=";
nocase; content:"d="; nocase; content:"c="; nocase; flowbits:unset,ET.PINCH; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008469;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PWS-LDPinch; sid:2008469; rev:2;)
```

```
#matt jonkman, re 3663a14f15dbee42422fc8685740f493
#
alert tcp $HOME_NET any -> $EXTERNAL_NET [587,25] (msg:"ET TROJAN LDPinch Reporting infection via Email"; flow:established,to_server; content:"X-Mailer|3a| Blat v2.6.2 w/GSS encryption,
a Win32 SMTP/NNTP mailer http|3a|//www.blat.net|0d 0a|"; content:"|0d 0a|Subject|3a| Contents of file|3a| WINDOWS/system32/"; distance:0; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2009242; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PWS-LDPinch; sid:2009242; rev:3;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET VIRUS PWS Banker Trojan Sending Report of Infection"; flow: established,to_server; content:"From|3a 20 22|PC ID|3a|"; nocase;
content:"Subject|3a| INFECTED"; nocase; content:"esta infectado"; nocase; classtype: trojan-activity;
reference:url,securityresponse.symantec.com/avcenter/venc/data/pwsteal.banker.b.html; reference:url,doc.emergingthreats.net/2001933; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PWS_Banker; sid:2001933; rev:9;)

#from castlecops research, http://www.castlecops.com, sig by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Generic Password Stealer User Agent Detected (RookIE)"; flow:established,to_server; content:"User-Agent|3a| RookIE";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003635; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PWS_Generic; sid:2003635;
rev:5;)

#from sandnet research, by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Generic Password Stealer Checkin URL Detected"; flow:established,to_server; uricontent:"method=get"; nocase;
uricontent:"&port="; nocase; uricontent:"&type="; nocase; uricontent:"&winver="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006384;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PWS_Generic; sid:2006384; rev:5;)

#by marcus at unsober
#ref: 5b0db5cfe1699345f3a077b8f62aaaff
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Trojan-PWS.Win32.VB.tr Checkin Detected"; flow:established,to_server; content:"POST "; depth:5; uricontent:".asp";
content:"id="; content:"&tit="; content:"&comm"; content:"Run|2B|Successfully"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008506;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PWS_Generic; sid:2008506; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN Banito/Agent.pb Pass Stealer Email Report Outbound"; flow:established,to_server; content:"Subject|3a| Vip Passw0rds|0d 0a 0d
0a|Victim Name |3a| "; content:"|0d 0a|######## ICQ PASSWORDS ########"; distance:0; within:70; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008551;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PWS_Generic; sid:2008551; rev:3;)

#by Jeremy at sudosecure
#ref: 5742862edc6fddd3f51bf9d07c8d7aba
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Generic PSW Agent server reply"; flow:from_server,established; content:"200 OK"; depth:15; content:"|0d 0a|
[Uptade]|0d 0a|Web="; within:300; content:"|0d 0a|[Guncellestirme]|0d 0a|Version="; within:100; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008662;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PWS_Generic; sid:2008662; rev:2;)

#by victor julien
#Ikarus: Trojan-PWS.Win32.Small.gs,
#re d752a38abd5327552d5b51cd0e091436
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Trojan-PWS.Win32.Small.gs Passwords leak over FTP"; flow:established,to_server; content:"IE7 Passwords|3a|"; depth:14;
content:"FF Passwords"; within:500; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008841; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PWS_Generic; sid:2008841; rev:5;)

#by cjeremy
#ref: 298bd867e7a19a8eaa358f75a550ef5e
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Password Stealer (PSW.Win32.Magania Family) GET"; flow:established,to_server; content:"GET "; depth:4;
uricontent:"pass="; uricontent:"type="; uricontent:"host="; uricontent:"port="; uricontent:"name="; uricontent:"pc="; uricontent:"user="; uricontent:"ip="; uricontent:"version=";
content:"|0d 0a|User-Agent|3a| NR"; classtype:trojan-activity; reference:url,www.f-secure.com/v-descs/trojan-psw_w32_magania.shtml; reference:url,www.threatexpert.com/reports.aspx?
find=Trojan-PWS.Magania; reference:url,doc.emergingthreats.net/2009094; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PWS_Generic; sid:2009094; rev:3;)

#by Matt Jonkman, Pakes.bwp update check
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Pakes User-Agent Detected"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| Mozilla/4.7 [en] (WinNT";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007767; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Pakes; sid:2007767; rev:4;)

#pakes.bwa
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Pakes Update Detected"; flow:established,to_server; uricontent:".php?wm="; nocase; uricontent:"&ucid="; nocase;
uricontent:"&e="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007768; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Pakes;
sid:2007768; rev:3;)

#seeing this pattern from several named trojans, from the sandnet
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Pushdo Update URL Detected"; flow:established,to_server; uricontent:"/40E800"; nocase; uricontent:"C00000"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007771; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Pakes; sid:2007771; rev:8;)

#seeing this pattern from several named trojans, from the sandnet
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Pakes/Cutwail/Kobcka Checkin URL"; flow:established,to_server; uricontent:"/firstrun.php?product="; nocase;
uricontent:"&aff="; nocase; uricontent:"&update="; nocase; content:"|0d 0a|User-Agent|3a| Mozilla|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008152;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Pakes; sid:2008152; rev:4;)

#seeing this pattern from several named trojans, from the sandnet
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Pakes Winifixer.com Related Checkin URL"; flow:established,to_server; content:"POST "; depth:5; uricontent:".php?
affid="; nocase; uricontent:"&uid="; nocase; uricontent:"&tm="; nocase; content:"|0d 0a|User-Agent|3a| Internet Explorer|0d 0a|"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008277; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Pakes; sid:2008277; rev:3;)

#by Pedro Marinho, re d2d5bf2669edce3c71dc16c46e8a67f7
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Pakes/Cutwail/Kobcka Checkin Detected High Ports"; flow:established,to_server; dsize:<160; content:"GET /?
bot_id=0&mode=1"; depth:21; content:"|0d 0a|Host|3a| "; distance:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008358; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Pakes; sid:2008358; rev:4;)

#ref: 399752201bec70afcdac049e698f6c3d
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 897 (msg:"ET TROJAN Backdoor PcClient\/CAK\/Pakes POST on non-http Port"; flow:established,to_server; content:"POST "; depth:5; content:".jsp";
nocase; within:50; pcre:"/\/\d{8,}\/\d{4,}\/\d{4,}\.jsp/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009093; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Pakes; sid:2009093; rev:2;)

#by Marcus at unsober
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Pandex checkin detected"; flow:established,to_server; content:"GET "; depth:4; uricontent:"?m="; uricontent:"&a=";
uricontent:"&os="; content:!"|0d 0a|User-Agent|3a| "; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008433; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Pandex; sid:2008433; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Parite Setup Connection (tqzn.com related)"; flow:established,to_server; uricontent:"/barbindsoft/barsetup.exe?
queryid="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009108; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Parite; sid:2009108;
rev:2;)

#by: Jeremy Conway at sudosecure.net
#ref: 030500a6ef292ecf6fc4e2a5bf5a424c
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET VIRUS Parite.B GET"; flow:established,to_server; content:"GET "; nocase; depth:4; content:"|0d0a|User-Agent|3a|
gomtour|0d0a|"; within:200; classtype:trojan-activity; reference:url,www.pandasecurity.com/homeusers/security-info/18181/information/Parite.B;
reference:url,www.pctools.com/mrc/infections/id/Virus.Parite.B/; reference:url,www.threatexpert.com/threats/w32-parite-b.html; reference:url,doc.emergingthreats.net/2009454;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Parite; sid:2009454; rev:4;)

#Submitted 2006-03-20 by Tom Fischer
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN PassSickle Reporting User Activity"; flow:established,to_server; uricontent:".php?id="; nocase; uricontent:"&data=";
nocase; pcre:"/User-Agent\x3a[^\n]+PassSickle/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2002859; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PassSickle; sid:2002859; rev:4;)

#by Paul Dokas
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Password Stealer - User-Agent (Ucheck)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| ";
content:"Opera/9.10"; distance:0; content:"|3b| Ucheck"; pcre:"/User-Agent\x3a[^\n]+\x3b\sUcheck/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009081;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Password_Stealer; sid:2009081; rev:5;)

#by Paul Dokas
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Password Stealer Reporting - ?a=%NN&b="; flow:to_server,established; content:"POST "; depth:5; nocase;
uricontent:"a=%"; uricontent:"&b="; pcre:"/a=\%[0-9a-fA-F]{2}\&b/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009082; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Password_Stealer; sid:2009082; rev:2;)

#by: Jeremy Conway at sudosecure.net
#ref: a03cadd15d8f658ee73c8829fb4a3019
#Disabling for FPs on baidu ads and others
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32/Pasta Downloader - GET Checkin to Fake GIF"; flow:established,to_server; content:"GET "; depth:4;
uricontent:".gif?"; nocase; uricontent:"t="; nocase; uricontent:"q="; nocase; uricontent:"p="; nocase; uricontent:"pn="; nocase; classtype:trojan-activity;
reference:url,malwarebytes.org/malwarenet.php?name=Trojan.Pasta; reference:url,doc.emergingthreats.net/2009522; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Pasta; sid:2009522; rev:2;)

#by dn1nj4
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Paymilon-A HTTP POST"; flow:established,to_server; content:"POST http|3a|//"; depth:12; content:"C|3a|\\";
distance:0; nocase; content:".exe|00 00|"; distance:0; classtype:trojan-activity; reference:url,www.sophos.com/security/analyses/viruses-and-spyware/malpaymilona.html;
reference:url,doc.emergingthreats.net/2010918; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Paymilion; sid:2010918; rev:4;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1900 (msg:"ET TROJAN Backdoor.Win32/PcClient.ZL Checkin"; flow:established,to_server; content:"|00 00 00 10 c8 00 00 00 b0 ff|"; depth:10;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008920; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PcClient; sid:2008920; rev:2;)

#Matt Jonkman, re 0c7918e9c9f3bae79bb8ff1b4b3f9b42
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN PcClient Backdoor Checkin Packet 1"; flow:established,to_server; dsize:4; content:"|82 87 99 45|";
flowbits:set,ET.PcClient; flowbits:noalert; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009238; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PcClient; sid:2009238; rev:2;)

#Matt Jonkman, re 0c7918e9c9f3bae79bb8ff1b4b3f9b42
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN PcClient Backdoor Checkin"; flowbits:isset,ET.PcClient; flow:established,to_server; dsize:248; content:"|52 0d 12
12|"; depth:4; flowbits:noalert; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009239; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PcClient; sid:2009239; rev:2;)

#by Daniel Clemens
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN PECompact2 Packed Binary - Likely Hostile"; flow:from_server,established; content:"|74 65 78 74|"; content:"|50 45 43 32|";
within:40; classtype:trojan-activity; reference:url,www.bitsum.com/pecompact.shtml; reference:url,bits.packetninjas.org/eblog/?p=306; reference:url,doc.emergingthreats.net/2008547;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PeCompact2; sid:2008547; rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Perfect Keylogger FTP Initial Install Log Upload"; flow:established,to_server; content:"Congratulations! Perfect Kelogger
was successfully installed"; depth:63; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007973; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Perfect_Keylogger; sid:2007973; rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN Perfect Keylogger Install Email Report"; flow:established,to_server; content:"Subject|3a| Perfect Keylogger was installed
successfully|3a|"; content:"Perfect Keylogger was installed on the computer "; distance:50; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008893;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Perfect_Keylogger; sid:2008893; rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Perfect Keylogger FTP Log Upload"; flow:established,to_server; content:"Log upload date|3a| "; depth:17; content:"|0d
0a|Time|3a| "; within:40; content:"To view DAT files, please do the following steps|3a|"; distance:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007974;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Perfect_Keylogger; sid:2007974; rev:4;)

#by Jeremy of sudosecure
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Perfect Keylogger FTP Initial Install Log Upload (Null obfuscated)"; flow:established,to_server;
content:"C|00|o|00|n|00|g|00|r|00|a|00|t|00|u|00|l|00|a|00|t|00|i|00|o|00|n|00|s|00|!|00| |00|P|00|e|00|r|00|f|00|e|00|c|00|t|00| |00|K|00|e|00|l|00|o|00|g|00|g|00|e|00|r|00|
|00|w|00|a|00|s|00| |00|s|00|u|00|c|00|c|00|e|00|s|00|s|00|f|00|u|00|l|00|l|00|y|00| |00|i|00|n|00|s|00|t|00|a|00|l|00|l|00|e|00|d|00|"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008327; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Perfect_Keylogger; sid:2008327; rev:2;)

#by Chris Green
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Personal Defender 2009 - prinimalka.py"; flow:established,to_server; uricontent:"/prinimalka.py"; classtype:trojan-
activity; reference:url,malwarebytes.besttechie.net/2008/11/03/removal-instructions-for-personal-defender-2009/; reference:url,doc.emergingthreats.net/2009405;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Personal_Defender; sid:2009405; rev:2;)

#by Chris Green
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Personal Defender 2009 - trash.py"; flow:established,to_server; uricontent:"/trash.py"; classtype:trojan-activity;
reference:url,malwarebytes.besttechie.net/2008/11/03/removal-instructions-for-personal-defender-2009/; reference:url,doc.emergingthreats.net/2009406;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Personal_Defender; sid:2009406; rev:2;)

#by matt jonkman
#win32.philis.J here
#
alert icmp any any -> any any (msg:"ET TROJAN Philis.J ICMP Sweep (Payload Hello,World)"; icode:0; itype:0; dsize:11; content:"Hello,World"; classtype:trojan-activity;
reference:url,vil.nai.com/vil/content/v_141203.htm; reference:url,doc.emergingthreats.net/2008017; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Philis;
sid:2008017; rev:3;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Phoenix Exploit Kit Facebook phishing page payload could be ZeuS"; flow:established,to_server; content:"GET ";
nocase; depth:4; uricontent:"/LoginFacebook.php"; pcre:"/\/[a-z]{2}[0-9]{3}[a-z]{2}\/LoginFacebook\.php$/U"; classtype:trojan-activity;
reference:url,malwareint.blogspot.com/2010/03/new-phishing-campaign-against-facebook.html; reference:url,doc.emergingthreats.net/2011121; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Phoenix; sid:2011121; rev:2;)

#2010-07-09 By Eoin Miller
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Phoenix Exploit Kit - pdfopen.pdf"; flow:established,to_server; uricontent:"pdfopen.pdf"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2011180; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Phoenix; sid:2011180; rev:1;)
```

```
#2010-07-09 By Eoin Miller
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Phoenix Exploit Kit - pdfswf.pdf"; flow:established,to_server; uricontent:"pdfswf.pdf"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2011181; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Phoenix; sid:2011181; rev:1;)

#2010-07-09 By Eoin Miller
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Phoenix Exploit Kit - libtiff.pdf"; flow:established,to_server; uricontent:"libtiff.pdf"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2011182; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Phoenix; sid:2011182; rev:1;)

#2010-07-09 By Eoin Miller
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Phoenix Exploit Kit malware payload download"; flow:established,to_server; uricontent:".php?deserialize=";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011183; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Phoenix; sid:2011183; rev:1;)

#2010-07-09 By Eoin Miller
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Phoenix Exploit Kit VBscript download"; flow:established,to_client; content:"Createobject(StrReverse("; nocase;
content:"|22|tcejbOmetsySeliF.gnitpircS|22|))"; nocase; distance:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011184; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Phoenix; sid:2011184; rev:2;)

#by Philipp Bescht, updates by Darren Spruel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Piptea.a Related Trojan Checkin (1)"; flow:established,to_server; uricontent:"/cd/cd.php?id="; uricontent:"&ver=";
pcre:"/\/cd\/cd\.php.id=[A-F0-9\-]+&ver=/U"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008382; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Piptea; sid:2008382; rev:4;)

#by Philipp Bescht, updates by Darren Spruel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Piptea.a Related Trojan Checkin (2)"; flow:established,to_server; uricontent:"/cd/un2.php?id="; uricontent:"&ver=";
pcre:"/\/cd\/un2\.php.id=[A-F0-9\-]+&ver=/U"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008383; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Piptea; sid:2008383; rev:4;)

#by Philipp Bescht, updates by Darren Spruel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Piptea.a Related Trojan Checkin (3)"; flow:established,to_server; uricontent:"/cd/un.php?id="; uricontent:"&ver=";
pcre:"/\/cd\/un\.php.id=[A-F0-9\-]+&ver=/U"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008384; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Piptea; sid:2008384; rev:4;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN PlayMP3z.biz Related Spyware/Trojan Install Report"; flow:established,to_server; uricontent:"?
stage=setup&application="; uricontent:"&campaign="; uricontent:"&code="; uricontent:"&version="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008626;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Playmp3z; sid:2008626; rev:2;)

#Sandnet analysis
#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Poebot Related User Agent (SPM_ID=)"; flow:established,to_server; content:"User-Agent|3a| SPM_ID="; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/2006391; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Poebot; sid:2006391; rev:4;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Pointfree.co.kr Trojan/Spyware Infection Checkin"; flow:established,to_server; uricontent:"log.php?mac=";
content:"&hdd="; uricontent:"&ver="; uricontent:"&ie="; uricontent:"&win="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008972;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Pointfree.co.kr; sid:2008972; rev:2;)

#by matt Jonkman, no AV coverage yet
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Pointpack.kr Related Trojan Checkin"; flow:established,to_server; uricontent:"php?"; uricontent:"kind=";
uricontent:"&pid="; uricontent:"&ver="; uricontent:"&uniq="; uricontent:"&addresses="; uricontent:"&hdmacid="; uricontent:"&dllver="; uricontent:"&subv="; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008260; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Pointpack.kr; sid:2008260; rev:3;)

#by Matt Jonkman, Analsis by Michael Hale Ligh
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 3460 (msg:"ET TROJAN Poison Ivy Key Exchange with CnC Init"; flow:established,to_server; dsize:256; flowbits:set,ET.Poison1; flowbits:noalert;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008380; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PoisonIvy; sid:2008380; rev:2;)

#by Matt Jonkman, Analsis by Michael Hale Ligh
#
alert tcp $EXTERNAL_NET 3460 -> $HOME_NET any (msg:"ET TROJAN Poison Ivy Key Exchange with CnC Response"; flow:established,from_server; dsize:256; flowbits:isset,ET.Poison1;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008381; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PoisonIvy; sid:2008381; rev:2;)

#by: Jeremy Conway at sudosecure.net
#ref: b853a0bc503b0e35959601cca79ec809
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Poisionivy RAT/Backdoor follow on POST Data PUSH Packet"; flow:established,to_server; flags:AP,12; content:"op=";
depth:3; nocase; content:"&servidor="; nocase; content:"&senha="; nocase; content:"&usuario="; nocase; content:"&base="; nocase; content:"&sgdb="; nocase; classtype:trojan-activity;
reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Backdoor%3AWin32%2FPoisonivy.I&ThreatID=-2147363597;
reference:url,www.viruslist.com/en/viruses/encyclopedia?virusid=133781; reference:url,doc.emergingthreats.net/2009806; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PoisonIvy; sid:2009806; rev:2;)

#by anonymous submitter #2
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN Chorns/Poison Ivy related Backdoor Initial Connection"; flow:established; dsize:12; content:"/FIRSTINF/|0d0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010344; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PoisonIvy; sid:2010344; rev:3;)

#by anonymous submitter #2
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN Chorns/Poison Ivy related Backdoor Keep Alive"; flow:established; dsize:12; content:"/AVAILABL/|0d0a|"; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/2010345; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PoisonIvy; sid:2010345; rev:3;)

#by Jaime Blasco, updates by evilghost
#these sigs are intended to catch post data to images. This is suspicious and often trojan or spyware
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Data POST to an image file (gif)"; flow:established,to_server; content:"POST "; depth:5; uricontent:".gif"; nocase;
content:".gif HTTP"; nocase; classtype:trojan-activity; pcre:"/POST\x20.*\/.+\.gif\x20HTTP\/1\.[0-1]$/i"; reference:url,doc.emergingthreats.net/2010066;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Post_to_image; sid:2010066; rev:3;)

#by Jaime Blasco, updates by evilghost
#these sigs are intended to catch post data to images. This is suspicious and often trojan or spyware
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Data POST to an image file (jpg)"; flow:established,to_server; content:"POST "; depth:5; uricontent:".jpg"; nocase;
content:".jpg HTTP"; nocase; classtype:trojan-activity; pcre:"/POST\x20.*\/.+\.jpg\x20HTTP\/1\.[0-1]$/i"; reference:url,doc.emergingthreats.net/2010067;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Post_to_image; sid:2010067; rev:3;)

#by Jaime Blasco, updates by evilghost
#these sigs are intended to catch post data to images. This is suspicious and often trojan or spyware
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Data POST to an image file (jpeg)"; flow:established,to_server; content:"POST "; depth:5; uricontent:".jpeg";
nocase; content:".jpeg HTTP"; nocase; classtype:trojan-activity; pcre:"/POST\x20.*\/.+\.jpeg\x20HTTP\/1\.[0-1]$/i"; reference:url,doc.emergingthreats.net/2010068;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Post_to_image; sid:2010068; rev:3;)

#by Jaime Blasco, updates by evilghost
#these sigs are intended to catch post data to images. This is suspicious and often trojan or spyware
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Data POST to an image file (bmp)"; flow:established,to_server; content:"POST "; depth:5; uricontent:".bmp"; nocase;
```

```
content:".bmp HTTP"; nocase; classtype:trojan-activity; pcre:"/POST\x20.*\/.+\.bmp\x20HTTP\/1\.[0-1]$/i"; reference:url,doc.emergingthreats.net/2010069;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Post_to_image; sid:2010069; rev:3;)

#by Jaime Blasco, updates by evilghost
#these sigs are intended to catch post data to images. This is suspicious and often trojan or spyware
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Data POST to an image file (png)"; flow:established,to_server; content:"POST "; depth:5; uricontent:".png"; nocase;
content:".png HTTP"; nocase; classtype:trojan-activity; pcre:"/POST\x20.*\/.+\.png\x20HTTP\/1\.[0-1]$/i"; reference:url,doc.emergingthreats.net/2010070;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Post_to_image; sid:2010070; rev:3;)

#Submitted by Brad Doctor
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET VIRUS Greeting card gif.exe email incoming SMTP"; flow: established,to_server; content:"postcard.gif.exe"; nocase; classtype:
trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/vbs.postcard@mm.html; reference:url,doc.emergingthreats.net/2001919;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Postcard; sid:2001919; rev:5;)

#Submitted by Brad Doctor
#
alert tcp $EXTERNAL_NET 110:220 -> $HOME_NET any (msg:"ET VIRUS Greeting card gif.exe email incoming POP3/IMAP"; flow: established,from_server; content:"postcard.gif.exe"; nocase;
classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/vbs.postcard@mm.html; reference:url,doc.emergingthreats.net/2001920;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Postcard; sid:2001920; rev:5;)

#Submitted by Brad Doctor
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET VIRUS Greeting card gif.exe email incoming HTTP"; flow: established,from_server; content:"postcard.gif.exe"; nocase;
classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/vbs.postcard@mm.html; reference:url,doc.emergingthreats.net/2001921;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Postcard; sid:2001921; rev:5;)

#Created by Jeremy Conway with contributions from Steven Adair
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN TROJ_PROX.AFV POST"; flow:to_server,established; content:"POST "; nocase; depth:5; uricontent:".php"; nocase;
content:"=|22|sid|22|"; nocase; content:"=|22|up|22|"; nocase; content:"=|22|wbfl|22|"; nocase; content:"=|22|v|22|"; nocase; content:"=|22|ping|22|"; nocase; content:"=|22|guid|22|";
nocase; classtype:trojan-activity; reference:url,trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ%5FPROXY%2EAFV&VSect=T; reference:url,doc.emergingthreats.net/2007728;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Prox; sid:2007728; rev:4;)

#by Scott Melnick, re 9376323d9f8a59f253c3800fcb355575
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Proxy.Win32.Agent.mx"; flow:established,to_server; uricontent:"q.php"; nocase; uricontent:"&m="; nocase;
uricontent:"&a="; nocase; uricontent:"&x="; nocase; uricontent:"&i="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006405;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Proxy.Win32.Agent.MX; sid:2006405; rev:2;)

#by Scott Melnick, re 9376323d9f8a59f253c3800fcb355575
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Proxy.Win32.Agent.mx (2)"; flow:established,to_server; uricontent:"q.php"; nocase; uricontent:"&p="; nocase;
uricontent:"&x="; nocase; uricontent:"&i="; nocase; uricontent:"&t="; nocase; uricontent:"&o="; nocase; uricontent:"&v="; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2006406; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Proxy.Win32.Agent.MX; sid:2006406; rev:3;)

#by William Salusky of AOL
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN ProxyBot Phone Home Traffic"; flow:established,to_server; uricontent:"ind.php?p="; uricontent:"&uid=";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008244; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Proxybot; sid:2008244; rev:3;)

#by Josh Smith
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Pushdo Checkin"; flow:established,to_server; content:"GET "; depth:4; uricontent:"m="; uricontent:"&a=";
uricontent:"&os="; pcre:"/&os=[a-f0-9]{50}/U"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008493; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Pushdo; sid:2008493; rev:3;)

#Matt Jonkman
#from sandnet analysis, looking for User Agents like bL0j3jKdUwy3kUCZnsqaHlFTNEU4Ik8IhfG5kpu1Up9qFuqAtSnmqDYUHgAWPsjf1soqBMqxqts1OkiavJn05uGl38NIw4lPZHKHvO36WFcSNu81CJx
#
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN QQPass Related User-Agent Infection Checkin (App4)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
App"; content:!"Host|3a| liveupdate.symanteclive update.com|0d 0a|"; pcre:"/User-Agent\: App\d+/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007569;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_QQHelper; sid:2007569; rev:8;)

#by Marcus at unsober.org
#re: 1c3ead1c4a033b6af8f29e53fedd96c1
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Qhosts Trojan Check-in"; flow:established,to_server; content:"POST "; depth:5; uricontent:".php"; content:"UserID=";
content:"&wv="; content:"&res="; content:"&lng="; classtype:trojan-activity; reference:url,www.symantec.com/security_response/writeup.jsp?docid=2003-100116-5901-99;
reference:url,doc.emergingthreats.net/2009517; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Qhosts; sid:2009517; rev:2;)

#by Daniel Clemens
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN RLPacked Binary - Likely Hostile"; flow:from_server,established; content:"|2E 70 61 63 6B 65 64|"; content:"|2E 52 4C 50 61
63 6B|"; within:50; classtype:trojan-activity; reference:url,rlpack.jezgra.net; reference:url,www.teamfurry.com/wordpress/2007/04/01/unpacking-rlpack/;
reference:url,doc.emergingthreats.net/2008285; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_RLPacked; sid:2008285; rev:2;)

#by Don Jackson of Secureworks
#
alert tcp any any -> any any (msg:"ET TROJAN Generic Raider Obfuscated VBScript"; flow:established; content:"execute"; content:"|22 22 22 22 22 3A|"; offset:8; content:"function";
nocase; pcre:"/\x22\x3A(\w)\x3D\x22execute\s+\x22{5}\x3A.*\x3Aexecute\s*\x28\s*\1\s*\x29\x3Aend\s+function\x3A/s"; classtype:trojan-activity; reference:url,bbs.duba.net/viewthread.php?
tid=21892104&page=1&extra=page=1; reference:url,doc.emergingthreats.net/2008278; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Raider_Obfuscated_VBS;
sid:2008278; rev:3;)

#by Myron Davis
#
alert udp $HOME_NET any -> $EXTERNAL_NET 20192 (msg:"ET TROJAN Ransky or variant backdoor communication ping"; dsize:<6; classtype:trojan-activity;
reference:url,www.sophos.com/virusinfo/analyses/trojranckcx.html; reference:url,doc.emergingthreats.net/2002728; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Ransky; sid:2002728; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Rcash.co.kr Bootup Checkin via HTTP"; flow:established,to_server; uricontent:"/install/Boot.asp?macaddr="; nocase;
uricontent:"&partner="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007807; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Rcash; sid:2007807; rev:2;)

#by marcus at unsober
#ref: fc6926b25b1df52729f7e206b461e8ef
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN RegHelper Installation"; flow:established,to_server; content:"GET "; depth:4; uricontent:"start=";
uricontent:"&Edition="; uricontent:"&RHRTVersion="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008376; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Reghelper; sid:2008376; rev:2;)

#by Marcus at unsober.org
#ref: c89eec06daf6ceb4ee1cdcd485db9916
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 21 (msg:"ET TROJAN Trojan.Win32.Regrun.ro FTP connection detected"; flow:established,to_server; content:"RETR k3ylogger.txt|0d 0a|"; depth:21;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008733; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Regrun; sid:2008733; rev:2;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Renos/ssd.com HTTP Checkin"; flow:established,to_server; uricontent:"/dlp.php?"; nocase; uricontent:"&m="; nocase;
uricontent:"&ydf="; nocase; uricontent:"&e="; nocase; uricontent:"&w=___"; nocase; uricontent:"&t="; nocase; uricontent:"&apzx="; nocase; uricontent:"&apz="; nocase; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/2007834; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Renos; sid:2007834; rev:2;)
```

```
#by Don Jackson of Secureworks. RE: US courts related phishes
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN RhiFrem Trojan Activity - cmd"; flow:to_server,established; content:"GET|20|"; offset:0; depth:4; uricontent:"?
mod=cmd&user="; content:"User|2D|Agent|3A| Mozilla/5.0 Gecko/20050212 Firefox/1.5.0.2"; pcre:"/^GET\x20[^\x0D\x0A]+\x3Fmod\x3Dcmd\x26user\x3D\w+
[^\x0D\x0A]*\x20HTTP\x2F1\x2E0\x0D\x0A.*\x0D\x0AHost\x3A\x20\w+/"; classtype:trojan-activity; reference:url,www.castlecops.com/U_S_Courts_phish792683.html;
reference:url,doc.emergingthreats.net/2008139; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Rhifrem; sid:2008139; rev:5;)

#by Don Jackson of Secureworks. RE: US courts related phishes
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN RhiFrem Trojan Activity - log"; flow:to_server,established; content:"POST|20|"; offset:0; depth:5; uricontent:"?
mod=log&user="; content:"User-Agent|3A| Mozilla/5.0 Gecko/20050212 Firefox/1.5.0.2"; pcre:"/^POST\x20[^\x0D\x0A]+\x3Fmod\x3Dlog\x26user\x3D\w+
[^\x0D\x0A]*\x20HTTP\x2F1\x2E0\x0D\x0A.*\x0D\x0AHost\x3A\x20\w+.*\x0D\x0A\x0D\x0Acurr\x3D.*\x26next\x3D/"; classtype:trojan-activity;
reference:url,www.castlecops.com/U_S_Courts_phish792683.html; reference:url,doc.emergingthreats.net/2008140; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Rhifrem; sid:2008140; rev:4;)

#by: Jeremy Conway at sudosecure.net
#ref: 14d98e50d25dfc3c1bc011c2856ac1a8
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Runner (Often Rootkit) - POST"; flow:established,to_server; content:"POST "; depth:5; content:"G="; nocase;
content:"&PG="; nocase; content:"&EPBB="; nocase; content:!"|0d0a|User-Agent|3a|"; classtype:trojan-activity; reference:url,www.spywarecease.com/spyware-
list/Spyware_Trojan.Win32.Runner.s.html; reference:url,www.threatexpert.com/threats/trojan-win32-runner.html; reference:url,doc.emergingthreats.net/2009711;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Runner; sid:2009711; rev:3;)

#by Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN SafeFighter Fake Scanner Installation in Progress"; flow:established,to_server; uricontent:"/safefighter.php";
nocase; content:"User-Agent|3a| NSIS"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2010065; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Safefighter; sid:2010065; rev:3;)

#by: Jeremy Conway at sudosecure.net
#ref: 7a70056ce64d1f4990e19633615b7ae1
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Sality - Fake Opera User-Agent"; flow:established,to_server; content:"GET "; depth:5; content:"|0d0a|User-Agent|3a|
Opera/8.81 (Windows NT 6.0|3b| U|3b| en)|0d0a|"; classtype:trojan-activity; reference:url,www.spywareremove.com/removeTrojanDownloaderSalityG.html;
reference:url,www.microsoft.com/security/portal/beta/Threat/Encyclopedia/Entry.aspx?Name=Virus%3AWin32%2FSality.AM; reference:url,doc.emergingthreats.net/2009525;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Sality; sid:2009525; rev:3;)

#by: Jeremy Conway at sudosecure.net
#ref: 02dbe5d487220e87b317474ca1f6d2cf
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Sality - Fake Opera User-Agent (Opera/8.89)"; flow:established,to_server; content:"GET "; depth:5;
content:"|0d0a|User-Agent|3a| Opera/8.89 (Windows NT 6.0|3b| U|3b| en)|0d0a|"; classtype:trojan-activity; reference:url,www.spywareremove.com/removeTrojanDownloaderSalityG.html;
reference:url,www.microsoft.com/security/portal/beta/Threat/Encyclopedia/Entry.aspx?Name=Virus%3AWin32%2FSality.AM; reference:url,doc.emergingthreats.net/2009530;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Sality; sid:2009530; rev:3;)

#Matt Jonkman
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET VIRUS Sality Trojan Web Update"; flow:to_server,established; uricontent:"/new_array2.php?speed="; nocase;
classtype:trojan-activity; reference:url,www.sophos.com/security/analyses/w32salityu.html; reference:url,doc.emergingthreats.net/2003424; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/VIRUS_Sality; sid:2003424; rev:3;)

#from castlecops research, http://www.castlecops.com, sig by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET VIRUS Sality Virus User Agent Detected (KUKU)"; flow:established,to_server; content:"User-Agent|3a| KUKU"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003636; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/VIRUS_Sality; sid:2003636; rev:6;)

#from the bleeding sandnet
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET VIRUS Sality Virus User Agent Detected (SPM_ID=)"; flow:established,to_server; content:"User-Agent|3a| SPM_ID="; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003651; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/VIRUS_Sality; sid:2003651; rev:5;)

#by: Jeremy Conway at sudosecure.net
#ref: f340e9fdf3073bffab640a37d0fb7d2e
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Sality - Fake Opera User-Agent"; flow:established,to_server; content:"GET "; depth:5; content:"|0d0a|User-Agent|3a|
Opera/9.28 (Windows NT 6.0|3b| U|3b| en)|0d0a|"; classtype:trojan-activity; reference:url,www.spywareremove.com/removeTrojanDownloaderSalityG.html;
reference:url,www.microsoft.com/security/portal/beta/Threat/Encyclopedia/Entry.aspx?Name=Virus%3AWin32%2FSality.AM; reference:url,doc.emergingthreats.net/2009474;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/VIRUS_Sality; sid:2009474; rev:3;)

#by Kevin Ross
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Sasfis Botnet Client Reporting Back to Controller After Command Execution"; flow:established,to_server;
uricontent:"/loader/bb.php"; nocase; uricontent:"id="; nocase; content:"v="; nocase; content:"tm="; nocase; uricontent:"tid="; nocase; uricontent:"r="; nocase; classtype:trojan-
activity; reference:url,www.fortiguard.com/analysis/sasfisanalysis.html; reference:url,doc.emergingthreats.net/2010756; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Sasfis; sid:2010756; rev:2;)

#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 8080 (msg:"ET TROJAN Saturn Proxy Initial Outbound Checkin (404.txt)"; flow:established,to_server; dsize:<50; content:"GET /404.txt HTTP/1.0";
depth:21; classtype:trojan-activity; flowbits:set,ET.saturn.checkin; reference:url,doc.emergingthreats.net/2007751; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Saturn_Proxy; sid:2007751; rev:3;)

#by Matt Jonkman
#
alert tcp $EXTERNAL_NET 8080 -> $HOME_NET any (msg:"ET TROJAN Saturn Proxy Checkin Response"; flow:established,from_server; flowbits:isset,ET.saturn.checkin; content:"HTTP/1.0 200 OK|0d
0a|Encryption|3a| on|0d 0a|"; offset:0; depth:33; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007752; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Saturn_Proxy; sid:2007752; rev:4;)

#this is a C&C, may or may not be unique to each variant, need to learn more about it...
#by Matt Jonkman
#
alert tcp $EXTERNAL_NET 443 -> $HOME_NET any (msg:"ET TROJAN Saturn Proxy C&C Activity"; flow:established,from_server; dsize:12; content:"|2d 00 00 00|"; offset:0; depth:4; content:"|00
00 55 00 00 00|"; distance:2; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007753; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Saturn_Proxy; sid:2007753; rev:3;)

#by darren spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN W32/Scar Downloader Request"; flow:established,to_server; uricontent:"/tasksz.php?load="; nocase; uricontent:"&id=";
nocase; pcre:"/tasksz\.php\?load=[0-9a-f]{32}&id=\d+$/U"; classtype:trojan-activity; reference:url,www.f-secure.com/v-descs/trojan_w32_scar_a.shtml;
reference:url,doc.emergingthreats.net/2010288; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Scar; sid:2010288; rev:2;)

#by matt jonkman
#kaspersky calls is win32.shark.hz. This sig will catch the report email outbound
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN Shark Pass Stealer Email Report"; flow:established,to_server; content:"|0d 0a|Subject|3a| Codesoft PW Stealer "; content:"|0d
0a 0d 0a|Codesoft PW Stealer File "; distance:0; content:"filename=|22|"; distance:0; content:".log|22 0d 0a|"; distance:0; within:20; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2007992; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Shark; sid:2007992; rev:3;)

#by Tom Fisher
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN SickleBot Reporting User Activity"; flow:established,to_server; content:"GET "; depth:4; uricontent:"id="; nocase;
content:"|0d 0a|User-Agent|3a| SickleBot"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2002776; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Sicklebot; sid:2002776; rev:5;)

#by Darren Spruell
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Silentbanker/Yaludle Checkin to C&C"; flow:to_server,established; content:"GET "; depth:4; uricontent:".php?id=";
nocase; content:"&c="; nocase; content:"&v="; nocase; content:"&b="; nocase; content:"&z="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009542;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Silentbanker; sid:2009542; rev:2;)

#by pedro marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN W32.SillyFDC Checkin"; flow:established,to_server; content:"GET "; depth:4; uricontent:".php"; nocase;
uricontent:"getowner=1&uniqueid="; content:"|0d 0a|User-Agent|3a| WinHttp.WinHttpRequest"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010268;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Silly; sid:2010268; rev:3;)

#by darren spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Silon Encrypted Data POST to C&C"; flow:established,to_server; uricontent:".php?i="; nocase; uricontent:"&k=";
nocase; pcre:"/\.php\?i=\w+_[0-9A-F]{8}&k=\d+$/Ui"; classtype:trojan-activity; reference:url,www.trusteer.com/webform/w32silon-malware-analysis;
reference:url,doc.emergingthreats.net/2010201; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Silon; sid:2010201; rev:2;)

#by Jeffrey Brown
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Sinowal/Mebroot Client POST"; flow:to_server,established; content:"POST "; depth:5; content:"|0d 0a|Connection|3a|
close|0d 0a 0d 0a a9 3a d4 31 4b 84|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008520; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Sinowal; sid:2008520; rev:3;)

#by Pedro Marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Trojan Sinowal Phoning Home"; flow:established,to_server; content:"GET "; depth:4; uricontent:"/ld/"; nocase;
uricontent:".php"; nocase; uricontent:"id="; uricontent:"&n="; uricontent:"&try="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008580;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Sinowal; sid:2008580; rev:2;)

#by Marcus at unsober.org
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Small.zon checkin"; flow:established,to_server; content:"GET "; depth:4; uricontent:"?n="; uricontent:"&id=";
uricontent:"&t="; uricontent:"&i="; pcre:"/\?n=\d+&id=.+&t=.+&i=\d+/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009300;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Small.zon; sid:2009300; rev:2;)

#y Tom Fischer
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Snatch Reporting User Activity"; flow:established,to_server; uricontent:"/snatch/module"; content:"|0d 0a|User-
Agent|3a 20|Snatch-System"; depth:512; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003515; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Snatch; sid:2003515; rev:4;)

#data from nalbright
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Social-bos.biz related trojan checkin (trackid=hex)"; flow:established,to_server; uricontent:".php?trackid=";
uricontent:"706172616D3D636D64266C616E673D"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008545; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Social-bos.biz; sid:2008545; rev:2;)

#matt Jonkman, Win32.Socks.n
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN 3alupKo/Win32.Socks.n Related Checkin URL"; flow:established,to_server; uricontent:".php?"; uricontent:"&v=";
uricontent:"&s="; uricontent:"&cip="; uricontent:"&lid="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008280; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Socks; sid:2008280; rev:3;)

#matt Jonkman, Win32.Socks.n
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN 3alupKo/Win32.Socks.n Related Checkin URL (2)"; flow:established,to_server; uricontent:"/?&v="; uricontent:"&s=";
uricontent:"&cip="; uricontent:"&lid="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008393; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Socks; sid:2008393; rev:2;)

#matt Jonkman, Win32.Socks.n
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN 3alupKo/Win32.Socks.n Related Checkin URL (3)"; flow:established,to_server; uricontent:"&ns="; uricontent:"&id=";
content:"|0d 0a|User-Agent|3a| Mozilla|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008395; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Socks; sid:2008395; rev:3;)

#Marcus at unsober
#re: 7596ec9308082edec613ac8d78ee4fe6
#updates by darren spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Zalupko/Koceg/Mandaph manda.php Checkin"; flow:established,to_server; uricontent:"/manda.php?"; nocase;
uricontent:"ns="; nocase; uricontent:"&id="; nocase; classtype:trojan-activity; reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?
name=Backdoor%3aWin32%2fKoceg.gen!B; reference:url,www.symantec.com/security_response/writeup.jsp?docid=2008-042816-0445-99&tabid=2; reference:url,www.threatexpert.com/report.aspx?
md5=b2aad8e259cbfdd2ba1fcbf22bcee2e9; reference:url,doc.emergingthreats.net/2008324; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Socks; sid:2008324;
rev:5;)

#Marcus at unsober
#re: 7596ec9308082edec613ac8d78ee4fe6
#updates by darren spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Zalupko/Koceg/Mandaph HTTP Checkin (2)"; flow:established,to_server; uricontent:"/manda.php?"; uricontent:"id=";
nocase; uricontent:"&v="; nocase; pcre:"/\/manda\.php\?id=(-)?\d{10}&v=[\w\.]+/U"; classtype:trojan-activity;
reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?name=Backdoor%3aWin32%2fKoceg.gen!B; reference:url,www.symantec.com/security_response/writeup.jsp?
docid=2008-042816-0445-99&tabid=2; reference:url,www.threatexpert.com/report.aspx?md5=b2aad8e259cbfdd2ba1fcbf22bcee2e9; reference:url,doc.emergingthreats.net/2010765;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Socks; sid:2010765; rev:2;)

#This is a new type of proxying via port 80. Tha agent opens up a conn to the controller, then repeats whatever the controller tells it to do
#the initial 2 packets seem to be a checkin, then a command of the host and port to connect to.
#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Socks666 Connection Initial Packet"; flow:established,to_server; dsize:24; content:"|9a 02 06 00|"; offset:0;
depth:4; flowbits:set,BS.BPcheckin; flowbits:noalert; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006396; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Socks666; sid:2006395; rev:5;)

#This is a new type of proxying via port 80. Tha agent opens up a conn to the controller, then repeats whatever the controller tells it to do
#the initial 2 packets seem to be a checkin, then a command of the host and port to connect to.
#by Matt Jonkman
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Socks666 Connect Command Packet"; flowbits:isset,BS.BPcheckin; flow:established,from_server; dsize:10; content:"|9a
02 07 00|"; offset:0; depth:4; flowbits:set,BS.BPset; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006396; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Socks666; sid:2006396; rev:5;)

#This is a new type of proxying via port 80. Tha agent opens up a conn to the controller, then repeats whatever the controller tells it to do
#the initial 2 packets seem to be a checkin, then a command of the host and port to connect to.
#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Socks666 Successful Connect Packet Packet"; flowbits:isset,BS.BPset; flow:established,to_server; dsize:16;
content:"|9a 02 08 00|"; offset:0; depth:4; flowbits:set,BS.BPcheckin; tag:session,300,seconds; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006396;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Socks666; sid:2006397; rev:6;)

#Caught a checkin, this should find it
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Socks666 Checkin Packet"; flow:established,to_server; dsize:30; content:"|9a 02 01 00|"; offset:0; depth:4;
flowbits:set,BS.BPcheckin1; flowbits:noalert; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006396; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Socks666; sid:2006398; rev:6;)

#Caught a checkin, this should find it
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Socks666 Checkin Success Packet"; flowbits:isset,BS.BPcheckin1; flow:established,from_server; dsize:4; content:"|9a
02 05 00|"; offset:0; depth:4; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006396; reference:url,www.emergingthreats.net/cgi-
```

```
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Socks666; sid:2006399; rev:5;)

#by matt jonkman. Softcash.org fake.googlebar related checkin
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Fake.Googlebar or Softcash.org Related Post-Infection Checkin"; flow:established,to_server; uricontent:"bl=";
uricontent:"&cuid="; uricontent:"&cnid="; uricontent:"&luid="; uricontent:"&rnd="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008236;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Softcash.org; sid:2008236; rev:2;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Sohanad Checkin via HTTP"; flow:established,to_server; content:"GET "; depth:4; uricontent:"/cs/bux/check.php";
content:!"|0d 0a|User-Agent|3a| "; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007898; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Sohanad; sid:2007898; rev:3;)

#by Joe Stewart of Lurhq/Secureworks
#
alert tcp any any -> any any (msg:"ET TROJAN SpamThru trojan peer exchange"; flow:established,to_server; content:"|01|hs5p|0000|"; depth:7; classtype:trojan-activity;
reference:url,www.secureworks.com/analysis/spamthru/; reference:url,doc.emergingthreats.net/2003138; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_SpamThru;
sid:2003138; rev:3;)

#by Joe Stewart of Lurhq/Secureworks
#
alert tcp any 25 -> any any (msg:"ET TROJAN SpamThru trojan SMTP test successful"; flow:established,to_client; dsize:6; content:"XSMTPX"; classtype:trojan-activity;
reference:url,www.secureworks.com/analysis/spamthru/; reference:url,doc.emergingthreats.net/2003139; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_SpamThru;
sid:2003139; rev:3;)

#by Joe Stewart of Lurhq/Secureworks
#
alert tcp any any -> any any (msg:"ET TROJAN SpamThru trojan update request"; flow:established,to_server; content:"|01|hs5p|0001|"; depth:7; classtype:trojan-activity;
reference:url,www.secureworks.com/analysis/spamthru/; reference:url,doc.emergingthreats.net/2003140; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_SpamThru;
sid:2003140; rev:3;)

#by Joe Stewart of Lurhq/Secureworks
#
alert tcp any any -> any any (msg:"ET TROJAN SpamThru trojan AV DLL request"; flow:established,to_server; content:"|01|hs5p|0007|"; depth:7; classtype:trojan-activity;
reference:url,www.secureworks.com/analysis/spamthru/; reference:url,doc.emergingthreats.net/2003141; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_SpamThru;
sid:2003141; rev:3;)

#by Joe Stewart of Lurhq/Secureworks
#
alert tcp any any -> any any (msg:"ET TROJAN SpamThru trojan spam template request"; flow:established,to_server; content:"|01|hs5p|0004|"; depth:7; classtype:trojan-activity;
reference:url,www.secureworks.com/analysis/spamthru/; reference:url,doc.emergingthreats.net/2003142; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_SpamThru;
sid:2003142; rev:3;)

#by Joe Stewart of Lurhq/Secureworks
#
alert tcp any any -> any any (msg:"ET TROJAN SpamThru trojan spam run report"; flow:established,to_server; content:"|01|hs5p|0005|"; depth:7; classtype:trojan-activity;
reference:url,www.secureworks.com/analysis/spamthru/; reference:url,doc.emergingthreats.net/2003143; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_SpamThru;
sid:2003143; rev:3;)

#by Joe Stewart of Lurhq/Secureworks
#
alert tcp any any -> any any (msg:"ET TROJAN SpamThru trojan AV scan report"; flow:established,to_server; content:"|01|hs5p|0008|"; depth:7; classtype:trojan-activity;
reference:url,www.secureworks.com/analysis/spamthru/; reference:url,doc.emergingthreats.net/2003144; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_SpamThru;
sid:2003144; rev:3;)

#by Christopher Campesi
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN Spy-Net Trojan Connection"; flow:established; content:"maininfo|7c|"; depth:9; content:"|7c|"; distance:3; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/2008644; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Spy-Net; sid:2008644; rev:3;)

#This one is lets the client know the server is connected and ready
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Spy-Net Trojan Connection (2)"; flow:established; content:"conectado|7c 0a|"; depth:11; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008645; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Spy-Net; sid:2008645; rev:3;)

#by Darren Spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN SpyEye Bot Checkin"; flow:established,to_server; uricontent:".php?guid="; nocase; uricontent:"&ver="; nocase;
uricontent:"&stat="; nocase; uricontent:"&cpu="; nocase; uricontent:"&ccrc="; nocase; classtype:trojan-activity; reference:url,www.symantec.com/connect/blogs/spyeye-bot-versus-zeus-bot;
reference:url,www.symantec.com/business/security_response/writeup.jsp?docid=2010-020216-0135-99; reference:url,malwareint.blogspot.com/2010/01/spyeye-new-bot-on-market.html;
reference:url,www.threatexpert.com/report.aspx?md5=2b8a408b56eaf3ce0198c9d1d8a75ec0; reference:url,doc.emergingthreats.net/2010789; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_SpyEye; sid:2010789; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Spyguarder.com Fake AV Install Report"; flow:established,to_server; uricontent:"/statscnt.js?scrW=";
uricontent:"&scrH="; uricontent:"&ua="; uricontent:"&referer="; uricontent:"&ref_id="; uricontent:"&cn_id="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008911;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Spyguarder.com; sid:2008911; rev:2;)

#from Secureworks research
#
alert udp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Srizbi registering with controller"; dsize:20; content:"|2d|"; offset:6; content:"|2d|"; distance:6; depth:1;
content:!"|00|server."; offset:44; classtype:trojan-activity; reference:url,www.secureworks.com/research/threats/ronpaul/; reference:url,doc.emergingthreats.net/2007711;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Srizbi; sid:2007711; rev:8;)

#from Secureworks research
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Srizbi requesting template"; flow:established,to_server; content:"GET|20|/"; depth:5; content:"|0d0a|X-Flags|3a20|";
within:200; content:"|0d0a|X-TM|3a20|"; within:20; content:"|0d0a|X-BI|3a20|"; within:20; classtype:trojan-activity; reference:url,www.secureworks.com/research/threats/ronpaul/;
reference:url,doc.emergingthreats.net/2007712; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Srizbi; sid:2007712; rev:8;)

#Matt Jonkman, info from Sunbelt Software
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Srv.SSA-KeyLogger Checkin Traffic"; flow:to_server,established; uricontent:"Srv.SSA-KeyLogger"; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/2002175; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Srv.SSA-KeyLogger; sid:2002175; rev:3;)

#this may have once been a legit tool, no longer appears to be so
#Sends an email after boot to announce it's location and password
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN Ssppyy.com Surveillance Agent Reporting via Email"; flow:established,to_server; content:"|0d 0a|Subject|3a| SSPPYY
notification|0d 0a|X-Mailer|3a| Mail|0d 0a|"; content:"The computer you are monitoring has connected online - The module name of"; distance:5; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2007780; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Ssppyy; sid:2007780; rev:3;)

#Greg Bowser/Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Steam Pass Stealer FTP Upload"; flow:established,to_server; dsize:33; content:"STEAM nicht eingespeichert!!!";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008332; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Steam; sid:2008332; rev:2;)

#by Marcus at unsober
#ref: b957da5c0bc6f21341795a6ead9eddd9
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Steam Steal0r"; flow:established,to_server; uricontent:"info=Steam|20|Steal0r|20|"; uricontent:"&acc=";
uricontent:"&pw="; content:"|0d 0a|User-Agent|3a| Mozilla/4.0 (compatible|3b| MSIE 6.0|3b| Windows NT 5.1|3b| SV1)"; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008360; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Steam; sid:2008360; rev:3;)
```

```
#idea submitted anonymously, sig should catch the malware download url the storm work uses
#disabling, current variants don't seem to be using this scheme, high load rule
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Storm Worm HTTP Request"; flow:established,to_server; content:"GET "; depth:4; offset:0; uricontent:"/?"; pcre:"/GET \/\?
[0-9a-f]{16}/Ui"; pcre:"/Host\: [0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006411;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Storm; sid:2006411; rev:6;)

#by Matt jonkman, info from many sources
#
alert icmp any any -> any any (msg:"ET TROJAN Storm Worm ICMP DDOS Traffic"; itype:8; icode:0; dsize:32; content:"abcdefghijklmnopqr|00 00|"; depth:22; threshold:type both, track
by_src, count 1, seconds 60; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007618; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Storm;
sid:2007618; rev:6;)

#new storm stuff, experimental. They're encrypting packets, size and frequency matching should still work
#disabling by default. 2007701 and 2007702 are more reliable. These tend to hit on skype and game traffic
#
#alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET 1024:65535 (msg:"ET TROJAN Storm Worm Encrypted Traffic Outbound - Likely Search by md5"; dsize:25; threshold: type threshold, count 40,
seconds 60, track by_src; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007634; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Storm;
sid:2007634; rev:3;)

#new storm stuff, experimental. They're encrypting packets, size and frequency matching should still work
#disabling by default. 2007701 and 2007702 are more reliable. These tend to hit on skype and game traffic
#
#alert udp $EXTERNAL_NET 1024:65535 -> $HOME_NET 1024:65535 (msg:"ET TROJAN Storm Worm Encrypted Traffic Inbound - Likely Connect Ack"; dsize:2; threshold: type threshold, count 10,
seconds 60, track by_dst; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007635; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Storm;
sid:2007635; rev:3;)

#Significant reports of falses on skype traffic. Disabling for now
#
#alert udp $EXTERNAL_NET 1024:65535 -> $HOME_NET 1024:65535 (msg:"ET TROJAN Storm Worm Encrypted Traffic Inbound - Likely Search by md5"; dsize:25; threshold: type threshold, count 40,
seconds 60, track by_dst; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007636; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Storm;
sid:2007636; rev:3;)

#Significant reports of falses on skype traffic. Disabling for now
#
#alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET 1024:65535 (msg:"ET TROJAN Storm Worm Encrypted Traffic Outbound - Likely Connect Ack"; dsize:2; threshold: type threshold, count 10,
seconds 60, track by_src; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007637; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Storm;
sid:2007637; rev:3;)

#more storm, uses a tcp connection now for some specialized commands. reversed by Joe Stewart
#temporarily disabling for falses
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1024:65535 (msg:"ET TROJAN Storm Making initial outbound connection"; flowbits:isnotset,BE.stormtcp.init; flow:established,to_server; dsize:4;
classtype:trojan-activity; flowbits:noalert; flowbits:set,BE.stormtcp.init; reference:url,doc.emergingthreats.net/bin/view/Main/StormWorm; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Storm; sid:2007640; rev:5;)

#more storm, uses a tcp connection now for some specialized commands. reversed by Joe Stewart
#temporarily disabling for falses
#
#alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET any (msg:"ET TROJAN Storm Controller Response to Drone via tcp"; flowbits:isset,BE.stormtcp.init; flow:established,from_server; dsize:4;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/StormWorm; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Storm; sid:2007641;
rev:5;)

#adding these for a specific storm variant that is encrypting traffic.
#Temporary, there has so far been only one key used, no others have been detected here. This has remained for
#at last a month, so may stay a while. These sigs are for THIS VARIANT'S KEY ONLY
#
alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET 1024:65535 (msg:"ET TROJAN Storm Worm Encrypted Variant 1 Traffic (1)"; dsize:25; content:"|10 a6|"; depth:2; threshold: type both, count
2, seconds 60, track by_src; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007701; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Storm;
sid:2007701; rev:4;)

#adding these for a specific storm variant that is encrypting traffic.
#Temporary, there has so far been only one key used, no others have been detected here. This has remained for
#at last a month, so may stay a while. These sigs are for THIS VARIANT'S KEY ONLY
#
alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET 1024:65535 (msg:"ET TROJAN Storm Worm Encrypted Variant 1 Traffic (2)"; dsize:25; content:"|10 a0|"; depth:2; threshold: type both, count
2, seconds 60, track by_src; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007702; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Storm;
sid:2007702; rev:4;)

#storm c&c with a typo'd UA
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Storm C&C with typo'd User-Agent (Windoss)"; flow:established,to_server; content:"User-Agent|3a| Mozilla/4.0
(compatible|3b| MSIE 6.0|3b| Windoss NT"; depth:200; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007742; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Storm; sid:2007742; rev:5;)

#by packet hack
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Possible Storm Variant HTTP Post (S)"; flow:established,to_server; content:"POST /s/ HTTP"; depth:13; nocase;
content:"|0d 0a|User-Agent|3a| Internet Explorer|0d 0a|"; content:"|0d 0a 0d 0a|a="; content:!"|0d 0a|Referer|3a|"; nocase; classtype:trojan-activity;
reference:url,cyber.secdev.ca/2009/11/russian-malware-bundle; reference:url,www.blackhat.com/presentations/bh-usa-08/Stewart/BH_US_08_Stewart_Protocols_of_the_Storm.pdf;
reference:url,doc.emergingthreats.net/2010441; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Storm; sid:2010441; rev:3;)

#by packet hack
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Possible Storm Variant HTTP Post (U)"; flow:established,to_server; content:"POST /u/ HTTP"; depth:13; nocase;
content:"|0d 0a|User-Agent|3a| Internet Explorer|0d 0a|"; content:"|0d 0a 0d 0a|a="; content:!"|0d 0a|Referer|3a|"; nocase; classtype:trojan-activity;
reference:url,cyber.secdev.ca/2009/11/russian-malware-bundle; reference:url,www.blackhat.com/presentations/bh-usa-08/Stewart/BH_US_08_Stewart_Protocols_of_the_Storm.pdf;
reference:url,doc.emergingthreats.net/2010442; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Storm; sid:2010442; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Stormy Variant HTTP Request"; flow:established,to_server; uricontent:"/zzu/zc.php?l="; nocase; uricontent:"&d=";
nocase; uricontent:"&v="; nocase; uricontent:"&k="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003435; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Stormy; sid:2003435; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Stpage Checkin (nomodem)"; flow:established,to_server; uricontent:"/nomodem.php"; uricontent:"if=";
uricontent:"&am="; uricontent:"&cl={"; uricontent:"&id="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008522; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Stpage; sid:2008522; rev:2;)

#by John Curry
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Pragma hack Detected Outbound - Likely Infected Source"; flow:established,to_client; content:"Pragma|3a| hack/";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010872; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Suspicious; sid:2010872;
rev:5;)

#by Pedro Marinho
#re 05574ba46ca69e91bdeec740cd3af10c
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN FraudTool.Win32.SysCleaner.a"; flow:established,to_server; content:"GET "; depth:4; uricontent:".php?"; nocase;
uricontent:"action=stat&wmid="; nocase; uricontent:"&event="; nocase; uricontent:"&uid="; nocase; uricontent:"&i1"; nocase; uricontent:"&i2"; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008732; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Syscleaner; sid:2008732; rev:2;)

#by matt jonkman. Win32 Trojan-System.Poser
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN System.Poser HTTP Checkin"; flow:established,to_server; uricontent:"/check.php?c="; nocase; uricontent:"&v=%";
nocase; content:"|0d 0a|User-Agent|3a| Microsoft BITS"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008035; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_System.Poser; sid:2008035; rev:3;)
```