


```
# Emerging Threats
#
# This distribution may contain rules under two different licenses.
#
#  Rules with sids 1 through 3464, and 100000000 through 100000908 are under the GPLv2.
#  A copy of that license is available at http://www.gnu.org/licenses/gpl-2.0.html
#
#  Rules with sids 2000000 through 2799999 are from Emerging Threats and are covered under the BSD License
#  as follows:
#
#*************************************************************
#  Copyright (c) 2003-2010, Emerging Threats
#  All rights reserved.
#
#  Redistribution and use in source and binary forms, with or without modification, are permitted provided that the
#  following conditions are met:
#
#  * Redistributions of source code must retain the above copyright notice, this list of conditions and the following
#    disclaimer.
#  * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the
#    following disclaimer in the documentation and/or other materials provided with the distribution.
#  * Neither the name of the nor the names of its contributors may be used to endorse or promote products derived
#    from this software without specific prior written permission.
#
#  THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS AS IS AND ANY EXPRESS OR IMPLIED WARRANTIES,
#  INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
#  DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
#  SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
#  SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
#  WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
#  USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
#
#*************************************************************
#
#
#
#

# This Ruleset is EmergingThreats Open optimized for snort-2.8.4.
#by Jaime Blasco
#
#alert tcp $HTTP_SERVERS $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE HTTP 401 Unauthorized"; flow:from_server,established; content:"HTTP/1."; depth:7; content:" 401";
within:5; threshold: type both, count 1, seconds 300, track by_dst; classtype:attempted-recon; reference:url,doc.emergingthreats.net/2009345; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_401_Unauthorized; sid:2009345; rev:6;)

#by Jaime Blasco
#
alert tcp $HTTP_SERVERS $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE Frequent HTTP 401 Unauthorized - Possible Brute Force Attack"; flow:from_server,established; content:"
401"; offset:7; depth:5; threshold:type both, track by_dst, count 30, seconds 60; classtype:attempted-recon; reference:url,doc.emergingthreats.net/2009346;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_401_Unauthorized; sid:2009346; rev:8;)

#by David Wharton
#
##alert tcp $HTTP_SERVERS $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE Possible ASPXSpy Request"; flow:established,from_server; content:"Thanks Snailsor,FuYu,BloodSword";
classtype:web-application-activity; reference:url,doc.emergingthreats.net/2009146; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_ASPXSpy;
sid:2009146; rev:3;)

#by David Wharton
#
##alert tcp $HTTP_SERVERS $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE Possible ASPXSpy Related Activity"; flow:established,from_server; content:"public string Password|3D
22|21232f297a57a5a743894a0e4a801fc3|22 3B|"; nocase; classtype:web-application-activity; reference:url,doc.emergingthreats.net/2009147; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_ASPXSpy; sid:2009147; rev:3;)

#by David Wharton
#
##alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET ATTACK_RESPONSE Possible ASPXSpy Upload Attempt"; flow:established,to_server; content:"public string Password|3D
22|21232f297a57a5a743894a0e4a801fc3|22 3B|"; nocase; classtype:web-application-activity; reference:url,doc.emergingthreats.net/2009149; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_ASPXSpy; sid:2009149; rev:3;)

#by Jaime Blasco
#
#alert udp $HOME_NET any -> $EXTERNAL_NET 69 (msg:"ET ATTACK_RESPONSE Cisco TclShell TFTP Read Request"; content:"|00 01 74 63 6C 73 68 2E 74 63 6C|"; classtype:bad-unknown;
reference:url,wwww.irmplc.com/downloads/whitepapers/Creating_Backdoors_in_Cisco_IOS_using_Tcl.pdf; reference:url,doc.emergingthreats.net/2009244;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Cisco_TCL_Shell; sid:2009244; rev:2;)

#by Jaime Blasco
#
alert udp $EXTERNAL_NET 69 -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Cisco TclShell TFTP Download"; content:"|54 63 6C 53 68 65 6C 6C|"; classtype:bad-unknown;
reference:url,wwww.irmplc.com/downloads/whitepapers/Creating_Backdoors_in_Cisco_IOS_using_Tcl.pdf; reference:url,doc.emergingthreats.net/2009245;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Cisco_TCL_Shell; sid:2009245; rev:2;)

#by Jaime Blasco
#
#alert tcp any any -> any any (msg:"ET SHELLCODE Bindshell2 Decoder Shellcode"; flow:established; content:"|53 53 53 53 53 43 53 43 53 FF D0 66 68|"; content:"|66 53 89 E1 95 68 A4
1A|"; distance:0; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009246; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009246; rev:3;)

#by Jaime Blasco
#
alert udp any any -> any any (msg:"ET SHELLCODE Bindshell2 Decoder Shellcode (UDP)"; content:"|53 53 53 53 53 43 53 43 53 FF D0 66 68|"; content:"|66 53 89 E1 95 68 A4 1A|"; distance:0;
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009285; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009285; rev:2;)

#by Jaime Blasco
#
#alert tcp any any -> any any (msg:"ET SHELLCODE Rothenburg Shellcode"; flow:established; content:"|D9 74 24 F4 5B 81 73 13|"; content:"|83 EB FC E2 F4|"; distance:0;
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009247; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009247; rev:3;)

#by Jaime Blasco
#
#alert udp any any -> any any (msg:"ET SHELLCODE Rothenburg Shellcode (UDP)"; content:"|D9 74 24 F4 5B 81 73 13|"; content:"|83 EB FC E2 F4|"; distance:0; classtype:shellcode-detect;
reference:url,doc.emergingthreats.net/2009284; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009284; rev:2;)

#by Jaime Blasco
#
```

```
#alert tcp any any -> any any (msg:"ET SHELLCODE Lindau (linkbot) xor Decoder Shellcode"; flow:established; content:"|EB 15 B9|"; content:"|81 F1|"; distance:0; content:"|80 74 31 FF|";
distance:0; content:"|E2 F9 EB 05 E8 E6 FF FF FF|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009248; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009248; rev:3;)

#by Jaime Blasco
#
#alert udp any any -> any any (msg:"ET SHELLCODE Lindau (linkbot) xor Decoder Shellcode (UDP)"; content:"|EB 15 B9|"; content:"|81 F1|"; distance:0; content:"|80 74 31 FF|"; distance:0;
content:"|E2 F9 EB 05 E8 E6 FF FF FF|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009283; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009283; rev:2;)

#by Jaime Blasco
#
#alert tcp any any -> any any (msg:"ET SHELLCODE Adenau Shellcode"; flow:established; content:"|eb 19 5e 31 c9 81 e9|"; content:"|81 36|"; distance:0; content:"|81 ee fc ff ff ff|";
distance:0; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009249; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009249; rev:3;)

#by Jaime Blasco
#
#alert udp any any -> any any (msg:"ET SHELLCODE Adenau Shellcode (UDP)"; content:"|eb 19 5e 31 c9 81 e9|"; content:"|81 36|"; distance:0; content:"|81 ee fc ff ff ff|"; distance:0;
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009282; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009282; rev:2;)

#by Jaime Blasco
#
#alert tcp any any -> any any (msg:"ET SHELLCODE Mainz/Bielefeld Shellcode"; flow:established; content:"|33 c9 66 b9|"; content:"|80 34|"; distance:0; content:"|eb 05 e8 eb ff ff ff|";
distance:0; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009250; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009250; rev:3;)

#by Jaime Blasco
#
#alert udp any any -> any any (msg:"ET SHELLCODE Mainz/Bielefeld Shellcode (UDP)"; content:"|33 c9 66 b9|"; content:"|80 34|"; distance:0; content:"|eb 05 e8 eb ff ff ff|"; distance:0;
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009281; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009281; rev:2;)

#by Jaime Blasco
#
#alert tcp any any -> any any (msg:"ET SHELLCODE Wuerzburg Shellcode"; flow:established; content:"|eb 27|"; content:"|5d 33 c9 66 b9|"; distance:0; content:"|8d 75 05 8b fe 8a 06 3c|";
distance:0; content:"|75 05 46 8a 06|"; distance:0; content:"|88 07 47 e2 ed eb 0a e8 da ff ff ff|"; distance:0; classtype:shellcode-detect;
reference:url,doc.emergingthreats.net/2009251; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009251; rev:3;)

#by Jaime Blasco
#
#alert udp any any -> any any (msg:"ET SHELLCODE Wuerzburg Shellcode (UDP)"; content:"|eb 27|"; content:"|5d 33 c9 66 b9|"; distance:0; content:"|8d 75 05 8b fe 8a 06 3c|"; distance:0;
content:"|75 05 46 8a 06|"; distance:0; content:"|88 07 47 e2 ed eb 0a e8 da ff ff ff|"; distance:0; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009280;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009280; rev:2;)

#by Jaime Blasco
#
#alert tcp any any -> any any (msg:"ET SHELLCODE Schauenburg Shellcode"; flow:established; content:"|eb 0f 8b 34 24 33 c9 80 c1|"; content:"|80 36|"; distance:0; content:"|46 e2 fa c3
e8 ec|"; distance:0; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009252; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009252; rev:3;)

#by Jaime Blasco
#
#alert udp any any -> any any (msg:"ET SHELLCODE Schauenburg Shellcode (UDP)"; content:"|eb 0f 8b 34 24 33 c9 80 c1|"; content:"|80 36|"; distance:0; content:"|46 e2 fa c3 e8 ec|";
distance:0; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009279; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009279; rev:2;)

#by Jaime Blasco
#
#alert tcp any any -> any any (msg:"ET SHELLCODE Koeln Shellcode"; flow:established; content:"|eb 0f 8b 34 24 33 c9 80 c1|"; content:"|80 36|"; distance:0; content:"|46 e2 fa c3 e8
ec|"; distance:0; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009253; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009253; rev:3;)

#by Jaime Blasco
#
#alert udp any any -> any any (msg:"ET SHELLCODE Koeln Shellcode (UDP)"; content:"|eb 0f 8b 34 24 33 c9 80 c1|"; content:"|80 36|"; distance:0; content:"|46 e2 fa c3 e8 ec|";
distance:0; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009278; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009278; rev:2;)

#by Jaime Blasco
#
#alert tcp any any -> any any (msg:"ET SHELLCODE Lichtenfels Shellcode"; flow:established; content:"|01 fc ff ff 83 e4 fc 8b ec 33 c9 66 b9|"; content:"|80 30|"; distance:0;
content:"|40 e2 fA|"; distance:0; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009254; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009254; rev:3;)

#by Jaime Blasco
#
#alert udp any any -> any any (msg:"ET SHELLCODE Lichtenfels Shellcode (UDP)"; content:"|01 fc ff ff 83 e4 fc 8b ec 33 c9 66 b9|"; content:"|80 30|"; distance:0; content:"|40 e2 fA|";
distance:0; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009277; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009277; rev:2;)

#by Jaime Blasco
#
#alert tcp any any -> any any (msg:"ET SHELLCODE Mannheim Shellcode"; flow:established; content:"|80 73 0e|"; content:"|43 e2|"; distance:0; content:"|73 73 73|"; distance:0;
content:"|81 86 8c 81|"; distance:0; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009255; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009255; rev:3;)

#by Jaime Blasco
#
#alert udp any any -> any any (msg:"ET SHELLCODE Mannheim Shellcode (UDP)"; content:"|80 73 0e|"; content:"|43 e2|"; distance:0; content:"|73 73 73|"; distance:0; content:"|81 86 8c
81|"; distance:0; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009276; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009276; rev:2;)

#by Jaime Blasco
#
#alert tcp any any -> any any (msg:"ET SHELLCODE Berlin Shellcode"; flow:established; content:"|31 c9 b1 fc 80 73 0c|"; content:"|43 e2 8b 9f|"; distance:0; classtype:shellcode-detect;
reference:url,doc.emergingthreats.net/2009256; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009256; rev:3;)

#by Jaime Blasco
#
#alert udp any any -> any any (msg:"ET SHELLCODE Berlin Shellcode (UDP)"; content:"|31 c9 b1 fc 80 73 0c|"; content:"|43 e2 8b 9f|"; distance:0; classtype:shellcode-detect;
reference:url,doc.emergingthreats.net/2009275; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009275; rev:2;)

#by Jaime Blasco
#
#alert tcp any any -> any any (msg:"ET SHELLCODE Leimbach Shellcode"; flow:established; content:"|5b 31 c9 b1|"; content:"|80 73|"; distance:0; content:"|43 e2|"; distance:0;
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009257; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009257; rev:3;)

#by Jaime Blasco
#
#alert udp any any -> any any (msg:"ET SHELLCODE Leimbach Shellcode (UDP)"; content:"|5b 31 c9 b1|"; content:"|80 73|"; distance:0; content:"|43 e2|"; distance:0; classtype:shellcode-
detect; reference:url,doc.emergingthreats.net/2009274; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009274;
rev:2;)

#by Jaime Blasco
#
```

```
#alert tcp any any -> any any (msg:"ET SHELLCODE Aachen Shellcode"; flow:established; content:"|8b 45 04 35|"; content:"|89 45 04 66 8b 45 02 66 35|"; distance:0; content:"|66 89 45
02|"; distance:0; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009258; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009258; rev:3;)

#by Jaime Blasco
#
#alert udp any any -> any any (msg:"ET SHELLCODE Aachen Shellcode (UDP)"; content:"|8b 45 04 35|"; content:"|89 45 04 66 8b 45 02 66 35|"; distance:0; content:"|66 89 45 02|";
distance:0; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009273; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009273; rev:2;)

#by Jaime Blasco
#
#alert tcp any any -> any any (msg:"ET SHELLCODE Furth Shellcode"; flow:established; content:"|31 c9 66 b9|"; content:"|80 73|"; distance:0; content:"|43 e2 1f|"; distance:0;
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009259; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009259; rev:3;)

#by Jaime Blasco
#
#alert udp any any -> any any (msg:"ET SHELLCODE Furth Shellcode (UDP)"; content:"|31 c9 66 b9|"; content:"|80 73|"; distance:0; content:"|43 e2 1f|"; distance:0; classtype:shellcode-
detect; reference:url,doc.emergingthreats.net/2009272; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009272;
rev:2;)

#by Jaime Blasco
#
#alert tcp any any -> any any (msg:"ET SHELLCODE Langenfeld Shellcode"; flow:established; content:"|eb 0f 5b 33 c9 66 b9|"; content:"|80 33|"; distance:0; content:"|43 e2 fa eb|";
distance:0; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009260; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009260; rev:3;)

#by Jaime Blasco
#
#alert udp any any -> any any (msg:"ET SHELLCODE Langenfeld Shellcode (UDP)"; content:"|eb 0f 5b 33 c9 66 b9|"; content:"|80 33|"; distance:0; content:"|43 e2 fa eb|"; distance:0;
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009271; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009271; rev:2;)

#by Jaime Blasco
#
#alert tcp any any -> any any (msg:"ET SHELLCODE Bonn Shellcode"; flow:established; content:"|31 c9 81 e9|"; content:"|83 eb|"; distance:0; content:"|80 73|"; distance:0; content:"|43
e2 f9|"; distance:0; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009261; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009261; rev:3;)

#by Jaime Blasco
#
#alert udp any any -> any any (msg:"ET SHELLCODE Bonn Shellcode (UDP)"; content:"|31 c9 81 e9|"; content:"|83 eb|"; distance:0; content:"|80 73|"; distance:0; content:"|43 e2 f9|";
distance:0; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009270; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009270; rev:2;)

#by Jaime Blasco
#
#alert tcp any any -> any any (msg:"ET SHELLCODE Siegburg Shellcode"; flow:established; content:"|31 eb 80 eb|"; content:"|58 80 30|"; distance:0; content:"|40 81 38|"; distance:0;
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009262; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009262; rev:3;)

#by Jaime Blasco
#
#alert udp any any -> any any (msg:"ET SHELLCODE Siegburg Shellcode (UDP)"; content:"|31 eb 80 eb|"; content:"|58 80 30|"; distance:0; content:"|40 81 38|"; distance:0;
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009269; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009269; rev:2;)

#by Jaime Blasco
#
#alert tcp any any -> any any (msg:"ET SHELLCODE Plain1 Shellcode"; flow:established; content:"|89 e1 cd|"; content:"|5b 5d 52 66 bd|"; distance:0; content:"|0f cd 09 dd 55 6a|";
distance:0; content:"|51 50|"; distance:0; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009263; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009263; rev:3;)

#by Jaime Blasco
#
#alert udp any any -> any any (msg:"ET SHELLCODE Plain1 Shellcode (UDP)"; content:"|89 e1 cd|"; content:"|5b 5d 52 66 bd|"; distance:0; content:"|0f cd 09 dd 55 6a|"; distance:0;
content:"|51 50|"; distance:0; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009268; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009268; rev:2;)

#by Jaime Blasco
#
#alert tcp any any -> any any (msg:"ET SHELLCODE Plain2 Shellcode"; flow:established; content:"|50 50 50 50 40 50 40 50 ff 56 1c 8b d8 57 57 68 02|"; content:"|8b cc 6a|"; distance:0;
content:"|51 53|"; distance:0; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009264; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009264; rev:3;)

#by Jaime Blasco
#
#alert udp any any -> any any (msg:"ET SHELLCODE Plain2 Shellcode (UDP)"; content:"|50 50 50 50 40 50 40 50 ff 56 1c 8b d8 57 57 68 02|"; content:"|8b cc 6a|"; distance:0; content:"|51
53|"; distance:0; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009267; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009267; rev:2;)

#by Jaime Blasco
#
#alert tcp any any -> any any (msg:"ET SHELLCODE Bindshell1 Decoder Shellcode"; flow:established; content:"|58 99 89 E1 CD 80 96 43 52 66 68|"; content:"|66 53 89 E1 6A 66 58 50 51
56|"; distance:0; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009265; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009265; rev:3;)

#by Jaime Blasco
#
#alert udp any any -> any any (msg:"ET SHELLCODE Bindshell1 Decoder Shellcode (UDP)"; content:"|58 99 89 E1 CD 80 96 43 52 66 68|"; content:"|66 53 89 E1 6A 66 58 50 51 56|";
distance:0; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2009266; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Common_ShellCode; sid:2009266; rev:2;)

#by Jaime Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 21 (msg:"ET ATTACK_RESPONSE FTP CWD to windows system32 - Suspicious"; flow:established,to_server; content:"CWD C|3a|\\WINDOWS\\system32\\";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008556; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_FTP; sid:2008556; rev:6;)

#Submitted by Joseph Gama
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET ATTACK_RESPONSE FTP inaccessible directory access COM1"; flow: established; content:"/COM1/"; nocase; classtype: string-detect;
reference:url,doc.emergingthreats.net/bin/view/Main/2000499; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Hidden_FTP_File_Activity;
sid:2000499; rev:8;)

#Submitted by Joseph Gama
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET ATTACK_RESPONSE FTP inaccessible directory access COM2"; flow: established; content:"/COM2/"; nocase; classtype: string-detect;
reference:url,doc.emergingthreats.net/bin/view/Main/2000500; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Hidden_FTP_File_Activity;
sid:2000500; rev:8;)

#Submitted by Joseph Gama
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET ATTACK_RESPONSE FTP inaccessible directory access COM3"; flow: established; content:"/COM3/"; nocase; classtype: string-detect;
reference:url,doc.emergingthreats.net/bin/view/Main/2000501; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Hidden_FTP_File_Activity;
sid:2000501; rev:8;)

#Submitted by Joseph Gama
#
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET ATTACK_RESPONSE FTP inaccessible directory access COM4"; flow: established; content:"/COM4/"; nocase; classtype: string-detect;
reference:url,doc.emergingthreats.net/bin/view/Main/2000502; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Hidden_FTP_File_Activity;
sid:2000502; rev:8;)

#Submitted by Joseph Gama
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET ATTACK_RESPONSE FTP inaccessible directory access LPT1"; flow: established; content:"/LPT1/"; nocase; classtype: string-detect;
reference:url,doc.emergingthreats.net/bin/view/Main/2000503; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Hidden_FTP_File_Activity;
sid:2000503; rev:8;)

#Submitted by Joseph Gama
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET ATTACK_RESPONSE FTP inaccessible directory access LPT2"; flow: established; content:"/LPT2/"; nocase; classtype: string-detect;
reference:url,doc.emergingthreats.net/bin/view/Main/2000504; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Hidden_FTP_File_Activity;
sid:2000504; rev:8;)

#Submitted by Joseph Gama
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET ATTACK_RESPONSE FTP inaccessible directory access LPT3"; flow: established; content:"/LPT3/"; nocase; classtype: string-detect;
reference:url,doc.emergingthreats.net/bin/view/Main/2000505; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Hidden_FTP_File_Activity;
sid:2000505; rev:8;)

#Submitted by Joseph Gama
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET ATTACK_RESPONSE FTP inaccessible directory access LPT4"; flow: established; content:"/LPT4/"; nocase; classtype: string-detect;
reference:url,doc.emergingthreats.net/bin/view/Main/2000506; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Hidden_FTP_File_Activity;
sid:2000506; rev:8;)

#Submitted by Joseph Gama
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET ATTACK_RESPONSE FTP inaccessible directory access AUX"; flow: established; content:"/AUX/"; nocase; classtype: string-detect;
reference:url,doc.emergingthreats.net/bin/view/Main/2000507; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Hidden_FTP_File_Activity;
sid:2000507; rev:8;)

#Submitted by Joseph Gama
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET ATTACK_RESPONSE FTP inaccessible directory access NULL"; flow: established; content:"/NULL/"; nocase; classtype: string-detect;
reference:url,doc.emergingthreats.net/bin/view/Main/2000508; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Hidden_FTP_File_Activity;
sid:2000508; rev:8;)

#by Matt Jonkman
#seeing some worms/trojans use an ftp server with all banners stripped out
#on off ports to download payload after the initial compromise.
#Just stats codes, no welcome, etc. Very unique
#something like:
#220
#USER a
#331
#PASS a
#230
#TYPE I
#200
#PORT 10,2,32,214,4,9
#200
#RETR msnnmaneger.exe
#150
#226
#QUIT
#221
#removing a few to simplify
#
#alert tcp $HOME_NET 1024: -> any 1024: (msg:"ET ATTACK_RESPONSE Off-Port FTP Without Banners - user"; flow:established,from_server; dsize:>7; content:"USER "; depth:5; offset:0;
content:" |0d 0a|"; distance:1; flowbits:set,ET.strippedftpuser; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007715;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Hostile_FTP; sid:2007715; rev:9;)

#by Matt Jonkman
#seeing some worms/trojans use an ftp server with all banners stripped out
#on off ports to download payload after the initial compromise.
#Just stats codes, no welcome, etc. Very unique
#something like:
#220
#USER a
#331
#PASS a
#230
#TYPE I
#200
#PORT 10,2,32,214,4,9
#200
#RETR msnnmaneger.exe
#150
#226
#QUIT
#221
#removing a few to simplify
#
#alert tcp $HOME_NET 1024: -> any 1024: (msg:"ET ATTACK_RESPONSE Off-Port FTP Without Banners - pass"; flowbits:isset,ET.strippedftpuser; flow:established,from_server; dsize:>7;
content:"PASS "; depth:5; offset:0; content:" |0d 0a|"; distance:1; flowbits:set,ET.strippedftppass; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2007717; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Hostile_FTP; sid:2007717;
rev:7;)

#by Matt Jonkman
#seeing some worms/trojans use an ftp server with all banners stripped out
#on off ports to download payload after the initial compromise.
#Just stats codes, no welcome, etc. Very unique
#something like:
#220
#USER a
#331
#PASS a
#230
#TYPE I
#200
#PORT 10,2,32,214,4,9
#200
#RETR msnnmaneger.exe
#150
#226
#QUIT
#221
#removing a few to simplify
#
#alert tcp $HOME_NET 1024: -> any 1024: (msg:"ET ATTACK_RESPONSE Off-Port FTP Without Banners - retr"; flowbits:isset,ET.strippedftppass; flow:established,from_server; dsize:>7;
content:"RETR "; depth:5; offset:0; tag:session,300,seconds; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007723;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Hostile_FTP; sid:2007723; rev:8;)

#matt jonkman, info from qru
#
```

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Windows LMHosts File Download - Likely DNSChanger Infection"; flow:established,to_client; content:"#|0d
0a|#|20|This|20|is|20|a|20|sample|20|HOSTS|20|file|20|used|20|by|20|Microsoft|20|TCP/IP|20|for|20|Windows.|0d 0a|#|0d
0a|#|20|This|20|file|20|contains|20|the|20|mappings|20|of|20|IP|20|addresses|20|to|20|host|20|names."; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2008559; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_LMHosts_Download; sid:2008559;
rev:5;)

#Matt Jonkman, information from Stephen Gill at Cymru
#
alert tcp any 21 -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Hostile FTP Server Banner (StnyFtpd)"; flow:established,from_server; content:"220 StnyFtpd 0wns j0"; offset:0; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002809; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Malicious_FTP; sid:2002809; rev:5;)

#Matt Jonkman, information from Stephen Gill at Cymru
#
alert tcp any 21 -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Hostile FTP Server Banner (Reptile)"; flow:established,from_server; content:"220 Reptile welcomes you"; offset:0; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002810; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Malicious_FTP; sid:2002810; rev:4;)

#Matt Jonkman, information from Stephen Gill at Cymru
#
alert tcp any 21 -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Hostile FTP Server Banner (Bot Server)"; flow:established,from_server; content:"220 Bot Server (Win32)"; offset:0; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002811; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Malicious_FTP; sid:2002811; rev:5;)

#Matt Jonkman, information from Stephen Gill at Cymru
#
alert tcp any 21 -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Unusual FTP Server Banner (warFTPd)"; flow:established,from_server; content:"220 "; content:"--warFTPd "; depth:40;
distance:0; nocase; classtype:trojan-activity; reference:url,www.warftp.org; reference:url,doc.emergingthreats.net/bin/view/Main/2003464; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Malicious_FTP; sid:2003464; rev:4;)

#Matt Jonkman, information from Stephen Gill at Cymru
#
alert tcp any 21 -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Unusual FTP Server Banner (freeFTPd)"; flow:established,from_server; content:"220 "; content:"--freeFTPd "; depth:40;
distance:0; nocase; classtype:trojan-activity; reference:url,www.freeftp.com; reference:url,doc.emergingthreats.net/bin/view/Main/2003465; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Malicious_FTP; sid:2003465; rev:4;)

#Matt Jonkman, off port ftp banners
#
alert tcp any 1024: -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Unusual FTP Server Banner on High Port (WinFtpd)"; flow:established,from_server; dsize:<18; content:"220 WinFtpd";
depth:11; offset:0; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007725; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Malicious_FTP; sid:2007725; rev:6;)

#Matt Jonkman, off port ftp banners
#
alert tcp any 1024: -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Unusual FTP Server Banner on High Port (StnyFtpd)"; flow:established,from_server; dsize:<30; content:"220 StnyFtpd";
depth:12; offset:0; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007726; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Malicious_FTP; sid:2007726; rev:6;)

#by Jaime Blasco
#
alert tcp any [21,1024:] -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Unusual FTP Server Banner (fuckFtpd)"; flow:established,from_server; dsize:<18; content:"220 fuckFtpd"; depth:12;
offset:0; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009210; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Malicious_FTP; sid:2009210; rev:3;)

#by Jaime Blasco
#
alert tcp any [21,1024:] -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Unusual FTP Server Banner (NzmxFtpd)"; flow:established,from_server; dsize:<18; content:"220 NzmxFtpd"; depth:12;
offset:0; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009211; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Malicious_FTP; sid:2009211; rev:3;)

#by josh smith
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET ATTACK_RESPONSE Matahari client"; flow:to_server,established; content:"Accept|2d|Encoding|3a 20|identity|0d 0a|";
content:"Next|2d|Polling"; distance:0; content:"Content|2d|Salt|3a| "; pcre:"/Content\x2dSalt\x3a\x20[0-9\.\-]+\x0d\x0a/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2010795; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Matahari; sid:2010795; rev:5;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter File Download Detected"; flow:to_client,established; content:"stdapi_fs_stat"; depth:54;
classtype:successful-user; reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf; reference:url,doc.emergingthreats.net/2009558; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009558; rev:2;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter Process List (ps) Command Detected"; flow:to_client,established;
content:"stdapi_sys_process_get_processes"; depth:65; classtype:successful-user; reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf;
reference:url,doc.emergingthreats.net/2009559; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009559; rev:2;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter Getuid Command Detected"; flow:to_client,established; content:"stdapi_sys_config_getuid";
depth:65; classtype:successful-user; reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf; reference:url,doc.emergingthreats.net/2009560;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009560; rev:2;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter Process Migration Detected"; flow:to_client,established; content:"core_migrate"; depth:60;
classtype:successful-user; reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf; reference:url,doc.emergingthreats.net/2009561; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009561; rev:2;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter ipconfig Command Detected"; flow:to_client,established;
content:"stdapi_net_config_get_interfaces"; depth:65; threshold: type threshold, track by_src, count 2, seconds 4; classtype:successful-user;
reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf; reference:url,doc.emergingthreats.net/2009562; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009562; rev:2;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter Sysinfo Command Detected"; flow:to_client,established; content:"stdapi_sys_config_sysinfo";
depth:60; classtype:successful-user; reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf; reference:url,doc.emergingthreats.net/2009563;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009563; rev:2;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter Route Command Detected"; flow:to_client,established; content:"stdapi_net_config_get_route";
depth:62; classtype:successful-user; reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf; reference:url,doc.emergingthreats.net/2009564;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009564; rev:2;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter Kill Process Command Detected"; flow:to_client,established;
content:"stdapi_sys_process_kill"; depth:60; classtype:successful-user; reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf; reference:url,doc.emergingthreats.net/2009565;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009565; rev:2;)

#by Kevin Ross
#
```

```
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter Print Working Directory Command Detected"; flow:to_client,established;
content:"stdapi_fs_getwd"; depth:55; classtype:successful-user; reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf; reference:url,doc.emergingthreats.net/2009566;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009566; rev:2;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter View Current Process ID Command Detected"; flow:to_client,established;
content:"stdapi_sys_process_getpid"; depth:60; classtype:successful-user; reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf; reference:url,doc.emergingthreats.net/2009567;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009567; rev:2;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter Execute Command Detected"; flow:to_client,established;
content:"stdapi_sys_process_execute"; depth:62; classtype:successful-user; reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf; reference:url,doc.emergingthreats.net/2009568;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009568; rev:2;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter System Reboot/Shutdown Detected"; flow:to_client,established;
content:"stdapi_sys_power_exitwindows"; depth:62; classtype:successful-user; reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf;
reference:url,doc.emergingthreats.net/2009569; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009569; rev:2;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter System Get Idle Time Command Detected"; flow:to_client,established;
content:"stdapi_ui_get_idle_time"; depth:60; classtype:successful-user; reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf; reference:url,doc.emergingthreats.net/2009570;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009570; rev:2;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter Make Directory Command Detected"; flow:to_client,established; content:"stdapi_fs_mkdir";
depth:55; classtype:successful-user; reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf; reference:url,doc.emergingthreats.net/2009571;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009571; rev:2;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter Remove Directory Command Detected"; flow:to_client,established;
content:"stdapi_fs_delete_dir"; depth:57; classtype:successful-user; reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf; reference:url,doc.emergingthreats.net/2009572;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009572; rev:2;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter Change Directory Command Detected"; flow:to_client,established; content:"stdapi_fs_chdir";
depth:57; classtype:successful-user; reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf; reference:url,doc.emergingthreats.net/2009573;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009573; rev:2;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter List (ls) Command Detected"; flow:to_client,established; content:"stdapi_fs_ls"; depth:52;
classtype:successful-user; reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf; reference:url,doc.emergingthreats.net/2009574; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009574; rev:3;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter rev2self Command Detected"; flow:to_client,established;
content:"stdapi_sys_config_rev2self"; depth:52; classtype:successful-user; reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf; reference:url,doc.emergingthreats.net/2009575;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009575; rev:3;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter Enabling/Disabling of Keyboard Detected"; flow:to_client,established;
content:"stdapi_ui_enable_keyboard"; depth:60; classtype:successful-user; reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf; reference:url,doc.emergingthreats.net/2009576;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009576; rev:2;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter Enabling/Disabling of Mouse Detected"; flow:to_client,established;
content:"stdapi_ui_enable_mouse"; depth:60; classtype:successful-user; reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf; reference:url,doc.emergingthreats.net/2009577;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009577; rev:2;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter File/Memory Interaction Detected"; flow:to_client,established;
content:"stdapi_fs_file_expand_path"; depth:60; classtype:successful-user; reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf; reference:url,doc.emergingthreats.net/2009578;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009578; rev:2;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter Registry Interation Detected"; flow:to_client,established;
content:"stdapi_registry_create_key"; depth:60; classtype:successful-user; reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf; reference:url,doc.emergingthreats.net/2009579;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009579; rev:2;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter File Upload Detected"; flow:to_client,established; content:"core_channel_write"; depth:50;
classtype:successful-user; reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf; reference:url,doc.emergingthreats.net/2009580; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009580; rev:2;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ATTACK_RESPONSE Metasploit Meterpreter Channel Interaction Detected, Likely Interaction With Executable";
flow:to_client,established; content:"core_channel_interact"; depth:60; classtype:successful-user; reference:url,www.nologin.org/Downloads/Papers/meterpreter.pdf;
reference:url,doc.emergingthreats.net/2009651; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009651; rev:3;)

#by shirkdog
#
#alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET 1024:65535 (msg:"ET ATTACK_RESPONSE Metasploit/Meterpreter - Sending metsrv.dll to Compromised Host"; flow:established;
content:"metsrv.dll|00|MZ"; depth:13; content:"!This program cannot be run in DOS mode."; distance:75; within:40; classtype:successful-admin;
reference:url,doc.emergingthreats.net/2009581; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2009581; rev:3;)

#by Varga-Perke Balint
#
#alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET 1024:65535 (msg:"ET ATTACK_RESPONSE Metasploit/Meterpreter - Sending metsrv.dll to Compromised Host"; flow:established; content:"|40 00
41 00 42 0043 00 44 00 6d 65 74 73 72 76 2e 64 6c 6c 00 49 6e 69 74 00 5f 52 65 66 6c 65 63 74 69 76 65 4c 6f 61|"; classtype:successful-admin;
reference:url,doc.emergingthreats.net/2010454; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Meterpreter; sid:2010454; rev:3;)

#Submitted by Joel Esler
#
alert tcp $HOME_NET any -> $EXTERNAL_NET !6661:6668 (msg:"ET ATTACK_RESPONSE IRC - Nick change on non-std port"; flow: to_server,established; dsize: <64; content:"NICK "; nocase;
offset: 0; depth: 5; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2000345; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Non-Standard_IRC; sid:2000345; rev:9;)

#Submitted by Joel Esler
#
alert tcp $EXTERNAL_NET !6661:6668 -> $HOME_NET any (msg:"ET ATTACK_RESPONSE IRC - Name response on non-std port"; flow: to_client,established; dsize: <128; content:"|3a|"; offset: 0;
depth: 1; content:" 302 "; content:"=+"; content:"@"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2000346; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Non-Standard_IRC; sid:2000346; rev:10;)

#Submitted by Joel Esler
#
alert tcp $HOME_NET any -> $EXTERNAL_NET !6661:6668 (msg:"ET ATTACK_RESPONSE IRC - Private message on non-std port"; flow: to_server,established; dsize: <128; content:"PRIVMSG ";
```

```
nocase; offset: 0; depth: 8; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2000347; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Non-Standard_IRC; sid:2000347; rev:9;)

#Submitted by Joel Esler
#
alert tcp $HOME_NET any -> $EXTERNAL_NET !6667 (msg:"ET ATTACK_RESPONSE IRC - Channel JOIN on non-std port"; flow: to_server,established; dsize: <64; content:"JOIN "; nocase; offset: 0;
depth: 5; pcre:"/&|#|\+|!/R"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2000348; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Non-Standard_IRC; sid:2000348; rev:10;)

#Submitted by Joel Esler
#
alert tcp $HOME_NET any -> $EXTERNAL_NET !6661:6668 (msg:"ET ATTACK_RESPONSE IRC - DCC file transfer request on non-std port"; flow: to_server,established; content:"PRIVMSG "; nocase;
offset: 0; depth: 8; content:" |3a|.DCC SEND"; nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2000349;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Non-Standard_IRC; sid:2000349; rev:9;)

#Submitted by Joel Esler
#
alert tcp $HOME_NET any -> $EXTERNAL_NET !6661:6668 (msg:"ET ATTACK_RESPONSE IRC - DCC chat request on non-std port"; flow: to_server,established; content:"PRIVMSG "; nocase; offset: 0;
depth: 8; content:" |3a|.DCC CHAT chat"; nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2000350; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Non-Standard_IRC; sid:2000350; rev:10;)

#Submitted by Joel Esler
#
alert tcp $HOME_NET any -> $EXTERNAL_NET !6661:6668 (msg:"ET ATTACK_RESPONSE IRC - channel join on non-std port"; flow: to_server,established; content:"JOIN |3a| #"; nocase; offset: 0;
depth: 8; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2000351; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Non-Standard_IRC; sid:2000351; rev:10;)

#Submitted by Joel Esler
#
alert tcp $HOME_NET any -> $EXTERNAL_NET !6661:6668 (msg:"ET ATTACK_RESPONSE IRC - dns request on non-std port"; flow: to_server,established; content:"USERHOST "; nocase; offset: 0;
depth: 9; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2000352; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Non-Standard_IRC; sid:2000352; rev:9;)

#Erik Fichtner
#
#alert tcp $HOME_NET any -> any 6667 (msg:"ET ATTACK_RESPONSE Likely Botnet Activity"; flowbits:isset,is_proto_irc; flow:to_server,established; content:"PRIVMSG|20|"; depth:8; nocase;
pcre:"/(cheguei gazelas|meh que tao|Status|Tempo|Total pacotes|Total bytes|M?dia de envio|portas? aberta)/i"; classtype: string-detect;
reference:url,doc.emergingthreats.net/bin/view/Main/2001620; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Non-Standard_IRC; sid:2001620;
rev:8;)

#By Chris Norton
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE Outbound PHP Connection"; flow: established,to_server; content:"From|3a| anon@anon.com"; nocase; offset: 0; depth:
19; content:"User-Agent|3a| PHP"; nocase; classtype: web-application-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001628; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Outbound_PHP_Fopen; sid:2001628; rev:9;)

#by Cees Elzinga
#note: most effective with a deep flow depth, or 0
#
alert tcp $HTTP_SERVERS $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE r57 phpshell footer detected"; flow:established,from_server; content:"r57shell - http-shell by
RST/GHC"; classtype:web-application-activity; reference:url,www.pestpatrol.com/spywarecenter/pest.aspx?id=453096755; reference:url,doc.emergingthreats.net/bin/view/Main/2003535;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_PHP_Shells; sid:2003535; rev:6;)

#by Cees Elzinga
#note: most effective with a deep flow depth, or 0
#
#alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET ATTACK_RESPONSE r57 phpshell source being uploaded"; flow:established,to_server; content:"/*  (c)oded by 1dt.w0lf";
content:"/*  RST/GHC http"; distance:0; classtype:web-application-activity; reference:url,www.pestpatrol.com/spywarecenter/pest.aspx?id=453096755;
reference:url,doc.emergingthreats.net/bin/view/Main/2003536; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_PHP_Shells; sid:2003536;
rev:8;)

#by Ryan Macdonald of R-fx networks (www.rfxn.com)
#those commented out are more prone to false positives. They'll be more reliable in a web-only environment
#
alert tcp $HTTP_SERVERS $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE x2300 phpshell detected"; flow:established,from_server; content:"x2300 Locus7Shell"; classtype:web-
application-activity; reference:url,www.rfxn.com/vdb.php; reference:url,doc.emergingthreats.net/bin/view/Main/2007651; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_PHP_Shells; sid:2007651; rev:5;)

#by Ryan Macdonald of R-fx networks (www.rfxn.com)
#those commented out are more prone to false positives. They'll be more reliable in a web-only environment
#
#alert tcp $HTTP_SERVERS $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE c99shell phpshell detected"; flow:established,from_server; content:"c99shell"; classtype:web-
application-activity; reference:url,www.rfxn.com/vdb.php; reference:url,doc.emergingthreats.net/bin/view/Main/2007652; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_PHP_Shells; sid:2007652; rev:5;)

#by Ryan Macdonald of R-fx networks (www.rfxn.com)
#those commented out are more prone to false positives. They'll be more reliable in a web-only environment
#
#alert tcp $HTTP_SERVERS $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE RFI Scanner detected"; flow:established,from_server; content:"RFI Scanner"; classtype:web-application-
activity; reference:url,www.rfxn.com/vdb.php; reference:url,doc.emergingthreats.net/bin/view/Main/2007653; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_PHP_Shells; sid:2007653; rev:5;)

#by Ryan Macdonald of R-fx networks (www.rfxn.com)
#those commented out are more prone to false positives. They'll be more reliable in a web-only environment
#
#alert tcp $HTTP_SERVERS $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE C99 Modified phpshell detected"; flow:established,from_server; content:"C99 Modified"; classtype:web-
application-activity; reference:url,www.rfxn.com/vdb.php; reference:url,doc.emergingthreats.net/bin/view/Main/2007654; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_PHP_Shells; sid:2007654; rev:5;)

#by Ryan Macdonald of R-fx networks (www.rfxn.com)
#those commented out are more prone to false positives. They'll be more reliable in a web-only environment
#
#alert tcp $HTTP_SERVERS $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE lila.jpg phpshell detected"; flow:established,from_server; content:"CMD PHP"; classtype:web-
application-activity; reference:url,www.rfxn.com/vdb.php; reference:url,doc.emergingthreats.net/bin/view/Main/2007655; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_PHP_Shells; sid:2007655; rev:5;)

#by Ryan Macdonald of R-fx networks (www.rfxn.com)
#those commented out are more prone to false positives. They'll be more reliable in a web-only environment
#
#alert tcp $HTTP_SERVERS $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE ALBANIA id.php detected"; flow:established,from_server; content:"UNITED ALBANIANS aka ALBOSS
PARADISE"; classtype:web-application-activity; reference:url,www.rfxn.com/vdb.php; reference:url,doc.emergingthreats.net/bin/view/Main/2007656;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_PHP_Shells; sid:2007656; rev:5;)

#by Ryan Macdonald of R-fx networks (www.rfxn.com)
#those commented out are more prone to false positives. They'll be more reliable in a web-only environment
#
#alert tcp $HTTP_SERVERS $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE Mic22 id.php detected"; flow:established,from_server; content:"Mic22"; classtype:web-application-
activity; reference:url,www.rfxn.com/vdb.php; reference:url,doc.emergingthreats.net/bin/view/Main/2007657; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_PHP_Shells; sid:2007657; rev:5;)

#by Christian Teutenberg
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET ATTACK_RESPONSE Backdoor reDuh http initiate"; flow:to_server,established; uricontent:"?action=checkPort&port=";
content:"|0d 0a|User-Agent|3A|"; nocase; content:"Java/"; distance:0; classtype:trojan-activity; reference:url,www.sensepost.com/labs/tools/pentest/reduh;
reference:url,doc.emergingthreats.net/2011667; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Reduh; sid:2011667; rev:3;)

#by Christian Teutenberg
#
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET ATTACK_RESPONSE Backdoor reDuh http tunnel"; flow:to_server,established; uricontent:"?action=getData&servicePort=";
content:"|0d 0a|User-Agent|3A|"; nocase; content:"Java/"; distance:0; threshold:type limit, track by_src, count 1, seconds 300; classtype:trojan-activity;
reference:url,www.sensepost.com/labs/tools/pentest/reduh; reference:url,doc.emergingthreats.net/2011668; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Reduh; sid:2011668; rev:3;)

#by Adam Ellison
#Detects the old style weak and crackable windows auth in use. By default this should not be in
#active use, but can be forced by hostile parties by a number of methods
#
alert tcp $HOME_NET 139 -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE Weak Netbios Lanman Auth Challenge Detected"; flow:from_server; content:"|ff 53 4d 42|"; content:"|00 11 22 33 44
55 66 77 88|"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2006417; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Short_Lanman_Auth_Challenge; sid:2006417; rev:8;)

#for a windows cmd shell opened on a local box
#
alert tcp $HOME_NET any -> any any (msg:"ET ATTACK_RESPONSE Possible MS CMD Shell opened on local system"; flow:established; dsize:<110; content:"Microsoft Windows "; depth:20;
content:"Copyright 1985-20"; distance:0; content:"Microsoft Corp"; distance:0; content:"|0a 0a|C|3a 5c|WINDOWS|5c|"; distance:0; classtype:successful-admin;
reference:url,doc.emergingthreats.net/bin/view/Main/2008953; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Windows_Shell; sid:2008953;
rev:8;)

#by Kevin Ross
#
#alert tcp $HTTP_SERVERS $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE Possible Ipconfig Information Detected in HTTP Response"; flow:from_server,established;
content:"Windows IP Configuration"; content:"Ethernet adapter Local Area Connection"; distance:8; within:40; classtype:successful-recon-limited;
reference:url,en.wikipedia.org/wiki/Ipconfig; reference:url,doc.emergingthreats.net/2009675; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Windows_Shell; sid:2009675; rev:3;)

#by Kevin Ross
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE Ipconfig Response Detected"; flow:from_server,established; content:"Windows IP Configuration"; content:"Ethernet
adapter Local Area Connection"; offset:35; distance:8; depth:55; classtype:successful-recon-limited; reference:url,en.wikipedia.org/wiki/Ipconfig;
reference:url,doc.emergingthreats.net/2009676; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Windows_Shell; sid:2009676; rev:3;)

#By Erik Fichtner
#
alert tcp $HOME_NET any -> 87.98.168.239/32 $HTTP_PORTS (msg:"ET ATTACK_RESPONSE Zone-H.org defacement notification"; flow: established,to_server; content:"notify_"; nocase;
pcre:"/notify_(defacer|domain|hackmode|reason)=/i"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001616; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Zone-h_Defacement; sid:2001616; rev:10;)

#by Matt Jonkman
#
alert tcp $HOME_NET $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE Possible /etc/passwd via HTTP (linux style)"; flow:established,from_server;
content:"root|3a|x|3a|0|3a|0|3a|root|3a|/root|3a|/"; nocase; classtype:misc-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002034;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_etc-passwd; sid:2002034; rev:8;)

#by Matt Jonkman
#
alert tcp $HOME_NET $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE Possible /etc/passwd via HTTP (BSD style)"; flow:established,from_server;
content:"root|3a|*|3a|0|3a|0|3a|"; nocase; content:"|3a|/root|3a|/bin"; nocase; classtype:misc-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003071;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_etc-passwd; sid:2003071; rev:5;)

#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET ATTACK_RESPONSE Possible /etc/passwd via SMTP (linux style)"; flow:established,from_server;
content:"root|3a|x|3a|0|3a|0|3a|root|3a|/root|3a|/"; nocase; classtype:misc-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003149;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_etc-passwd; sid:2003149; rev:4;)

#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET ATTACK_RESPONSE Possible /etc/passwd via SMTP (BSD style)"; flow:established,from_server; content:"root|3a|*|3a|0|3a|0|3a|"; nocase;
content:"|3a|/root|3a|/bin"; nocase; classtype:misc-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003150; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_etc-passwd; sid:2003150; rev:4;)

#by kevin ross
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT Possible Adobe Multimedia Doc.media.newPlayer Memory Corruption Attempt"; flow:to_client,established;
content:"PDF-"; nocase; depth:300; content:"this.media.newPlayer|28|null"; nocase; distance:0; content:"util.printd"; nocase; within:150; classtype:attempted-user;
reference:url,www.metasploit.com/redmine/projects/framework/repository/revisions/7881/entry/modules/exploits/windows/fileformat/adobe_media_newplayer.rb; reference:url,vrt-
sourcefire.blogspot.com/2009/12/adobe-reader-medianewplayer-analysis.html; reference:url,www.securityfocus.com/bid/37331; reference:cve,2009-4324;
reference:url,doc.emergingthreats.net/2010495; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Adobe; sid:2010495; rev:10;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS Adobe 0day Shovelware"; flow:established,to_server; content:"GET "; nocase; depth:4; content:!"|0d
0a|Referer|3a|"; nocase; uricontent:"/ppp/listdir.php?dir="; nocase; pcre:"/\/[a-z]{2}\/[a-z]{4}01\/ppp\/listdir\.php\?dir=/Ui"; classtype:trojan-activity;
reference:url,isc.sans.org/diary.html?storyid=7747; reference:url,doc.emergingthreats.net/2010496; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Adobe; sid:2010496; rev:6;)

#kevin ross
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT Possible Adobe Reader and Acrobat Forms Data Format Remote Security Bypass Attempt"; flow:established,to_client;
content:"|0d 0a|%FDF-"; depth:600; content:"/F(JavaScript|3a|"; nocase; distance:0; classtype:attempted-user; reference:url,www.securityfocus.com/bid/37763; reference:cve,2009-3956;
reference:url,doc.emergingthreats.net/2010664; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Adobe; reference:url,www.stratsec.net/files/SS-2010-
001_Stratsec_Acrobat_Script_Injection_Security_Advisory_v1.0.pdf; sid:2010664; rev:4;)

#kevin ross
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Possible NOS Microsystems Adobe Reader/Acrobat getPlus Get_atlcomHelper ActiveX Control Multiple Stack Overflows
Remote Code Execution Attempt"; flow:established,to_client; content:"E2883E8F-472F-4fb0-9522-AC9BF37916A7"; nocase; content:"offer-"; nocase; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*
[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*E2883E8F-472F-4fb0-9522-AC9BF37916A7.+offer-(ineligible|preinstalled|declined|accepted)/si"; classtype:attempted-user;
reference:url,www.securityfocus.com/bid/37759; reference:url,www.kb.cert.org/vuls/id/773545; reference:url,www.adobe.com/support/security/bulletins/apsb10-02.html;
reference:url,www.exploit-db.com/exploits/11172/; reference:cve,2009-3958; reference:url,doc.emergingthreats.net/2010665; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Adobe; sid:2010665; rev:5;)

#kevin ross
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS Adobe Macromedia Flash Player In Windows XP Remote Arbitrary Code Execution CLSID Access Attempt";
flow:established,to_client; content:"clsid"; nocase; content:"D27CDB6E-AE6D-11cf-96B8-444553540000"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?
\s*clsid\s*\x3a\s*\x7B?\s*D27CDB6E-AE6D-11cf-96B8-444553540000/si"; classtype:attempted-user; reference:url,tools.cisco.com/security/center/viewAlert.x?alertId=19710;
reference:url,www.kb.cert.org/vuls/id/204889; reference:url,www.microsoft.com/technet/security/advisory/979267.mspx; reference:url,doc.emergingthreats.net/2010666;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Adobe; sid:2010666; rev:2;)

#by L0rd Ch0de1m0rt
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS Adobe Flash 0Day Exploit Attempt"; flow:established,from_server; content:"CWS|09|"; content:"|BA D5 19 5D 86
67 D5 8E 7F BC D0 3C 6E D8 E2 17 16 E8 3A 9F CF 59 B8 7B F6|"; distance:16; classtype:misc-attack; reference:url,www.exploit-db.com/exploits/13787/;
reference:url,doc.emergingthreats.net/2011672; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Adobe; sid:2011672; rev:2;)

#by kevin ross
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Possible NOS Microsystems Adobe Reader/Acrobat getPlus Get_atlcom Helper ActiveX Control Multiple Stack Overflows
Remote Code Execution Attempt"; flow:established,to_client; content:"clsid"; nocase; content:"E2883E8F-472F-4fb0-9522-AC9BF37916A7"; nocase; distance:0; content:!"offer-"; nocase;
pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*E2883E8F-472F-4fb0-9522-AC9BF37916A7.+(service-url|banner|noexec|OS|Lang|return-page|core-
product|userid|itemid|_c[xy]|sec-param|secparam)/si"; classtype:attempted-user; reference:url,www.securityfocus.com/bid/37759; reference:url,www.kb.cert.org/vuls/id/773545;
reference:url,www.exploit-db.com/exploits/11172/; reference:url,www.adobe.com/support/security/bulletins/apsb10-02.html; reference:cve,2009-3958;
reference:url,doc.emergingthreats.net/2011675; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Adobe; sid:2011675; rev:2;)
```

```
#by jaime blasco
#seeing if these last, ua may change often
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS FakeAV AntivirusDoktor2009 User-Agent (768)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
768"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010682; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_AntivirusDoktor2009;
sid:2010682; rev:3;)

#by jaime blasco
#seeing if these last, ua may change often
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS FakeAV AntivirusDoktor2009 User-Agent (657)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
657"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010683; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_AntivirusDoktor2009;
sid:2010683; rev:5;)

#by David Wharton
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS Internal User may have Visited an ASProx Infected Site (ads-t.ru)"; flow:established,from_server; content:"
<script src=http\://www.ads-t.ru/ads.js>"; nocase; classtype:trojan-activity; reference:url,garwarner.blogspot.com/2009/10/cyber-security-awareness-month-day-one.html;
reference:url,doc.emergingthreats.net/2010032; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Asprox; sid:2010032; rev:2;)

#by David Wharton
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS Internal User may have Visited an ASProx Infected Site (bannert.ru)"; flow:established,from_server;
content:"<script src=http|3a|//www.bannert.ru/ads.js>"; nocase; classtype:trojan-activity; reference:url,garwarner.blogspot.com/2009/10/cyber-security-awareness-month-day-one.html;
reference:url,doc.emergingthreats.net/2010033; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Asprox; sid:2010033; rev:3;)

#by David Wharton
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS Internal User may have Visited an ASProx Infected Site (bannerdriven.ru)"; flow:established,from_server;
content:"<script src=http|3a|//www.bannerdriven.ru/ads.js>"; nocase; classtype:trojan-activity; reference:url,garwarner.blogspot.com/2009/10/cyber-security-awareness-month-day-one.html;
reference:url,doc.emergingthreats.net/2010034; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Asprox; sid:2010034; rev:4;)

#by Daniel Sheperd
#
alert udp any any -> any 53 (msg:"ET DOS DNS BIND 9 Dynamic Update DoS attempt"; byte_test:1,&,40,2; byte_test:1,>,0,5; byte_test:1,>,0,1; content:"|00 00 06|"; offset:8; content:"|c0
0c 00 ff|"; distance:2; classtype:attempted-dos; reference:cve,2009-0696; reference:url,doc.emergingthreats.net/2009701; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Bind; sid:2009701; rev:2;)

#by Kevin Ross, temporary, based on a specific exploit if generated in hping
#
alert tcp $EXTERNAL_NET any -> $HOME_NET [22,23,80,443,10000] (msg:"ET CURRENT_EVENTS Possible Cisco PIX/ASA Denial Of Service Attempt (Hping Created Packets)"; flow:to_server;
content:"|58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58|"; depth:40; content:"|58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58
58 58 58 58 58 58 58|"; distance:300; isdataat:300,relative; threshold: type threshold, track by_src, count 60, seconds 80; classtype:attempted-dos;
reference:url,www.securityfocus.com/bid/34429/info; reference:url,www.securityfocus.com/bid/34429/exploit;
reference:url,www.cisco.com/en/US/products/products_applied_mitigation_bulletin09186a0080a99518.html; reference:cve,2009-1157; reference:url,doc.emergingthreats.net/2010624;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Cisco; sid:2010624; rev:2;)

#by Kevin Ross, temporary, based on a specific exploit if generated in hping
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 5060 (msg:"ET CURRENT_EVENTS Possible Cisco ASA 5500 Series Adaptive Security Appliance Remote SIP Inspection Device Reload Denial of Service
Attempt"; flow:established,to_server; content:"REGISTER"; depth:8; nocase; isdataat:400,relative; pcre:"/REGISTER.{400}/smi"; classtype:attempted-dos;
reference:url,tools.cisco.com/security/center/viewAlert.x?alertId=19915; reference:cve,2010-0569; reference:url,doc.emergingthreats.net/2010817;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Cisco; sid:2010817; rev:3;)

#Temporarily disabled until we get a fix for an FP problem
#
#alert udp $EXTERNAL_NET any -> $HOME_NET 5060 (msg:"ET CURRENT_EVENTS Possible Cisco ASA 5500 Series Adaptive Security Appliance Remote SIP Inspection Device Reload Denial of Service
Attempt"; content:"REGISTER"; depth:8; nocase; isdataat:400,relative; pcre:"/REGISTER.{400}/smi"; classtype:attempted-dos; reference:url,tools.cisco.com/security/center/viewAlert.x?
alertId=19915; reference:cve,2010-0569; reference:url,doc.emergingthreats.net/2010818; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Cisco;
sid:2010818; rev:3;)

#matt jonkman, idea from Jason Weir
#
#alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"ET CURRENT_EVENTS DHL Spam Inbound"; flow:established,to_server; content:"Content-Disposition|3A| attachment|3b|"; nocase;
content:"filename=|22|DHL_"; nocase; pcre:"/filename=\x22DHL_(label_id|ID.document)\.Nr[0-9]{4,5}\.zip\x22/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010148;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_DHL; sid:2010148; rev:9;)

#matt jonkman, idea from Jason Weir
#
#alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"ET CURRENT_EVENTS WU Malicious Spam Inbound"; flow:established,to_server; content:"Content-Disposition|3A| attachment|3b|";
nocase; content:"filename"; within:100; content:"WU_Details_"; within:50; pcre:"/filename\s*=\s*"WU_Details_.....\.zip/m"; classtype:trojan-activity;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_DHL; reference:url,doc.emergingthreats.net/2010376; sid:2010376; rev:3;)

#by jason weir and wolvee
#
#alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"ET CURRENT_EVENTS Facebook Spam Inbound (1)"; flow:established,to_server; content:"Content-Disposition|3A| attachment|3b|";
nocase; content:"filename"; within:100; content:"Facebook_Password"; within:50; pcre:"/filename\s*=\s*Facebook_Password_[0-9]{5}\.zip/m"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2010497; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_DHL; sid:2010497; rev:3;)

#by jason weir and wolvee
#
#alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"ET CURRENT_EVENTS Facebook Spam Inbound (2)"; flow:established,to_server; content:"Content-Disposition|3A| attachment|3b|";
nocase; content:"filename=|22|Facebook"; pcre:"/filename=\x22Facebook_(Password|Support|Document)_[A-Z0-9]{4,7}\.zip\x22/m"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2010498; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_DHL; sid:2010498; rev:4;)

#Matt Jonkman
#
#alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"ET CURRENT_EVENTS MySpace Spam Inbound"; flow:established,to_server; content:"Content-Disposition|3A| attachment|3b|"; nocase;
content:"filename"; within:100; content:"MySpace"; within:50; pcre:"/filename\s*=\s*MySpace_document_[0-9]{5}\.zip/m"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2010629; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_DHL; sid:2010629; rev:3;)

#Matt Jonkman
#
#alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"ET CURRENT_EVENTS UPS Spam Inbound"; flow:established,to_server; content:"Content-Disposition|3A| attachment|3b|"; nocase;
content:"filename"; within:100; content:"UPS"; within:50; pcre:"/filename\s*=\s*UPS_invoice_NR[0-9]{5}\.zip/m"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010644;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_DHL; sid:2010644; rev:3;)

#evilghost
#
#alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"ET CURRENT_EVENTS UPS Spam Inbound Variant 2"; flow:established,to_server; content:"Content-Disposition|3A| attachment|3b|";
nocase; content:"filename"; within:100; content:"UPS_INVOICE_NR"; within:50; pcre:"/filename=\x22UPS_INVOICE_NR\.[0-9]{4}-[0-9]{6}\.zip\x22/mi"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/201150; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_DHL; sid:2011150; rev:3;)

#evilghost
#
#alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"ET CURRENT_EVENTS UPS Spam Inbound Variant 3"; flow:established,to_server; content:"Content-Disposition|3a| attachment|3b|";
nocase; content:"filename=|22|UPS_LABEL_NR."; nocase; within:50; pcre:"/filename=\x22UPS_LABEL_NR\.[A-Z]+_[0-9]{4}-\d+\.ZIP\x22/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2011151; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_DHL; sid:2011151; rev:3;)

#by many very smart people
#This may be a high load sig. Take time and seriously consider
#that your dns_servers var is set as narrowly as possible
#disabling, remove in the not too distant future
#
#alert udp any 53 -> $DNS_SERVERS any (msg:"ET DNS Excessive DNS Responses with 1 or more RR's (100+ in 10 seconds) - possible Cache Poisoning Attempt"; byte_test:2,>,0,6;
byte_test:2,>,0,10; threshold: type both, track by_src, count 100, seconds 10; classtype:bad-unknown; reference:url,doc.emergingthreats.net/bin/view/Main/2008446;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_DNS_Poisoning; sid:2008446; rev:9;)

#this will catch large numbers of nxdomain replies, a sign that someone may be trying to poison you
#
```

```
#alert udp any 53 -> $HOME_NET any (msg:"ET DNS Excessive NXDOMAIN responses - Possible DNS Poisoning Attempt Backscatter"; byte_test:1,&,128,2; byte_test:1,&,1,3; byte_test:1,&,2,3;
threshold: type both, track by_src, count 100, seconds 10; classtype:bad-unknown; reference:url,doc.emergingthreats.net/bin/view/Main/2008470; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_DNS_Poisoning; sid:2008470; rev:3;)

#by Greg Martin at Econet
#
#alert udp any 53 -> $HOME_NET any (msg:"ET DNS Query Responses with 3 RR's set (50+ in 2 seconds) - possible NS RR Cache Poisoning Attempt"; content: "|85 00 00 01 00 01 00 01|";
offset: 2; depth:8; threshold: type both, track by_src,count 50, seconds 2; classtype:bad-unknown; reference:url,infosec20.blogspot.com/2008/07/kaminsky-dns-cache-poisoning-poc.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2008447; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_DNS_Poisoning; sid:2008447; rev:7;)

#by Greg Martin at Econet
#
#alert udp any 53 -> $HOME_NET any (msg:"ET DNS Query Responses with 3 RR's set (50+ in 2 seconds) - possible A RR Cache Poisoning Attempt"; content: "|81 80 00 01 00 01 00 01|";
offset: 2; depth:8; threshold: type both, track by_src, count 50, seconds 2; classtype:bad-unknown; reference:url,infosec20.blogspot.com/2008/07/kaminsky-dns-cache-poisoning-poc.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2008475; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_DNS_Poisoning; sid:2008475; rev:4;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS Potential Fake Anti-Virus Download Inst_58s6.exe"; flow:established,to_server; uricontent:"/Inst_58s6.exe";
nocase; classtype:trojan-activity; reference:url,cyveillanceblog.com/general-cyberintel/malware-google-search-results; reference:url,doc.emergingthreats.net/2010339;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_FakeAV; sid:2010339; rev:2;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS Potential FakeAV download ASetup_2009.exe variant"; flow:established,to_server; content:"GET "; nocase;
depth:4; uricontent:"Setup_"; nocase; uricontent:".exe"; nocase; content:!"|0d 0a|Referer|3a| "; nocase; pcre:"/\/[A-Z]Setup_[0-9]{4}\.exe$/Ui"; classtype:trojan-activity;
reference:url,www.prevx.com/avgraph/1/AVG.html; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Fakeav_Setup_dl;
reference:url,doc.emergingthreats.net/2010901; sid:2010901; rev:4;)

#2010-07-09 By Evilghost and Mike Cox
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS FakeAV Download with Cookie WinSec"; flow:established,to_server; uricontent:"/down.php?c="; nocase;
content:"|0d 0a|Cookie|3a| WinSec"; nocase; classtype:trojan-activity; reference:url,www.virustotal.com/analisis/6b5ff522ddf418a5cca87ebd924736774c1a58a9b51bb44ee72dac01f0db317a-
1278686791; reference:url,doc.emergingthreats.net/2011178; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_FakeAV; sid:2011178; rev:3;)

#by Eoin Miller
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS Likely FAKEAV scanner page encountered - i1000000.gif"; flow:established,to_server;
uricontent:"/i1000000.gif"; nocase; classtype:bad-unknown; reference:url,doc.emergingthreats.net/2011760; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_FakeAV; sid:2011760; rev:6;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS Potential FakeAV download Setup_103s1 or Setup_207 variant"; flow:established,to_server; content:"GET ";
nocase; depth:4; uricontent:"/Setup_"; nocase; uricontent:".exe"; nocase; content:!"|0d 0a|Referer|3a| "; nocase; pcre:"/\/Setup_[0-9]{3}([A-Z][0-9])?\.exe$/Ui"; classtype:trojan-
activity; reference:url,www.prevx.com/avgraph/1/AVG.html; reference:url,doc.emergingthreats.net/2010867; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Fakeav_Setup_dl; sid:2010867; rev:5;)

#by mike cox
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS RFI Scanner Success (Fx29ID)"; flow:established,from_server; content:"FeeLCoMzFeeLCoMz";
classtype:successful-user; reference:url,doc.emergingthreats.net/2010463; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_FeeLCoMz; sid:2010463;
rev:4;)

#by kevin ross
#needs removed somewhere around the end of may 2010
#Modified Slightly to Improve Detection (Action seems to be able to come either side of Launch so removed it and left in launch and win and added in a content match for .exe
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT Possible Foxit/Adobe PDF Reader Launch Action Remote Code Execution Attempt"; flow:to_client,established;
content:"PDF-"; nocase; depth:300; content:"Launch"; distance:0; content:"Win"; distance:0; content:".exe"; nocase; distance:0; classtype:attempted-user;
reference:url,www.kb.cert.org/vuls/id/570177; reference:url,www.h-online.com/security/news/item/Criminals-attempt-to-exploit-unpatched-hole-in-Adobe-Reader-979286.html;
reference:url,www.sudosecure.net/archives/673; reference:url,www.h-online.com/security/news/item/Adobe-issues-official-workaround-for-PDF-vulnerability-971932.html;
reference:url,blog.didierstevens.com/2010/03/31/escape-from-foxit-reader/; reference:url,www.m86security.com/labs/i/PDF-Launch-Feature-Used-to-Install-Zeus,trace.1301~.asp;
reference:url,doc.emergingthreats.net/2010968; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/sigs/CURRENT_EVENTS/CURRENT_Foxit; sid:2010968; rev:4;)

#by eoin miller and peers
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS Hostile domain, NeoSploit FakeAV google.analytics.com.*.info"; flow:established,to_server; content:"GET ";
nocase; depth:4; content:"|0d 0a|Host|3a| google.analytics.com."; nocase; content:".info|0d 0a|"; within:15; classtype:trojan-activity;
reference:url,www.malwaredomainlist.com/forums/index.php?action=printpage#-#-topic=3781.0; reference:url,doc.emergingthreats.net/2010866; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Hostile_Google_Fake_Domain; sid:2010866; rev:3;)

#by mike cox
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS iPhone Bot iKee.B Contacting C&C"; flow:to_server,established; uricontent:"/xml/p.php?id="; nocase;
pcre:"/\/xml\/p\.php\?id=\d{2,}/Ui"; classtype:trojan-activity; reference:url,mtc.sri.com/iPhone/; reference:url,doc.emergingthreats.net/2010551;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Ikee; sid:2010551; rev:7;)

#by mareadmin
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET CURRENT_EVENTS Possible JAVA pack200-zip-exploit attempt"; flow:to_client; content:"e.pack.gz"; content:"|0d 0a|Content-
Encoding|3a| pack200-gzip"; within:55; classtype:attempted-user; reference:url,isc.sans.org/diary.html?storyid=6805&rss; reference:url,doc.emergingthreats.net/2009665;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Java; sid:2009665; rev:3;)

#by kevin ross
#A bit more basic detection for the Java Exploit
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT Possible Java Deployment Toolkit Launch Method Remote Code Execution Attempt"; flow:established,to_client;
content:"-J-jar -J"; pcre:"/(launch\x28.+-J-jar -J|-J-jar -J.+launch\x28)/i"; classtype:attempted-user; reference:url,seclists.org/fulldisclosure/2010/Apr/119;
reference:url,www.darknet.org.uk/2010/04/serious-java-bug-exposes-users-to-code-execution/; reference:url,doc.emergingthreats.net/2011053; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Java; sid:2011053; rev:2;)

#by mike cox
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT Java Web Start Command Injection (.jar)"; flow:established,from_server; content:"http|3a| -J-jar -J|5C 5C 5C
5C|"; nocase; content:".launch("; nocase; pcre:"/http|3a| -J-jar -J\x5C\x5C\x5C\x5C\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\x5C\x5C[^\n]*\.jar/i"; classtype:web-application-attack;
reference:url,seclists.org/fulldisclosure/2010/Apr/119; reference:url,doc.emergingthreats.net/2011698; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Java; sid:2011698; rev:5;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET WEB_CLIENT Java JAR PROPFIND via DAV possible alternative JVM exploit"; flow:established,to_server; content:"PROPFIND ";
depth:9; nocase; uricontent:".jar"; nocase; content:"|0d 0a|User-Agent|3a| Microsoft-WebDAV-MiniRedir"; nocase; content:!"|0d 0a|Referer|3a| "; nocase; classtype:bad-unknown;
reference:url,blogs.zdnet.com/security/?p=6082; reference:url,doc.emergingthreats.net/2011009; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Java_Webdav; sid:2011009; rev:3;)

#by kevin ross
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Possible Java Deployment Toolkit CSLID Command Execution Attempt"; flow:to_client,established; content:"CAFEEFAC-
DEC7-0000-0000-ABCDEFFEDCBA"; nocase; content:"launch"; nocase; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*CAFEEFAC-DEC7-0000-0000-ABCDEFFEDCBA/si";
classtype:attempted-user; reference:url,seclists.org/fulldisclosure/2010/Apr/119; reference:url,doc.emergingthreats.net/2011010; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Java_Webdav; sid:2011010; rev:4;)

#by kevin ross
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS Possible Microsoft Windows Shortcut LNK File Automatic File Execution Attempt Via WebDAV";
flow:established,to_client; content:"<lp2|3A|executable>T</lp2|3A|executable>"; nocase; content:"<D|3A|lockscope><D|3A|shared/></D|3A|lockscope>"; nocase; distance:0; content:"
<D|3A|locktype><D|3A|write/></D|3A|locktype>"; nocase; distance:0; content:"<D|3A|getcontenttype>shortcut</D|3A|getcontenttype>"; nocase; distance:0; classtype:attempted-user;
reference:url,support.microsoft.com/kb/2286198; reference:url,www.kb.cert.org/vuls/id/940193; reference:url,tools.cisco.com/security/center/viewAlert.x?alertId=20918;
```

```
reference:cve,2010-2568; reference:url,doc.emergingthreats.net/2011239; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Lnk; sid:2011239; rev:2;)

#by kevin ross
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS Possible Microsoft Windows .lnk File Processing WebDAV Arbitrary Code Execution Attempt";
flow:established,to_client; content:"<lp2|3A|executable>T</lp2|3A|executable>"; nocase; content:"<D|3A|lockscope><D|3A|exclusive/></D|3A|lockscope>"; nocase; distance:0; content:"
</D|3A|lockentry>"; nocase; distance:0; content:"<D|3A|lockscope><D|3A|shared/></D|3A|lockscope>"; nocase; distance:0; classtype:attempted-user;
reference:url,tools.cisco.com/security/center/viewAlert.x?alertId=20918; reference:url,www.kb.cert.org/vuls/id/940193;
reference:url,www.microsoft.com/technet/security/advisory/2286198.mspx; reference:cve,2010-2568; reference:url,doc.emergingthreats.net/2011270;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Lnk; sid:2011270; rev:2;)

#by kevin ross
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT Possible Microsoft Internet Explorer URI Validation Remote Code Execution Attempt"; flow:established,to_client;
content:"#|3A|../../"; content:"C|3A 5C|"; nocase; within:50; pcre:"/\x2E\x2E\x2F\x2E\x2E\x2F.+C\x3A\x5C[a-z]/si"; classtype:attempted-user;
reference:url,www.securityfocus.com/bid/37884; reference:cve,2010-0027; reference:url,doc.emergingthreats.net/2010798; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSIE; sid:2010798; rev:3;)

#Modified to avoid the short content matches as these should be accurate enough. Revision number has been incremented and msg slightly modified and a few more references added (BID,
Cisco & Microsoft)
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT Possible Internet Explorer srcElement Memory Corruption Attempt"; flow:established,to_client;
content:"document.createEventObject"; nocase; content:".innerHTML"; within:100; nocase; content:"window.setInterval"; distance:0; nocase; classtype:attempted-user;
reference:url,www.microsoft.com/technet/security/bulletin/ms10-002.mspx; reference:url,tools.cisco.com/security/center/viewAlert.x?alertId=19726;
reference:url,www.kb.cert.org/vuls/id/492515; reference:cve,2010-0249; reference:url,doc.emergingthreats.net/2010799; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSIE; sid:2010799; rev:3;)

#kevin ross
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Internet Explorer Tabular DataURL ActiveX Control Memory Corruption Attempt"; flow:established,to_client;
content:"333C7BC4-460F-11D0-BC04-0080C7055A83"; nocase; content:"DataURL"; nocase; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*333C7BC4-460F-11D0-BC04-
0080C7055A83/si"; classtype:attempted-user; reference:url,securitytracker.com/alerts/2010/Mar/1023773.html; reference:url,tools.cisco.com/security/center/viewAlert.x?alertId=20202;
reference:url,www.metasploit.com/redmine/projects/framework/repository/revisions/9018/entry/modules/exploits/windows/browser/ms10_018_ie_tabular_activex.rb;
reference:url,www.microsoft.com/technet/security/bulletin/ms10-018.mspx; reference:url,www.vupen.com/english/advisories/2010/0744; reference:url,www.kb.cert.org/vuls/id/744549;
reference:cve,2010-0805; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSIE; reference:url,doc.emergingthreats.net/2011007; sid:2011007; rev:6;)

#kevin ross
#
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 1433 (msg:"ET CURRENT_EVENTS MSSQL sp_replwritetovarbin - potential memory overwrite case 1"; flow:to_server,established;
content:"s|00|p|00|_|00|r|00|e|00|p|00|l|00|w|00|r|00|i|00|t|00|e|00|t|00|o|00|v|00|a|00|r|00|b|00|i|00|n"; nocase; classtype:attempted-user;
reference:url,archives.neohapsis.com/archives/fulldisclosure/2008-12/0239.html; reference:url,doc.emergingthreats.net/bin/view/Main/2008909; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSSQL; sid:2008909; rev:2;)

#kevin ross
#
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 1433 (msg:"ET CURRENT_EVENTS MSSQL sp_replwritetovarbin - potential memory overwrite case 2"; flow:to_server,established;
content:"sp_replwritetovarbin"; nocase; classtype:attempted-user; reference:url,archives.neohapsis.com/archives/fulldisclosure/2008-12/0239.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2008910; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSSQL; sid:2008910; rev:2;)

#by David Wharton
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS Microsoft DirectShow ActiveX Exploit Attempt"; flow:to_client,established; content:"clsid"; nocase;
content:"0955AC62-BF2E-4CBA-A2B9-A63F772D46CF"; nocase; content:"omybro"; nocase; content:"logo.gif"; nocase; classtype:web-application-attack;
reference:url,csis.dk/dk/nyheder/nyheder.asp?tekstID=799; reference:url,tools.cisco.com/security/center/viewAlert.x?alertId=18595; reference:url,doc.emergingthreats.net/2009491;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009491; rev:3;)

#by anonymous #1
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS Likely MSVIDCTL.dll exploit in transit"; flow:to_client,established; content:"|00 03 00 00 11 20 34|";
content:"|ff ff ff ff 0c 0c 0c 0c 00|"; within:70; classtype:trojan-activity; reference:url,isc.sans.org/diary.html?storyid=6733;
reference:url,tools.cisco.com/security/center/viewAlert.x?alertId=18595; reference:url,doc.emergingthreats.net/2009493; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009493; rev:3;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (29)"; flow:to_client,established; content:"clsid"; nocase;
content:"A8DCF3D5-0780-4EF4-8A83-2CFFAACB8ACE"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*A2E30750-6C3D-11D3-B653-00C04F79498E/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009598;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009598; rev:4;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (30)"; flow:to_client,established; content:"clsid"; nocase;
content:"AD8E510D-217F-409B-8076-29C5E73B98E8"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*AD8E510D-217F-409B-8076-29C5E73B98E8/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009599;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009599; rev:4;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (31)"; flow:to_client,established; content:"clsid"; nocase;
content:"B0EDF163-910A-11D2-B632-00C04F79498E"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*B0EDF163-910A-11D2-B632-00C04F79498E/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009600;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009600; rev:4;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (32)"; flow:to_client,established; content:"clsid"; nocase;
content:"B64016F3-C9A2-4066-96F0-BD9563314726"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*B64016F3-C9A2-4066-96F0-BD9563314726/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009601;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009601; rev:4;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (33)"; flow:to_client,established; content:"clsid"; nocase;
content:"BB530C63-D9DF-4B49-9439-63453962E598"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*BB530C63-D9DF-4B49-9439-63453962E598/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009602;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009602; rev:4;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (34)"; flow:to_client,established; content:"clsid"; nocase;
content:"C531D9FD-9685-4028-8B68-6E1232079F1E"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*C531D9FD-9685-4028-8B68-6E1232079F1E/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009603;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009603; rev:4;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (35)"; flow:to_client,established; content:"clsid"; nocase;
content:"C5702CCC-9B79-11D3-B654-00C04F79498E"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*C5702CCC-9B79-11D3-B654-00C04F79498E/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009604;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009604; rev:4;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (37)"; flow:to_client,established; content:"clsid"; nocase;
content:"C5702CCE-9B79-11D3-B654-00C04F79498E"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*C5702CCE-9B79-11D3-B654-00C04F79498E/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009606;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009606; rev:2;)
```

```
#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (38)"; flow:to_client,established; content:"clsid"; nocase;
content:"C5702CCF-9B79-11D3-B654-00C04F79498E"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*C5702CCF-9B79-11D3-B654-00C04F79498E/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009607;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009607; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (40)"; flow:to_client,established; content:"clsid"; nocase;
content:"C6B14B32-76AA-4A86-A7AC-5C79AAF58DA7"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*C6B14B32-76AA-4A86-A7AC-5C79AAF58DA7/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009609;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009609; rev:2;)

#by wolvee
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (41)"; flow:to_client,established; content:"clsid"; nocase;
content:"CAAFDD83-CEFC-4E3D-BA03-175F17A24F91"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*CAAFDD83-CEFC-4E3D-BA03-175F17A24F91/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009610;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009610; rev:2;)

#by wolvee
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (42)"; flow:to_client,established; content:"clsid"; nocase;
content:"D02AAC50-027E-11D3-9D8E-00C04F72D980"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*D02AAC50-027E-11D3-9D8E-00C04F72D980/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009611;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009611; rev:2;)

#by wolvee
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS Vulnerable Microsoft Video ActiveX CLSID access (43)"; flow:to_client,established; content:"clsid"; nocase;
content:"F9769A06-7ACA-4E39-9CFB-97BB35F0E77E"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*F9769A06-7ACA-4E39-9CFB-97BB35F0E77E/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009612;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009612; rev:2;)

#by wolvee
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (44)"; flow:to_client,established; content:"clsid"; nocase;
content:"FA7C375B-66A7-4280-879D-FD459C84BB02"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*FA7C375B-66A7-4280-879D-FD459C84BB02/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009613;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009613; rev:2;)

#by wolvee
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (1)"; flow:to_client,established; content:"clsid"; nocase;
content:"011B3619-FE63-4814-8A84-15A194CE9CE3"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*011B3619-FE63-4814-8A84-15A194CE9CE3/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009614;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009614; rev:2;)

#by wolvee
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (2)"; flow:to_client,established; content:"clsid"; nocase;
content:"0149EEDF-D08F-4142-8D73-D23903D21E90"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*0149EEDF-D08F-4142-8D73-D23903D21E90/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009615;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009615; rev:2;)

#by wolvee
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (3)"; flow:to_client,established; content:"clsid"; nocase;
content:"0369B4E5-45B6-11D3-B650-00C04F79498E"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*0369B4E5-45B6-11D3-B650-00C04F79498E/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009616;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009616; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (4)"; flow:to_client,established; content:"clsid"; nocase;
content:"0369B4E6-45B6-11D3-B650-00C04F79498E"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*0369B4E6-45B6-11D3-B650-00C04F79498E/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009617;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009617; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (5)"; flow:to_client,established; content:"clsid"; nocase;
content:"055CB2D7-2969-45CD-914B-76890722F112"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*055CB2D7-2969-45CD-914B-76890722F112/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009618;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009618; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (6)"; flow:to_client,established; content:"clsid"; nocase;
content:"15D6504A-5494-499C-886C-973C9E53B9F1"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*15D6504A-5494-499C-886C-973C9E53B9F1/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009619;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009619; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (7)"; flow:to_client,established; content:"clsid"; nocase;
content:"1BE49F30-0E1B-11D3-9D8E-00C04F72D980"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*1BE49F30-0E1B-11D3-9D8E-00C04F72D980/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009620;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009620; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (8)"; flow:to_client,established; content:"clsid"; nocase;
content:"1C15D484-911D-11D2-B632-00C04F79498E"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*1C15D484-911D-11D2-B632-00C04F79498E/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009621;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009621; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (9)"; flow:to_client,established; content:"clsid"; nocase;
content:"1DF7D126-4050-47F0-A7CF-4C4CA9241333"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*1DF7D126-4050-47F0-A7CF-4C4CA9241333/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009622;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009622; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (10)"; flow:to_client,established; content:"clsid"; nocase;
content:"2C63E4EB-4CEA-41B8-919C-E947EA19A77C"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*2C63E4EB-4CEA-41B8-919C-E947EA19A77C/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009623;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009623; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (11)"; flow:to_client,established; content:"clsid"; nocase;
content:"334125C0-77E5-11D3-B653-00C04F79498E"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*334125C0-77E5-11D3-B653-00C04F79498E/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009624;
```

```
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009624; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (12)"; flow:to_client,established; content:"clsid"; nocase;
content:"37B0353C-A4C8-11D2-B634-00C04F79498E"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*37B0353C-A4C8-11D2-B634-00C04F79498E/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009625;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009625; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (13)"; flow:to_client,established; content:"clsid"; nocase;
content:"37B03543-A4C8-11D2-B634-00C04F79498E"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*37B03543-A4C8-11D2-B634-00C04F79498E/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009626;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009626; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (14)"; flow:to_client,established; content:"clsid"; nocase;
content:"37B03544-A4C8-11D2-B634-00C04F79498E"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*37B03544-A4C8-11D2-B634-00C04F79498E/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009627;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009627; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (15)"; flow:to_client,established; content:"clsid"; nocase;
content:"418008F3-CF67-4668-9628-10DC52BE1D08"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*418008F3-CF67-4668-9628-10DC52BE1D08/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009628;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009628; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (16)"; flow:to_client,established; content:"clsid"; nocase;
content:"4A5869CF-929D-4040-AE03-FCAFC5B9CD42"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*4A5869CF-929D-4040-AE03-FCAFC5B9CD42/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009629;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009629; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (17)"; flow:to_client,established; content:"clsid"; nocase;
content:"577FAA18-4518-445E-8F70-1473F8CF4BA4"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*577FAA18-4518-445E-8F70-1473F8CF4BA4/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009630;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009630; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (18)"; flow:to_client,established; content:"clsid"; nocase;
content:"59DC47A8-116C-11D3-9D8E-00C04F72D980"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*59DC47A8-116C-11D3-9D8E-00C04F72D980/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009631;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009631; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (19)"; flow:to_client,established; content:"clsid"; nocase;
content:"7F9CB14D-48E4-43B6-9346-1AEBC39C64D3"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*7F9CB14D-48E4-43B6-9346-1AEBC39C64D3/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009632;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009632; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (20)"; flow:to_client,established; content:"clsid"; nocase;
content:"823535A0-0318-11D3-9D8E-00C04F72D980"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*823535A0-0318-11D3-9D8E-00C04F72D980/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009633;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009633; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (21)"; flow:to_client,established; content:"clsid"; nocase;
content:"8872FF1B-98FA-4D7A-8D93-C9F1055F85BB"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*8872FF1B-98FA-4D7A-8D93-C9F1055F85BB/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009634;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009634; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (22)"; flow:to_client,established; content:"clsid"; nocase;
content:"8A674B4C-1F63-11D3-B64C-00C04F79498E"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*8A674B4C-1F63-11D3-B64C-00C04F79498E/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009635;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009635; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (23)"; flow:to_client,established; content:"clsid"; nocase;
content:"8A674B4D-1F63-11D3-B64C-00C04F79498E"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*8A674B4D-1F63-11D3-B64C-00C04F79498E/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009636;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009636; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (24)"; flow:to_client,established; content:"clsid"; nocase;
content:"9CD64701-BDF3-4D14-8E03-F12983D86664"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*9CD64701-BDF3-4D14-8E03-F12983D86664/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009638;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009638; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (25)"; flow:to_client,established; content:"clsid"; nocase;
content:"9E77AAC4-35E5-42A1-BDC2-8F3FF399847C"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*9E77AAC4-35E5-42A1-BDC2-8F3FF399847C/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009639;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009639; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (26)"; flow:to_client,established; content:"clsid"; nocase;
content:"A1A2B1C4-0E3A-11D3-9D8E-00C04F72D980"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*A1A2B1C4-0E3A-11D3-9D8E-00C04F72D980/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009640;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009640; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (27)"; flow:to_client,established; content:"clsid"; nocase;
content:"A2E3074E-6C3D-11D3-B653-00C04F79498E"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*A2E3074E-6C3D-11D3-B653-00C04F79498E/si";
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009641;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009641; rev:2;)

#by wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (28)"; flow:to_client,established; content:"clsid"; nocase;
content:"A2E30750-6C3D-11D3-B653-00C04F79498E"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*A2E30750-6C3D-11D3-B653-00C04F79498E/si";
```

```
classtype:web-application-attack; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009642;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MSVidCtl; sid:2009642; rev:2;)

#by Christopher Campesi
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"ET CURRENT_EVENTS Remote SMB2.0 DoS Exploit"; flow:to_server,established; content:"|ff|SMB|72 00 00 00 00 18 53 c8|"; offset:4;
content:!"|00 00|"; within:2; classtype:attempted-dos; reference:url,securityreason.com/exploitalert/7138; reference:url,doc.emergingthreats.net/2009886;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MS_SMB_DOS; sid:2009886; rev:4;)

#by Chandan at Secpod
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Snapshot Viewer for Microsoft Access ActiveX Control Arbitrary File Download (1)"; flow:to_client,established;
content:"F0E42D50-368C-11D0-AD81-00A0C90DC8D9"; nocase; pcre:"/(SnapshotPath|CompressedPath|PrintSnapshot)/i"; pcre:"/(exe|bat|com|dll|ini)/i"; classtype:web-application-attack;
reference:bugtraq,30114; reference:url,downloads.securityfocus.com/vulnerabilities/exploits/30114.html; reference:url,pstgroup.blogspot.com/2008/07/exploitmicrosoft-office-snapshot-
viewer.html; reference:url,doc.emergingthreats.net/bin/view/Main/2008407; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MS_Snapshot; sid:2008407;
rev:4;)

#by Chandan at Secpod
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Snapshot Viewer for Microsoft Access ActiveX Control Arbitrary File Download (2)"; flow:to_client,established;
content:"F0E42D60-368C-11D0-AD81-00A0C90DC8D9"; nocase; pcre:"/(SnapshotPath|CompressedPath|PrintSnapshot)/i"; pcre:"/(exe|bat|com|dll|ini)/i"; classtype:web-application-attack;
reference:bugtraq,30114; reference:url,downloads.securityfocus.com/vulnerabilities/exploits/30114.html; reference:url,pstgroup.blogspot.com/2008/07/exploitmicrosoft-office-snapshot-
viewer.html; reference:url,doc.emergingthreats.net/bin/view/Main/2008408; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MS_Snapshot; sid:2008408;
rev:4;)

#by Chandan at Secpod
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Snapshot Viewer for Microsoft Access ActiveX Control Arbitrary File Download (3)"; flow:to_client,established;
content:"clsid"; nocase; content:"F2175210-368C-11D0-AD81-00A0C90DC8D9"; nocase; pcre:"/(SnapshotPath|CompressedPath|PrintSnapshot)/i"; pcre:"/(exe|bat|com|dll|ini)/i"; classtype:web-
application-attack; reference:bugtraq,30114; reference:url,downloads.securityfocus.com/vulnerabilities/exploits/30114.html; reference:url,pstgroup.blogspot.com/2008/07/exploitmicrosoft-
office-snapshot-viewer.html; reference:url,doc.emergingthreats.net/bin/view/Main/2008409; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_MS_Snapshot; sid:2008409; rev:2;)

#by Eoin Miller
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS Hidden iframe Served by nginx - Likely Hostile Code"; flow:established,to_client; content:"|0d 0a|Server|3a|
nginx"; nocase; offset:15; depth:15; content:"<iframe src="; nocase; content:"style=|22|visibility|3a|hidden|3b 22| width=|22|1|22| height=|22|1|22|></iframe>"; nocase; classtype:bad-
unknown; reference:url,doc.emergingthreats.net/2011714; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malvertising; sid:2011714; rev:4;)

#by Eoin Miller
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS MALVERTISING Adobe Exploited Check-In"; flow:established,to_server; content:"GET "; nocase; depth:4;
uricontent:".php?&&reader_version="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011715; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malvertising; sid:2011715; rev:2;)

#2010-07-14 By Eoin Miller
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS Malvertising drive by kit encountered - Loading..."; flow:established,to_client; content:"HTTP/1"; depth:6;
content:"<html><head></head><body>Loading...<div id=|22|page|22| style=|22|display|3a| none|22|>"; nocase; classtype:bad-unknown; reference:url,doc.emergingthreats.net/2011223;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malvertising; sid:2011223; rev:4;)

#2010-07-14 By Eoin Miller
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS Malvertising drive by kit encountered - bmb cookie"; flow:established,to_client; content:"HTTP/1"; depth:6;
content:"Set-Cookie|3a| bmb="; nocase; classtype:bad-unknown; reference:url,doc.emergingthreats.net/2011222; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malvertising; sid:2011222; rev:2;)

#2010-07-14 By Eoin Miller
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS Malvertising drive by kit collecting browser info"; flow:established,to_server; uricontent:"/plugins.php?
p=appName"; nocase; classtype:bad-unknown; reference:url,doc.emergingthreats.net/2011224; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malvertising; sid:2011224; rev:3;)

#by eoin miller
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS MALVERTISING client requesting drive by - /x/?src="; flow:established,to_server; uricontent:"/x/?src=";
nocase; uricontent:"&o=o"; nocase; classtype:bad-unknown; reference:url,doc.emergingthreats.net/2011230; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malvertising; sid:2011230; rev:3;)

#by eoin miller
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS MALVERTISING client requesting redirect to drive by - .php?c=cust"; flow:established,to_server;
uricontent:".php?c=cust"; nocase; classtype:bad-unknown; reference:url,doc.emergingthreats.net/2011231; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malvertising; sid:2011231; rev:4;)

#by Jamie Blasco of OSSIM based on malwareurl.com data
#174 ocurrences
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS MALWARE Likely Rogue Antivirus Download - Antivirus_21.exe"; flow:established,to_server; content:"GET ";
depth:4; nocase; uricontent:"/download/Antivirus_"; nocase; uricontent:".exe"; nocase; pcre:"/download\x2FAntivirus_\d+\x2Eexe/Ui"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2010050; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; sid:2010050; rev:3;)

#139 ocurrences
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS MALWARE Likely Rogue Antivirus Download - ws.exe"; flow:established,to_server; content:"GET "; depth:4;
nocase; uricontent:"/install/ws.exe"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010051; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; sid:2010051; rev:2;)

#105 ocurrences
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS MALWARE Likely Rogue Antivirus Download - ws.zip"; flow:established,to_server; content:"GET "; nocase;
depth:4; uricontent:"/install/ws.zip"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010052; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; sid:2010052; rev:4;)

#139 ocurrences
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS TROJAN Likely FakeRean Download"; flow:established,to_server; content:"GET "; depth:4; nocase;
uricontent:"/installer/InstallerClean.exe"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010053; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; sid:2010053; rev:2;)

#117
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS TROJAN Likely TDSS Download (codec.exe)"; flow:established,to_server; content:"GET "; depth:4; nocase;
uricontent:"/codec.exe"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010054; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; sid:2010054; rev:3;)

#107
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS TROJAN Likely TDSS Download (pcdef.exe)"; flow:established,to_server; content:"GET "; depth:4; nocase;
uricontent:"/pcdef.exe"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010055; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; sid:2010055; rev:2;)

#93 ocurrences
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS TROJAN Likely TDSS Download (197.exe)"; flow:established,to_server; content:"GET "; depth:4; nocase;
uricontent:"/codec/197.exe"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010056; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; sid:2010056; rev:2;)

#91 ocurrences
```

```
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS MALWARE Likely Rogue Antivirus Download - installpv.exe"; flow:established,to_server; content:"GET ";
depth:4; nocase; uricontent:"/installpv.exe"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010057; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; sid:2010057; rev:2;)

#70 ocurrences
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS MALWARE Likely Unknown Trojan Download"; flow:established,to_server; content:"GET "; depth:4; nocase;
uricontent:"/softwarefortubeview.40009.exe"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010058; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; sid:2010058; rev:2;)

#56 ocurrences
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS TROJAN Likely Unknown Trojan Infostealer Download"; flow:established,to_server; content:"GET "; depth:4;
nocase; uricontent:"/crack.45000.exe"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010059; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; sid:2010059; rev:2;)

#51 ocurrences
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS TROJAN Likely Possible Rogue A/V Win32/FakeXPA Download"; flow:established,to_server; content:"GET ";
depth:4; nocase; uricontent:"/Soft_21.exe"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010060; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; sid:2010060; rev:2;)

#47 ocurrences
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS MALWARE Likely Rogue Antivirus Download - InternetAntivirusPro.exe"; flow:established,to_server;
content:"GET "; depth:4; nocase; uricontent:"/InternetAntivirusPro.exe"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010061;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; sid:2010061; rev:5;)

#30 ocurrences
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS MALWARE Likely Rogue Antivirus Download - AntivirusPlus.exe"; flow:established,to_server; content:"GET ";
depth:4; nocase; uricontent:"/AntivirusPlus.exe"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010062; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; sid:2010062; rev:2;)

#by evilghost 11/2/09
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS MALWARE Potential exploit redirect, in.cgi pepsi"; flow:established,to_server; uricontent:"ts/in.cgi?pepsi";
nocase; pcre:"/ts\/in\.cgi\?pepsi\d+/Ui"; classtype:bad-unknown; reference:url,malwareurl.com; reference:url,doc.emergingthreats.net/2010222; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; sid:2010222; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS MALWARE Potential Malware Download, flash-HQ-plugin.40000.exe"; flow:established,to_server;
uricontent:"flash-"; nocase; uricontent:"-plugin"; nocase; uricontent:".exe"; nocase; pcre:"/flash-[\w-]{0,3}plugin.\d+\.exe/Ui"; classtype:bad-unknown; reference:url,malwareurl.com;
reference:url,doc.emergingthreats.net/2010440; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; sid:2010440; rev:3;)

#by mike cox
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS MALWARE Potential Malware Download, pdf exploit"; flow:established,to_server;
uricontent:"/ssp/files/annonce.pdf"; nocase; classtype:bad-unknown; reference:url,malwareurl.com; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; reference:url,doc.emergingthreats.net/2010444; sid:2010444; rev:2;)

#by mike cox
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS MALWARE Potential Malware Download, loadjavad.php exploit"; flow:established,to_server;
uricontent:"/ssp/loadjavad.php"; nocase; classtype:bad-unknown; reference:url,malwareurl.com; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; reference:url,doc.emergingthreats.net/2010446; sid:2010446; rev:2;)

#by mike cox
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS MALWARE Potential Malware Download, rogue antivirus (IAInstall.exe)"; flow:established,to_server;
uricontent:"/download/IAInstall.exe"; nocase; classtype:bad-unknown; reference:url,malwareurl.com; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; reference:url,doc.emergingthreats.net/2010447; sid:2010447; rev:2;)

#by mike cox
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS MALWARE Potential Malware Download, trojan zbot"; flow:established,to_server;
uricontent:"/globaldirectory/updatetool.exe"; nocase; classtype:bad-unknown; reference:url,malwareurl.com; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; reference:url,doc.emergingthreats.net/2010448; sid:2010448; rev:2;)

#by mike cox
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS MALWARE Potential Malware Download, exploit redirect"; flow:established,to_server; uricontent:"/fkzd/2.htm";
nocase; classtype:bad-unknown; reference:url,malwareurl.com; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads;
reference:url,doc.emergingthreats.net/2010449; sid:2010449; rev:2;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Potential Fake AV GET installer.1.exe"; flow:established,to_server; content:"GET "; depth:4; nocase;
uricontent:"/installer."; nocase; uricontent:".exe"; nocase; pcre:"/\/installer\.\d+\.exe/Ui"; classtype:trojan-activity; reference:url,www.malwareurl.com;
reference:url,doc.emergingthreats.net/2010452; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; sid:2010452; rev:4;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Potential Fake AV GET installer_1.exe"; flow:established,to_server; content:"GET "; depth:4; nocase;
uricontent:"/installer_"; nocase; uricontent:".exe"; nocase; pcre:"/\/installer_\d+\.exe/Ui"; classtype:trojan-activity; reference:url,www.malwareurl.com;
reference:url,doc.emergingthreats.net/2010453; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; sid:2010453; rev:4;)

#by evilghost
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Potential Fake AV Download (download/install.php)"; flow:established,to_server; content:"GET "; nocase; depth:4;
uricontent:"download/install.php"; pcre:"/\x0d\x0aHost\: [a-z\x2e]+(security|virus|pro|anti|scan|mypc|total|protect|check|guard|defend)/i"; classtype:trojan-activity;
reference:url,lists.emergingthreats.net/pipermail/emerging-sigs/2009-December/004891.html; reference:url,malwareurl.com; reference:url,www.malwaredomainlist.com;
reference:url,doc.emergingthreats.net/2010465; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; sid:2010465; rev:2;)

#by mike cox
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS Malwareurl.com - potential oficla download (annonce.pdf)"; flow:established,to_server; content:"GET ";
depth:4; nocase; uricontent:"/ssp/files/annonce.pdf"; nocase; pcre:"/\/ssp\/files\/annonce\.pdf$/Ui"; classtype:trojan-activity; reference:url,www.malwareurl.com;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; reference:url,doc.emergingthreats.net/2010532; sid:2010532; rev:2;)

#by mike cox
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS Malwareurl.com - potential oficla download (loadjavad.php)"; flow:established,to_server; content:"GET ";
depth:4; nocase; uricontent:"/ssp/loadjavad.php"; nocase; pcre:"/\/ssp\/loadjavad\.php$/Ui"; classtype:trojan-activity; reference:url,www.malwareurl.com;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; reference:url,doc.emergingthreats.net/2010534; sid:2010534; rev:2;)

#by waldo kitty
#149 occurances
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS MALWARE Likely Rogue Antivirus Download - Setup_2005.exe"; flow:established,to_server; content:"GET ";
depth:4; nocase; uricontent:"/download/Setup_"; nocase; uricontent:".exe"; nocase; pcre:"/download\x2FSetup_\d+\x2Eexe/Ui"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/xxxxxxx; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; sid:2010684; rev:1;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS Malwareurl - wywg executable download Likely Malware"; flow:established,to_server; content:"GET "; nocase;
depth:4; uricontent:"/wywg/"; nocase; uricontent:".exe"; nocase; pcre:"/\/wywg\/[a-z0-9]{2,5}\/[a-z0-9]+\.exe$/Ui"; classtype:trojan-activity; reference:url,malwareurl.com;
```

```
reference:url,doc.emergingthreats.net/2010716; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; sid:2010716; rev:2;)

#by Mike Cox
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS MALWARE Unknown Malware Download Attempt"; flow:established,to_server; uricontent:"/installer/Installer";
nocase; uricontent:".exe"; nocase; pcre:"/\/\d+\/installer\/Installer(Clean)?\.exe$/Ui"; classtype:bad-unknown; reference:url,malwareurl.com; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Malwareurl_top_downloads; reference:url,doc.emergingthreats.net/2010796; sid:2010796; rev:2;)

#by matt jonkman, re http://www.incidents.org/diary.html?storyid=4405
#Mass File Injection attacks
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS Client Visiting Possibly Compromised Site (HaCKeD By BeLa & BodyguarD)"; flow:established,from_server;
content:"HaCKeD By BeLa & BodyguarD"; content:".js"; classtype:web-application-attack; reference:url,www.incidents.org/diary.html?storyid=4405;
reference:url,doc.emergingthreats.net/bin/view/Main/2008206; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Mass_File_Injections; sid:2008206;
rev:2;)

#by matt jonkman, re http://www.incidents.org/diary.html?storyid=4405
#Mass File Injection attacks
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS Possible File Injection Compromise (HaCKeD By BeLa & BodyguarD)"; flow:established,to_server;
content:"HaCKeD By BeLa & BodyguarD"; classtype:web-application-attack; reference:url,www.incidents.org/diary.html?storyid=4405;
reference:url,doc.emergingthreats.net/bin/view/Main/2008207; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Mass_File_Injections; sid:2008207;
rev:2;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS NACHA/Zeus Phishing Executable Download Attempt"; flow:established,to_server; content:"GET "; depth:4;
content:"nacha.org."; nocase; uricontent:".exe"; nocase; pcre:"/\x0d\x0aHost\: (www\.)?nacha\.org\./i"; classtype:trojan-activity; reference:url,garwarner.blogspot.com/2009/11/newest-
zeus-nacha-electronic-payments.html; reference:url,doc.emergingthreats.net/2010342; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Nacha;
sid:2010342; rev:3;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS NeoSploit Exploit Kit Java exploit drive-by host likely infected (kav)"; flow:established,to_server;
uricontent:"/kav"; nocase; content:"|0d 0a|accept-encoding|3a| pack200-gzip,gzip|0d 0a|"; nocase; content:"|0d 0a|content-type|3a| application/x-java-archive|0d 0a|"; nocase;
content:!"|0d 0a|Referer|3a| "; nocase; content:"|0d 0a|User-Agent|3a| Mozilla"; nocase; content:" Java/"; nocase; within:50; classtype:trojan-activity;
reference:url,www.malwaredomainlist.com/forums/index.php?action=printpage%3btopic=3781.0; reference:url,doc.emergingthreats.net/2010870; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Neosploit; sid:2010870; rev:5;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS NeoSploit Exploit Kit Java exploit drive-by host likely infected (nte)"; flow:established,to_server;
uricontent:"/nte/"; nocase; content:"|0d 0a|accept-encoding|3a| pack200-gzip,gzip|0d 0a|"; nocase; content:"|0d 0a|content-type|3a| application/x-java-archive|0d 0a|"; nocase;
content:!"|0d 0a|Referer|3a| "; nocase; content:"|0d 0a|User-Agent|3a| Mozilla"; nocase; content:" Java/"; nocase; within:50; classtype:trojan-activity;
reference:url,www.malwaredomainlist.com/forums/index.php?action=printpage%3btopic=3781.0; reference:url,doc.emergingthreats.net/2010871; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Neosploit; sid:2010871; rev:5;)

#by mike cox
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS Fake AV Related CSS Download"; flow:established,from_server; content:"#hello_nod32_guys_how_u_doing";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011670; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Nod32;
sid:2011670; rev:2;)

#by Nate Hausrath
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS Pinkslipbot Trojan Downloader"; flow:to_server,established; uricontent:"/jl/jloader.pl?u="; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010742; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Pinkslipbot; sid:2010742;
rev:2;)

#by Paul Dokas. Testing this out for a bit..., modified by kevin ross
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS Nginx Serving PDF - Possible hostile content (PDF)"; flow:established,from_server; content:"|0d
0a|Server|3a| nginx"; depth:300; content:"PDF-"; nocase; within:300; threshold:type limit, seconds 60, count 10, track by_src; classtype:bad-unknown;
reference:url,doc.emergingthreats.net/bin/view/Main/2009076; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Possible_Malicious_PDF; sid:2009076;
rev:5;)

##Jaime Blasco Alienvault VRT
#PSYB0T related Activity
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS Psyb0t Code Download"; flow:established,to_server; uricontent:"/udhcpc.env"; nocase; classtype:trojan-
activity; reference:url,www.adam.com.au/bogaurd/PSYB0T.pdf; reference:url,doc.emergingthreats.net/2009170; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Psybot; sid:2009170; rev:2;)

##Jaime Blasco Alienvault VRT
#PSYB0T related Activity
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET CURRENT_EVENTS Psyb0t Bot Nick"; flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK [NIP]-"; nocase;
classtype:trojan-activity; reference:url,www.adam.com.au/bogaurd/PSYB0T.pdf; reference:url,doc.emergingthreats.net/2009171; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Psybot; sid:2009171; rev:3;)

##Jaime Blasco Alienvault VRT
#PSYB0T related Activity
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET CURRENT_EVENTS Psyb0t joining an IRC Channel"; flow:established,to_server; flowbits:isset,is_proto_irc; content:"JOIN #mipsel";
classtype:trojan-activity; reference:url,www.adam.com.au/bogaurd/PSYB0T.pdf; reference:url,doc.emergingthreats.net/2009172; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Psybot; sid:2009172; rev:2;)

#by Jeffrey Brown. re 308c6885573ce652bab37c739f52cb19
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS New Malware Information Post"; flow:to_server,established; content:"POST "; nocase; depth:5; content:"|0d
0a|Pragma|3a| no-cache|0d 0a 0d 0a|"; content:"|C9 78 C7 02 69 06 7E 34 78 17|"; distance:4; within:14; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009092;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Rusibank.com; sid:2009092; rev:4;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS TROJAN SEO HTTP REFERER landing capture rewrite, likely Fake AV"; flow:established,to_server; content:"GET
"; depth:4; nocase; content:"|0d 0a|Referer|3a| "; nocase; content:"search?"; nocase; within:50; content:"q="; nocase; within:100; uricontent:".com"; nocase; pcre:"/\/[a-z]+\/[a-z0-9]
{120,}\/[a-z0-9]+\/.+\.com$/U"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011066; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_SEO_FakeAV; sid:2011066; rev:4;)

#by Michael Sconzo of ERCOT
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS Iframe in Purported Image Download (jpeg) - Likely SQL Injection Attacks Related";
flow:established,from_server; content:"|0d 0a|content-type|3a| "; nocase; content:" image/jpeg"; nocase; distance:0; within:30; content:"<iframe"; nocase; distance:0; pcre:"/content-
type\:\s+image\/jpeg/im"; pcre:"/<iframe.*?src.*?>.*?<\/iframe>/im"; classtype:web-application-attack; reference:url,doc.emergingthreats.net/bin/view/Main/2008313;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_SQL_Injections; sid:2008313; rev:4;)

#by Michael Sconzo of ERCOT
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS Iframe in Purported Image Download (gif) - Likely SQL Injection Attacks Related";
flow:established,from_server; content:"|0d 0a|content-type|3a| "; nocase; content:" image/gif"; nocase; distance:0; within:30; content:"<iframe"; nocase; distance:0; pcre:"/content-
type\:\s+image\/gif/im"; pcre:"/<iframe.*?src.*?>.*?<\/iframe>/im"; classtype:web-application-attack; reference:url,doc.emergingthreats.net/bin/view/Main/2008314;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_SQL_Injections; sid:2008314; rev:4;)

#by Michael Sconzo of ERCOT
#
```

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS Iframe in Purported Image Download (png) - Likely SQL Injection Attacks Related";
flow:established,from_server; content:"|0d 0a|content-type|3a| "; nocase; content:" image/png"; nocase; distance:0; within:30; content:"<iframe"; nocase; distance:0; pcre:"/content-
type\:\s+image\/png/im"; pcre:"/<iframe.*?src.*?>.*?<\/iframe>/im"; classtype:web-application-attack; reference:url,doc.emergingthreats.net/bin/view/Main/2008315;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_SQL_Injections; sid:2008315; rev:4;)

#Greg Martin
#disabling, needs deleting in june or so 2010
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET DELETED ASPROX Infected Site - ngg.js Request"; flow:established,to_server; uricontent:"/ngg.js"; nocase;
content:!"nextgen-gallery"; nocase; classtype:trojan-activity; reference:url,infosec20.blogspot.com/; reference:url,doc.emergingthreats.net/bin/view/Main/2008373;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_SQL_Injections; sid:2008373; rev:4;)

#by Jack Pepper
#
#alert tcp $HOME_NET $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET CURRENT_EVENTS Possible ASPROX Hostile JS Being Served by a Local Webserver (/ngg.js)"; flow:established,from_server;
content:"<script src=http|3a|//"; nocase; content:!"nextgen-gallery"; nocase; within:15; content:"/ngg.js>"; nocase; within:50; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2008387; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_SQL_Injections;
reference:url,infosec20.blogspot.com/2008/07/asprox-payload-morphed.html; sid:2008387; rev:6;)

#by Jack Pepper
#
#alert tcp $HOME_NET $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET CURRENT_EVENTS Possible ASPROX Hostile JS Being Served by a Local Webserver (/b.js)"; flow:established,from_server;
content:"<script src=http|3a|//"; nocase; content:"/b.js>"; nocase; within:50; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008388;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_SQL_Injections; sid:2008388; rev:5;)

#by sp0ok3r
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS Skype Easybits Extras Manager - Exploit"; flow:established,from_server; content:"gygte"; nocase;
content:"gygte"; nocase; distance:0; classtype:trojan-activity; reference:url,www.m86security.com/labs/traceitem.asp?article=1347; reference:url,doc.emergingthreats.net/2011680;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Skype; sid:2011680; rev:4;)

#by Pedro Marinho, re 58816f781154bda381fdcb1e3fab7bdd
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Unnamed - kuaiche.com related"; flow:established,to_server; content:"GET "; depth:4;
uricontent:"/config/fgun_install_"; content:"|0d 0a|User-Agent|3a| NSI SDL/1.2 (Mozilla)|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008359;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Unknown_trojan; sid:2008359; rev:4;)

#different trojan, by marcus at unsober
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Unknown Keylogger checkin"; flow:established; content:"GET "; depth:4; uricontent:"?mail=";
uricontent:"subject=Keylogger"; uricontent:"&body="; content:"|0d 0a|User-Agent|3a| Mozilla/4.0 (compatible\; MSIE 6.0\; Windows NT 5.1\; SV1)"; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2008368; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Unknown_trojan; sid:2008368; rev:3;)

#Unknown handshake over SMTP discovered by Thierry Chich and reported on mail list. Added by Frank Knobbe 2008-09-17.
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN Suspicious SMTP handshake outbound"; flow:established,to_server; content:"001 RUTHERE"; depth:11; classtype:unknown;
reference:url,doc.emergingthreats.net/bin/view/Main/2008562; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Unknown_trojan; sid:2008562; rev:3;)

#Unknown handshake over SMTP discovered by Thierry Chich and reported on mail list. Added by Frank Knobbe 2008-09-17.
#
#alert tcp $EXTERNAL_NET 25 -> $HOME_NET any (msg:"ET TROJAN Suspicious SMTP handshake reply"; flow:established,from_server; content:"701 IMHERE"; depth:10; classtype:unknown;
reference:url,doc.emergingthreats.net/bin/view/Main/2008563; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Unknown_trojan; sid:2008563; rev:3;)

#by Victor Julien
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET DELETED Unknown Keepalive out"; flow:established,to_server; dsize:5; content:"|17 24 1B 00 00|";
flowbits:isnotset,ET.teamviewerkeepaliveout; flowbits:set,ET.unknownkeepaliveup; flowbits:noalert; classtype:unknown; reference:url,doc.emergingthreats.net/bin/view/Main/2008779;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Unknown_trojan3; sid:2008779; rev:4;)

#by Victor Julien
#
##alert tcp $EXTERNAL_NET 1024: -> $HOME_NET any (msg:"ET DELETED Unknown Keepalive in"; flow:established,to_client; dsize:5; content:"|17 24 1B 00 00|";
flowbits:isnotset,ET.teamviewerkeepaliveout; flowbits:isset,ET.unknownkeepaliveup; classtype:unknown; reference:url,doc.emergingthreats.net/bin/view/Main/2008780;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Unknown_trojan3; sid:2008780; rev:4;)

#by David Wharton
#
alert tcp any $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Windows Help Center Arbitrary Command Execution Exploit Attempt"; flow:established,from_server; content:"hcp|3a|//"; nocase;
content:"<script "; nocase; distance:0; content:"defer"; nocase; distance:0; content:"unescape"; nocase; distance:0; pcre:"/src\s*=\s*[\x22\x27]?hcp\x3a\x2f\x2F[^\n]*
<script\s*defer[^\n]*unescape/i"; classtype:misc-attack; reference:url,www.exploit-db.com/exploits/13808/; reference:url,doc.emergingthreats.net/2011173;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_WinHelp; sid:2011173; rev:6;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS Executable requested from /wp-content/languages"; flow:established,to_server; uricontent:"/wp-
content/languages/"; nocase; uricontent:".exe"; nocase; classtype:trojan-activity; reference:url,www.malwareurl.com; reference:url,doc.emergingthreats.net/2011220;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Wordpress; sid:2011220; rev:2;)

#by jerry
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS Zbot update (av-i386-daily.zip)"; flow:established,to_server; uricontent:"av_base/av-i386-daily.zip";
nocase; classtype:trojan-activity; reference:url,www.threatexpert.com/report.aspx?md5=06e69bfb6fffa17c4fc1e23af71b345c; reference:url,doc.emergingthreats.net/2010565;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Zeus; sid:2010568; rev:3;)

#by jerry
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS Zbot update (av_base/pay.php)"; flow:established,to_server; uricontent:"av_base/pay.php"; nocase;
classtype:trojan-activity; reference:url,www.threatexpert.com/report.aspx?md5=06e69bfb6fffa17c4fc1e23af71b345c; reference:url,doc.emergingthreats.net/2010566;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Zeus; sid:2010566; rev:3;)

#by jerry
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS Zbot update (av_base/ip.php)"; flow:established,to_server; uricontent:"av_base/ip.php"; nocase;
classtype:trojan-activity; reference:url,www.threatexpert.com/report.aspx?md5=06e69bfb6fffa17c4fc1e23af71b345c; reference:url,doc.emergingthreats.net/2010567;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Zeus; sid:2010567; rev:3;)

#by spooker
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS Zeus Bot / Zbot Checkin (/us01d/in.php)"; flow:established,to_server; content:"GET "; nocase; depth:4;
uricontent:"/us01d/in.php"; nocase; classtype:trojan-activity; reference:url,garwarner.blogspot.com/2010/01/american-bankers-association-version-of.html;
reference:url,doc.emergingthreats.net/2010729; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_Zeus; sid:2010729; rev:4;)

#by anon 4
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS FakeAlert/FraudPack/FakeAV/Guzz/Dload/Vobfus/ZPack Encrypted GIF download 1"; flow:established,to_server;
content:"GET "; depth:4; uricontent:"/perce/"; nocase; uricontent:"/qwerce.gif"; nocase; classtype:trojan-activity;
reference:url,threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_AGENT.GUZZ&VSect=T; reference:url,www.threatexpert.com/threats/trojan-fraudpack-sd6.html;
reference:url,vil.nai.com/vil/content/v_157489.htm; reference:url,blog.threatfire.com/2009/06/streamviewers-gif-images-embedded-with-encrypted-malware.html;
reference:url,doc.emergingthreats.net/2010231; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_fakealerts; sid:2010231; rev:5;)

#by anon 4
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS FakeAlert/FraudPack/FakeAV/Guzz/Dload/Vobfus/ZPack Encrypted GIF download 2"; flow:established,to_server;
content:"GET "; depth:4; uricontent:"/werber/"; nocase; uricontent:"/217.gif"; nocase; classtype:trojan-activity;
reference:url,threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_AGENT.GUZZ&VSect=T; reference:url,vil.nai.com/vil/content/v_157489.htm;
reference:url,threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_DLOAD.TID&VSect=T; reference:url,blog.threatfire.com/2009/06/streamviewers-gif-images-embedded-with-
encrypted-malware.html; reference:url,doc.emergingthreats.net/2010232; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_fakealerts; sid:2010232;
rev:4;)

#by anon 4
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS FakeAlert/FraudPack/FakeAV/Guzz/Dload/Vobfus/ZPack Encrypted GIF download 3"; flow:established,to_server;
content:"GET "; depth:4;  uricontent:"/item/"; nocase; uricontent:"/titem.gif"; nocase; classtype:trojan-activity;
reference:url,threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_AGENT.GUZZ&VSect=T; reference:url,vil.nai.com/vil/content/v_157489.htm;
reference:url,blog.threatfire.com/2009/06/streamviewers-gif-images-embedded-with-encrypted-malware.html; reference:url,doc.emergingthreats.net/2010233;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_fakealerts; sid:2010233; rev:4;)

#by anon 4
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS FakeAlert/FraudPack/FakeAV/Guzz/Dload/Vobfus/ZPack HTTP Post 1"; flow:established,to_server; content:"POST
"; depth:5; uricontent:"/senm.php?data="; nocase; content:"data="; nocase; classtype:trojan-activity; reference:url,threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?
VName=TROJ_AGENT.GUZZ&VSect=T; reference:url,www.threatexpert.com/report.aspx?md5=7ca709f154e6abc678fbc4df8a3256b6; reference:url,www.threatexpert.com/threats/trojan-fraudpack-sd6.html;
reference:url,doc.emergingthreats.net/2010234; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_fakealerts; sid:2010234; rev:4;)

#by anon 4
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS FakeAlert/FraudPack/FakeAV/Guzz/Dload/Vobfus/ZPack HTTP Post 2"; flow:established,to_server; content:"POST
"; depth:5; uricontent:"/perce/"; nocase; uricontent:"/qwerce.gif"; nocase; content:"data="; nocase; classtype:trojan-activity;
reference:url,threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_AGENT.GUZZ&VSect=T; reference:url,www.threatexpert.com/threats/trojan-fraudpack-sd6.html;
reference:url,vil.nai.com/vil/content/v_157489.htm; reference:url,doc.emergingthreats.net/2010235; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_fakealerts; sid:2010235; rev:4;)

#by anon 4
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS FakeAlert/FraudPack/FakeAV/Guzz/Dload/Vobfus/ZPack HTTP Post 3"; flow:established,to_server; content:"POST
"; depth:5; uricontent:"/werber/"; nocase; uricontent:"/217.gif"; nocase; content:"data="; nocase; classtype:trojan-activity;
reference:url,threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_AGENT.GUZZ&VSect=T; reference:url,vil.nai.com/vil/content/v_157489.htm;
reference:url,threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_DLOAD.TID&VSect=T; reference:url,doc.emergingthreats.net/2010236;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_fakealerts; sid:2010236; rev:4;)

#by anon 4
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS FakeAlert/FraudPack/FakeAV/Guzz/Dload/Vobfus/ZPack HTTP Post 4"; flow:established,to_server; content:"POST
"; depth:5; uricontent:"/item/"; nocase; uricontent:"/titem.gif"; nocase; content:"data="; nocase; classtype:trojan-activity;
reference:url,threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_AGENT.GUZZ&VSect=T; reference:url,vil.nai.com/vil/content/v_157489.htm;
reference:url,doc.emergingthreats.net/2010237; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_fakealerts; sid:2010237; rev:4;)

#by anon 4
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS FakeAlert/FraudPack/FakeAV/Guzz/Dload/Vobfus/ZPack HTTP Post 5"; flow:established,to_server; content:"POST
"; depth:5; uricontent:"/report.php?data="; nocase; content:"data="; nocase; classtype:trojan-activity; reference:url,threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?
VName=TROJ_AGENT.GUZZ&VSect=T; reference:url,vil.nai.com/vil/content/v_157489.htm; reference:url,threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_DLOAD.TID&VSect=T;
reference:url,doc.emergingthreats.net/2010238; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_fakealerts; sid:2010238; rev:4;)

#by anon 4
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS FakeAlert/FraudPack/FakeAV/Guzz/Dload/Vobfus/ZPack HTTP Post 6"; flow:established,to_server; content:"POST
"; depth:5; uricontent:"/arrows/"; nocase; uricontent:"/arrow_up.gif"; nocase; content:"data="; nocase; classtype:trojan-activity;
reference:url,threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_AGENT.GUZZ&VSect=T; reference:url,vil.nai.com/vil/content/v_157489.htm;
reference:url,threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_DLOAD.TID&VSect=T; reference:url,www.threatexpert.com/report.aspx?
md5=316fd88ac18d21889b1dbf9b979c1959; reference:url,doc.emergingthreats.net/2010239; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_fakealerts;
sid:2010239; rev:4;)

#by matt jonkman
#
alert udp $HOME_NET any -> $DNS_SERVERS 53 (msg:"ET CURRENT_EVENTS Infected System Looking up chr.santa-inbox.com CnC Server"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10;
offset:2; content:"|03|chr|0b|santa-inbox|03|com"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008531;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/CURRENT_EVENTS/CURRENT_santa-inbox.com; sid:2008531; rev:3;)

#Submitted by Cody Hatch
#
alert udp $EXTERNAL_NET any -> $HOME_NET 514 (msg:"ET DOS Cisco 514 UDP flood DoS"; content:"|25 25 25 25 25 58 58 25 25 25 25 25|"; classtype: attempted-dos;
reference:url,www.cisco.com/warp/public/707/IOS-cbac-dynacl-pub.shtml; reference:url,doc.emergingthreats.net/bin/view/Main/2000010; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/DOS/DOS_Cisco_514_UDP_DoS; sid:2000010; rev:11;)

#Submitted by Cody Hatch
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 23 (msg:"ET DOS Catalyst memory leak attack"; flow: to_server,established; content:"|41 41 41 0a|"; depth: 20; classtype: attempted-dos;
reference:url,www.cisco.com/en/US/products/products_security_advisory09186a00800b138e.shtml; reference:url,doc.emergingthreats.net/bin/view/Main/2000011;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_Cisco_Catalyst_memory_leak_attack; sid:2000011; rev:8;)

#submitted by Cody Hatch
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET DOS Cisco Router HTTP DoS"; flow: to_server,established; uricontent:"/%%"; classtype: attempted-dos;
reference:url,www.cisco.com/warp/public/707/cisco-sn-20040326-exploits.shtml; reference:url,doc.emergingthreats.net/bin/view/Main/2000006; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/DOS/DOS_Cisco_Router_HTTP_DOS; sid:2000006; rev:11;)

#By Blake Hartstein at Demarc
#
alert udp $EXTERNAL_NET any -> $HOME_NET 162 (msg:"ET SNMP Cisco Non-Trap PDU request on SNMPv1 trap port"; content:"|02 01 00|"; depth:3; byte_test:1,>,159,8,relative; byte_test:1,
<,164,8,relative; classtype:attempted-dos; reference:cve,2004-0714; reference:bugtraq,10186; reference:url,doc.emergingthreats.net/bin/view/Main/2002880;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_Cisco_SNMP; sid:2002880; rev:8;)

#By Blake Hartstein at Demarc
#
alert udp $EXTERNAL_NET any -> $HOME_NET 162 (msg:"ET SNMP Cisco Non-Trap PDU request on SNMPv2 trap port"; content:"|02 01|"; depth:2; byte_test:1,>,0,0,relative; byte_test:1,
<,3,0,relative; byte_test:1,>,159,9,relative; byte_test:1,<,167,9,relative; classtype:attempted-dos; reference:cve,2004-0714; reference:bugtraq,10186;
reference:url,doc.emergingthreats.net/bin/view/Main/2002881; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_Cisco_SNMP; sid:2002881; rev:8;)

#By Blake Hartstein at Demarc
#
alert udp $EXTERNAL_NET any -> $HOME_NET 162 (msg:"ET SNMP Cisco Non-Trap PDU request on SNMPv3 trap port"; content:"|02 01 03|"; depth:3; byte_test:1,>,159,43,relative; byte_test:1,
<,167,43,relative; classtype:attempted-dos; reference:cve,2004-0714; reference:bugtraq,10186; reference:url,doc.emergingthreats.net/bin/view/Main/2002882;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_Cisco_SNMP; sid:2002882; rev:7;)

#By Blake Hartstein at Demarc
#
alert udp $EXTERNAL_NET !161 -> $HOME_NET 49152: (msg:"ET SNMP Cisco Non-Trap PDU request on SNMPv1 random port"; content:"|02 01 00|"; depth:3; byte_test:1,>,159,8,relative;
byte_test:1,<,164,8,relative; classtype:attempted-dos; reference:cve,2004-0714; reference:bugtraq,10186; reference:url,doc.emergingthreats.net/bin/view/Main/2002926;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_Cisco_SNMP; sid:2002926; rev:7;)

#By Blake Hartstein at Demarc
#
alert udp $EXTERNAL_NET !161 -> $HOME_NET 49152: (msg:"ET SNMP Cisco Non-Trap PDU request on SNMPv2 random port"; content:"|02 01|"; depth:2; byte_test:1,>,0,0,relative; byte_test:1,
<,3,0,relative; byte_test:1,>,159,9,relative; byte_test:1,<,167,9,relative; classtype:attempted-dos; reference:cve,2004-0714; reference:bugtraq,10186;
reference:url,doc.emergingthreats.net/bin/view/Main/2002927; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_Cisco_SNMP; sid:2002927; rev:7;)

#By Blake Hartstein at Demarc
#
alert udp $EXTERNAL_NET !161 -> $HOME_NET 49152: (msg:"ET SNMP Cisco Non-Trap PDU request on SNMPv3 random port"; content:"|02 01 03|"; depth:3; byte_test:1,>,159,43,relative;
byte_test:1,<,167,43,relative; classtype:attempted-dos; reference:cve,2004-0714; reference:bugtraq,10186; reference:url,doc.emergingthreats.net/bin/view/Main/2002928;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_Cisco_SNMP; sid:2002928; rev:7;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET DOS Cisco 4200 Wireless Lan Controller Long Authorisation Denial of Service Attempt"; flow:to_server,established;
content:"GET "; depth:4; nocase; uricontent:"/screens/frameset.html"; nocase; content:"Authorization|3A 20|Basic"; nocase; content:!"|0a|"; distance:2; within:118;
isdataat:120,relative; pcre:"/\x2Fscreens\x2Fframeset\x2Ehtml.+Authorization\x3A Basic.{120}/msi"; classtype:attempted-dos; reference:url,www.securityfocus.com/bid/35805;
reference:url,www.cisco.com/warp/public/707/cisco-amb-20090727-wlc.shtml; reference:cve,2009-1164; reference:url,doc.emergingthreats.net/2010674;
```

```
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_Cisco_WLAN; sid:2010674; rev:3;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 6014 (msg:"ET DOS IBM DB2 kuddb2 Remote Denial of Service Attempt"; flow:established,to_server; content:"|00 05 03 31 41|"; classtype:attempted-
dos; reference:url,www.securityfocus.com/bid/38018; reference:url,intevydis.blogspot.com/2010/01/ibm-db2-97-kuddb2-dos.html; reference:url,doc.emergingthreats.net/2010755;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_DB2; sid:2010755; rev:4;)

#by Blake Hartstein of Demarc
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 2049 (msg:"ET DOS FreeBSD NFS RPC Kernel Panic"; flow:to_server,established; content:"|00 01 86 a5|"; offset:16; depth:4; content:"|00 00 00
01|"; distance:4; within:4; content:"|00 00 00 00|"; distance:8; depth:4; content:"|00 00 00 00 00 00|"; distance:0; depth:6; classtype:attempted-dos; reference:cve,2006-0900;
reference:bugtraq,19017; reference:url,doc.emergingthreats.net/bin/view/Main/2002853; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_FreeBSD; sid:2002853; rev:3;)

#by Blake Hartstein of Demarc
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 1755 (msg:"ET DOS Microsoft Streaming Server Malformed Request"; flow:established,to_server; content:"MSB "; depth:4; content:"|06 01 07 00 24
00 00 40 00 00 00 00 00 00 01 00 00 00|"; distance:0; within:18; classtype:attempted-dos; reference:bugtraq,1282; reference:url,www.microsoft.com/technet/security/bulletin/ms00-
038.mspx; reference:url,doc.emergingthreats.net/bin/view/Main/2002843; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_MS00-038; sid:2002843; rev:4;)

#From Erik Fichtner:
#hit on pmtu frames with next-hop mtu not 0 (old RFC shortcut) and (added this so the sig wouldn't trigger missing reference:url, search errors)
#below a sane value, eg 576 bytes. Adjust to taste.
#true RFC791 min = 68, true end-to-end pmtu compatble min = 132.
#real world might even go as high as 1100 bytes min. YMMV.
#Updated to be 6 in the byte test as per Shane Castle
#
#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET DOS ICMP Path MTU lowered below acceptable threshold"; itype: 3; icode: 4; byte_test:2,<,576,6; byte_test:2,!=,0,7; classtype:
denial-of-service; reference:cve,CAN-2004-1060; reference:url,www.microsoft.com/technet/security/bulletin/MS05-019.mspx; reference:url,isc.sans.org/diary.php?date=2005-04-12;
reference:url,doc.emergingthreats.net/bin/view/Main/2001882; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_MS05-019; sid:2001882; rev:10;)

#Submitted by Chris Norton
#
#alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 1433 (msg:"ET DOS Possible Microsoft SQL Server Remote Denial Of Service Attempt"; flow: established,to_server; content:"|10 00 00 10 cc|";
depth:5; classtype: attempted-dos; reference:bugtraq,11265; reference:url,doc.emergingthreats.net/bin/view/Main/2001366; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/DOS/DOS_MSSQL_DOS; sid:2001366; rev:10;)

#By Blake Hartstein at Demarc
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"ET DOS NetrWkstaUserEnum Request with large Preferred Max Len"; flow:established,to_server; content:"|ff|SMB"; content:"|10 00 00
00|"; distance:0; content:"|02 00|"; distance:14; depth:2; byte_jump:4,12,relative,little,multiplier 2; content:"|00 00 00 00 00 00 00 00|"; distance:12; depth:8;
byte_test:4,>,2,0,relative; classtype:attempted-dos; reference:cve,2006-6723; reference:url,doc.emergingthreats.net/bin/view/Main/2003236; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/DOS/DOS_MS_SMB; sid:2003236; rev:3;)

#Erik Fichtner
#
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"ET DOS Excessive SMTP MAIL-FROM DDoS"; flow: to_server, established; content:"MAIL FROM|3a|"; nocase; window: 0; id:0; threshold:
type limit, track by_src, count 30, seconds 60; classtype: denial-of-service; reference:url,doc.emergingthreats.net/bin/view/Main/2001795; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/DOS/DOS_Mail-From; sid:2001795; rev:9;)

#By Blake Hartstein at Demarc
#
##alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET DELETED HELO Non-Displayable Characters MailEnable Denial of Service"; flow:established,to_server; content:"HELO "; nocase;
depth:60; pcre:"/^[^\n]*[\x00-\x08\x0e-\x1f]/R"; classtype:attempted-dos; reference:cve,2006-3277; reference:bugtraq,18630; reference:url,doc.emergingthreats.net/bin/view/Main/2002998;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_MailEnable; sid:2002998; rev:7;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 3306 (msg:"ET DOS Possible MYSQL GeomFromWKB() function Denial Of Service Attempt"; flow:to_server,established; content:"SELECT"; nocase;
content:"geometrycollectionfromwkb"; distance:0; nocase; pcre:"/SELECT.+geometrycollectionfromwkb/si"; classtype:attempted-dos; reference:url,www.securityfocus.com/bid/37297/info;
reference:url,marc.info/?l=oss-security&m=125881733826437&w=2; reference:url,downloads.securityfocus.com/vulnerabilities/exploits/37297.txt; reference:cve,2009-4019;
reference:url,doc.emergingthreats.net/2010491; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_Mysql; sid:2010491; rev:2;)

#temp disabled till we figure out all options
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 3306 (msg:"ET DOS Possible MYSQL SELECT WHERE to User Variable Denial Of Service Attempt"; flow:to_server,established; content:"SELECT";
nocase; content:"WHERE"; distance:0; nocase; content:"SELECT"; nocase; content:"INTO"; distance:0; nocase; content:"|60|"; within:50; content:"|60|";
pcre:"/SELECT.+WHERE.+SELECT.+\x60/si"; classtype:attempted-dos; reference:url,www.securityfocus.com/bid/37297/info; reference:url,marc.info/?l=oss-security&m=125881733826437&w=2;
reference:url,downloads.securityfocus.com/vulnerabilities/exploits/37297-2.txt; reference:cve,2009-4019; reference:url,doc.emergingthreats.net/2010492;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_Mysql; sid:2010492; rev:3;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 3306 (msg:"ET DOS Possible MySQL ALTER DATABASE Denial Of Service Attempt"; flow:established,to_server; content:"ALTER "; nocase;
content:"DATABASE"; nocase; within:12; content:"|22|."; distance:0; content:"UPGRADE "; nocase; distance:0; content:"DATA"; nocase; within:8;
pcre:"/ALTER.+DATABASE.+\x22\x2E(\x22|\x2E\x22|\x2E\x2E\x2F\x22).+UPGRADE.+DATA/si"; classtype:attempted-dos; reference:url,securitytracker.com/alerts/2010/Jun/1024160.html;
reference:url,dev.mysql.com/doc/refman/5.1/en/alter-database.html; reference:cve,2010-2008; reference:url,doc.emergingthreats.net/2011761; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/DOS/DOS_Mysql; sid:2011761; rev:2;)

#by kevin ross, mike cox and joel esler
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET DOS Netgear DG632 Web Management Denial Of Service Attempt"; flow:established,to_server; content:"POST "; nocase; depth:5;
uricontent:"/cgi-bin/firmwarecfg"; nocase; classtype:attempted-dos; reference:url, securitytracker.com/alerts/2009/Jun/1022403.html; reference:cve,2009-2256;
reference:url,doc.emergingthreats.net/2010554; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_Netgear; sid:2010554; rev:2;)

#by Bart Roos
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack"; flags:A; window:0; threshold: type threshold, track
by_src,count 100, seconds 60; classtype:attempted-dos; reference:url,doc.emergingthreats.net/2009414; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_Nkiller2;
sid:2009414; rev:3;)

#by matt jonkman and waldo kitty
#
alert udp $EXTERNAL_NET 123 -> $HOME_NET 123 (msg:"ET DOS Potential Inbound NTP denial-of-service attempt (repeated mode 7 request)"; dsize:1; content:"|17|"; threshold:type limit,
count 1, seconds 60, track by_src; classtype:attempted-dos; reference:url,www.kb.cert.org/vuls/id/568372; reference:cve,2009-3563; reference:url,doc.emergingthreats.net/2010486;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_Ntp; sid:2010486; rev:2;)

#by matt jonkman and waldo kitty
#
alert udp $EXTERNAL_NET 123 -> $HOME_NET 123 (msg:"ET DOS Potential Inbound NTP denial-of-service attempt (repeated mode 7 reply)"; dsize:4; content:"|97 00 00 00|"; threshold:type
limit, count 1, seconds 60, track by_src; classtype:attempted-dos; reference:url,www.kb.cert.org/vuls/id/568372; reference:cve,2009-3563; reference:url,doc.emergingthreats.net/2010487;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_Ntp; sid:2010487; rev:2;)

#by matt jonkman and waldo kitty
#
alert udp $HOME_NET 123 -> $EXTERNAL_NET 123 (msg:"ET DOS Potential Inbound NTP denial-of-service attempt (repeated mode 7 request)"; dsize:1; content:"|17|"; threshold:type limit,
count 1, seconds 60, track by_src; classtype:attempted-dos; reference:url,www.kb.cert.org/vuls/id/568372; reference:cve,2009-3563; reference:url,doc.emergingthreats.net/2010488;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_Ntp; sid:2010488; rev:2;)

#by matt jonkman and waldo kitty
#
alert udp $HOME_NET 123 -> $EXTERNAL_NET 123 (msg:"ET DOS Potential Inbound NTP denial-of-service attempt (repeated mode 7 reply)"; dsize:4; content:"|97 00 00 00|"; threshold:type
limit, count 1, seconds 60, track by_src; classtype:attempted-dos; reference:url,www.kb.cert.org/vuls/id/568372; reference:cve,2009-3563; reference:url,doc.emergingthreats.net/2010489;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_Ntp; sid:2010489; rev:2;)

#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 443 (msg:"ET DOS SSL Bomb DoS Attempt"; flow:to_server,established; content:"|16 03 00|"; offset:0; depth:3; content:"|01|"; within:1;
distance:2; byte_jump:1,37,relative,align; byte_test:2,>,255,0,relative; classtype:attempted-dos; reference:cve,CAN-2004-0120;
reference:url,www.microsoft.com/technet/security/bulletin/MS04-011.mspx; reference:url,doc.emergingthreats.net/bin/view/Main/2000016; reference:url,www.emergingthreats.net/cgi-
```

```
bin/cvsweb.cgi/sigs/DOS/DOS_SSL_Bomb_Attempt; sid:2000016; rev:7;)

#by Kevin Ross
#
##alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET DELETED Possible Slowloris Tool HTTP/Proxy Denial Of Service Attempt"; flow:to_server,established; content:"GET /";
depth:5; content:"User-Agent|3a| Mozilla/4.0 (compatible|3b| MSIE 7.0|3b| Windows NT 5.1|3b| Trident/4.0"; offset:30; depth:90; threshold: type threshold, track by_src, count 100,
seconds 30; classtype:attempted-dos; reference:url,isc.sans.org/diary.html?storyid=6601; reference:url,www.packetstormsecurity.com/filedesc/slowloris.pl.txt.html;
reference:url,doc.emergingthreats.net/2009413; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_Slowliris; sid:2009413; rev:3;)

#by kevin ross
#
#alert udp $EXTERNAL_NET any -> $HOME_NET 69 (msg:"ET DOS Possible SolarWinds TFTP Server Read Request Denial Of Service Attempt"; content:"|00 01 01|"; depth:3; content:"NETASCII";
classtype:attempted-dos; reference:url,www.exploit-db.com/exploits/12683/; reference:url,doc.emergingthreats.net/2011673; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/DOS/DOS_Solarwinds; sid:2011673; rev:3;)

#by kevin ross
#
#alert udp $EXTERNAL_NET any -> $HOME_NET 69 (msg:"ET DOS SolarWinds TFTP Server Long Write Request Denial Of Service Attempt"; content:"|00 02|"; depth:2; isdataat:1000,relative;
content:!"|0A|"; within:1000; content:"NETASCII"; distance:1000; classtype:attempted-dos; reference:url,www.exploit-db.com/exploits/13836/;
reference:url,doc.emergingthreats.net/2011674; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_Solarwinds; sid:2011674; rev:3;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 5900 (msg:"ET DOS Possible VNC ClientCutText Message Denial of Service/Memory Corruption Attempt"; flow:established,to_server; content:"|06|";
depth:1; isdataat:1000,relative; content:!"|0A|"; within:1000; classtype:attempted-dos;
reference:url,www.fortiguard.com/encyclopedia/vulnerability/vnc.server.clientcuttext.message.memory.corruption.html; reference:url,doc.emergingthreats.net/2011732;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/DOS/DOS_VNC; sid:2011732; rev:2;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET EXPLOIT Adobe Acrobat Reader Malicious URL Null Byte"; flow: to_server,established; uricontent:".pdf|00|"; nocase;
classtype:attempted-admin; reference:url,idefense.com/application/poi/display?id=126&type=vulnerabilities; reference:url,www.securiteam.com/windowsntfocus/5BP0D20DPW.html;
reference:cve,2004-0629; reference:url,doc.emergingthreats.net/bin/view/Main/2001217; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Adobe_Acrobat_BO;
sid:2001217; rev:10;)

#From Bdoctor
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 617 (msg:"ET EXPLOIT Arkeia full remote access without password or authentication"; flow: from_server,established;
content:"|464F3A20596F7520686176652073756 3|"; content:"|6520636C69656E7420696E666F726D61|"; classtype: attempted-admin; reference:url,metasploit.com/research/vulns/arkeia_agent;
reference:url,doc.emergingthreats.net/bin/view/Main/2001742; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Arkeia; sid:2001742; rev:8;)

#by Akash Mahajan
#
alert udp $EXTERNAL_NET any -> $HOME_NET 14000 (msg:"ET EXPLOIT Borland VisiBroker Smart Agent Heap Overflow"; content:"|44 53 52 65 71 75 65 73 74|"; pcre:"/[0-9a-zA-Z]{50,}/R";
classtype:successful-dos; reference:bugtraq,28084; reference:url,aluigi.altervista.org/adv/visibroken-adv.txt; reference:url,doc.emergingthreats.net/bin/view/Main/2007937;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Borland; sid:2007937; rev:3;)

#by Blake Hartstein
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 5250 (msg:"ET EXPLOIT MISC Computer Associates Negative Content-Length Buffer Overflow"; flow:established,to_server; content:"Content-
Length|3A|"; nocase; pcre:"/^Content-Length\x3a\s*-\d+/smi"; classtype:web-application-attack; reference:bugtraq,16354; reference:cve,2005-3653;
reference:url,doc.emergingthreats.net/bin/view/Main/2002791; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_CA; sid:2002791; rev:4;)

#Blake Hartstein of Demarc
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 2200 (msg:"ET EXPLOIT CA BrightStor ARCserve Mobile Backup LGSERVER.EXE Heap Corruption"; flow:established,to_server; content:"|4e 3d 2c 1b|";
depth:4; isdataat:2891,relative; classtype:attempted-admin; reference:cve,2007-0449; reference:url,doc.emergingthreats.net/bin/view/Main/2003369;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_CA; sid:2003369; rev:3;)

#by Shirkdog
#
alert udp $EXTERNAL_NET any -> $HOME_NET 111 (msg:"ET EXPLOIT Computer Associates Brightstor ARCServer Backup RPC Server (Catirpc.dll) DoS"; content:"|00 00 00 00|"; offset:4; depth:4;
content:"|00 00 00 03|"; distance:8; within:4; content:"|00 00 00 08|"; distance:0; within:4; content:"|00 00 00 00|"; distance:0; within:4; content:"|00 00 00 00|"; distance:4;
within:4; content:"|00 00 00 00 00 00 00 00|"; distance:8; within:32; classtype:attempted-dos; reference:url,www.milw0rm.com/exploits/3248;
reference:url,doc.emergingthreats.net/bin/view/Main/2003370; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_CA; sid:2003370; rev:3;)

#by Shirkdog
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 1900 (msg:"ET EXPLOIT Computer Associates Mobile Backup Service LGSERVER.EXE Stack Overflow"; flow:established,to_server; content:"0000033000";
depth:10; isdataat:1000,relative; classtype:attempted-admin; reference:url,www.milw0rm.com/exploits/3244; reference:url,doc.emergingthreats.net/bin/view/Main/2003378;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_CA; sid:2003378; rev:3;)

#Also by Shirkdog
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 2200 (msg:"ET EXPLOIT Computer Associates BrightStor ARCserve Backup for Laptops LGServer.exe DoS"; flow:established,to_server; content:"|ff ff
ff ff|"; offset:16; depth:4; classtype:attempted-dos; reference:url,www.securityfocus.com/archive/1/archive/1/458650/100/0/threaded;
reference:url,doc.emergingthreats.net/bin/view/Main/2003379; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_CA; sid:2003379; rev:3;)

#another from Shirkdog
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 1024:65535 (msg:"ET EXPLOIT Computer Associates Brightstor ARCServe Backup Mediasvr.exe Remote Exploit"; flow:established,to_server;
content:"|00 06 09 7e|"; offset:16; depth:4; content:"|00 00 00 bf|"; distance:4; within:4; content:"|00 00 00 00 00 00 00 00|"; distance:0; within:8; classtype:attempted-admin;
reference:url,www.milw0rm.com/exploits/3604; reference:url,doc.emergingthreats.net/bin/view/Main/2003518; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_CA; sid:2003518; rev:3;)

#by shirkdog as well
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 1024:65535 (msg:"ET EXPLOIT CA Brightstor ARCServe caloggerd DoS"; flow:established,to_server; content:"|00 06 09 82|"; offset:16; depth:4;
content:"|00 00 00 01|"; distance:4; within:4; content:"|00 00 00 00 00 00 00 00|"; distance:0; within:8; classtype:attempted-dos; reference:url,www.milw0rm.com/exploits/3939;
reference:url,doc.emergingthreats.net/bin/view/Main/2003750; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_CA; sid:2003750; rev:3;)

#by shirkdog as well
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 1024:65535 (msg:"ET EXPLOIT CA Brightstor ARCServe Mediasvr DoS"; flow:established,to_server; content:"|00 06 09 7e|"; offset:16; depth:4;
content:"|00 00 00 7e|"; distance:4; within:4; content:"|00 00 00 00 00 00 00 00|"; distance:0; within:8; classtype:attempted-dos; reference:url, www.milw0rm.com/exploits/3940;
reference:url,doc.emergingthreats.net/bin/view/Main/2003751; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_CA; sid:2003751; rev:3;)

#by David Maciejak
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET EXPLOIT CVSTrac filediff Arbitrary Remote Code Execution"; flow: to_server,established; uricontent:"filediff|3f|f=";
nocase; pcre:"/filediff\?f=.+&v1=[\d.]+&v2=[\d.]+\;.+/Ui"; classtype:web-application-attack; reference:bugtraq,10878; reference:cve,2004-1456;
reference:url,doc.emergingthreats.net/bin/view/Main/2002697; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_CVSTrac; sid:2002697; rev:6;)

#
alert tcp $EXTERNAL_NET any -> $HOME_NET 2401 (msg:"ET EXPLOIT CVS server heap overflow attempt (target Linux)"; flow: to_server,established; dsize: >512; content:"|45 6e 74 72 79 20 43
43 43 43 43 43 43 43 43 2f 43 43|"; offset: 0; depth: 20; threshold: type limit, track by_dst, count 1, seconds 60; classtype: attempted-admin;
reference:url,doc.emergingthreats.net/bin/view/Main/2000048; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_CVS_HEAP_Overflow; sid:2000048; rev:5;)

#
alert tcp $EXTERNAL_NET any -> $HOME_NET 2401 (msg:"ET EXPLOIT CVS server heap overflow attempt (target BSD)"; flow: to_server,established; dsize: >512; content:"|45 6e 74 72 79 20 61
61 61 61 61 61 61 61 61 61 61 61|"; offset: 0; depth: 18; threshold: type limit, track by_dst, count 1, seconds 60; classtype: attempted-admin;
reference:url,doc.emergingthreats.net/bin/view/Main/2000031; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_CVS_HEAP_Overflow; sid:2000031; rev:5;)

#
alert tcp $EXTERNAL_NET any -> $HOME_NET 2401 (msg:"ET EXPLOIT CVS server heap overflow attempt (target Solaris)"; flow: to_server,established; dsize: >512; content:"|41 72 67 75 6d 65
6e 74 20 62 62 62 62 62 62 62 62 62 62|"; offset: 0; depth: 18; threshold: type limit, track by_dst, count 1, seconds 60; classtype: attempted-admin;
reference:url,doc.emergingthreats.net/bin/view/Main/2000049; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_CVS_HEAP_Overflow; sid:2000049; rev:5;)
```

```
#Submitted by Cody Hatch
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET EXPLOIT Cisco %u IDS evasion"; flow: to_server,established; uricontent:"%u002F"; classtype: attempted-dos;
reference:url,doc.emergingthreats.net/bin/view/Main/2000012; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Cisco_%u_Evasion; sid:2000012; rev:9;)

#Submitted by Cody Hatch
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"ET EXPLOIT Catalyst SSH protocol mismatch"; flow: to_server,established; content:"|61 25 61 25 61 25 61 25 61 25 61 25 61 25|";
classtype: attempted-dos; reference:url,www.cisco.com/warp/public/707/catalyst-ssh-protocolmismatch-pub.shtml; reference:url,doc.emergingthreats.net/bin/view/Main/2000007;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Cisco_Catalyst_SSH_Protocol_Mismatch; sid:2000007; rev:7;)

#Submitted by Cody Hatch
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET EXPLOIT Cisco IOS HTTP server DoS"; flow: to_server,established; uricontent:"/TEST?/"; nocase; classtype: attempted-dos;
reference:url,doc.emergingthreats.net/bin/view/Main/2000013; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Cisco_HTTP_Server_DoS; sid:2000013; rev:10;)

#Submitted by Cody Hatch
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET EXPLOIT Cisco IOS HTTP DoS"; flow: to_server,established; uricontent:"/error?/"; nocase; classtype: attempted-dos;
reference:url,www.cisco.com/warp/public/707/ioshttpserverquery-pub.shtml; reference:url,doc.emergingthreats.net/bin/view/Main/2000009; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Cisco_IOS_HTTP_DOS; sid:2000009; rev:10;)

#by Shirkdog
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET EXPLOIT Cisco-MARS/JBoss jmx-console POST"; flow:to_server,established; content:"POST "; depth:5; nocase; uricontent:"/jmx-
console/HtmlAdaptor"; nocase; flowbits:set,cmars.jboss; classtype:attempted-admin; reference:bugtraq,19071; reference:url,doc.emergingthreats.net/bin/view/Main/2003064;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Cisco_Mars; sid:2003064; rev:5;)

#by Shirkdog
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET EXPLOIT Cisco-MARS/JBoss Remote Command Execution"; flowbits:isset,cmars.jboss; flow:to_server,established;
content:"action=invokeOp"; nocase; content:"jboss.script"; nocase; content:"Runtime|2e|getRuntime|25|28|25|29|2e|exec|25|28"; nocase; classtype: attempted-admin;
reference:bugtraq,19071; reference:url,doc.emergingthreats.net/bin/view/Main/2003065; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Cisco_Mars;
sid:2003065; rev:4;)

#Submitted by Cody Hatch
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 23 (msg:"ET EXPLOIT Cisco Telnet Buffer Overflow"; flow: to_server,established; content:"|3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 61
7e 20 25 25 25 25 25 58 58|"; threshold: type limit, track by_src, count 1, seconds 120; classtype: attempted-dos; reference:url,www.cisco.com/warp/public/707/cisco-sn-20040326-
exploits.shtml; reference:url,doc.emergingthreats.net/bin/view/Main/2000005; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Cisco_Telnet_Buffer_Overflow;
sid:2000005; rev:7;)

#by Dale Peterson of digitalbond.com
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 20222 (msg:"ET SCADA CitectSCADA ODBC Overflowflow Attempt"; flow:established,to_server; dsize:4; byte_test:4,>,399,0; classtype:attempted-user;
reference:cve,2008-2639; reference:url,www.digitalbond.com/index.php/2008/09/08/ids-signature-for-citect-vuln/; reference:url,doc.emergingthreats.net/bin/view/Main/2008542;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Citect_SCADA; sid:2008542; rev:6;)

#by Blake Hartstein at Demarc
#
alert udp $EXTERNAL_NET any -> $HOME_NET 1900 (msg:"ET EXPLOIT UPnP DLink M-Search Overflow Attempt"; content:"M-SEARCH "; depth:9; nocase; isdataat:500,relative; pcre:"/M-SEARCH\s+
[^\n]{500}/i"; classtype:attempted-user; reference:url,www.eeye.com/html/research/advisories/AD20060714.html; reference:url,doc.emergingthreats.net/bin/view/Main/2003039;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Dlink; sid:2003039; rev:4;)

#By Mark Tombaugh
#
##alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET EXPLOIT Incoming Electronic Mail for UNIX Expires Header Buffer Overflow Exploit"; flow:established; content:"Expires|3a|";
content:"|40 60 6e 63|"; distance:52; within:300; content:"|2d 70|"; distance:2; within:20; classtype:misc-attack; reference:url,www.frsirt.com/exploits/20050822.elmexploit.c.php;
reference:url,www.instinct.org/elm/; reference:url,doc.emergingthreats.net/bin/view/Main/2002315; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Elm;
sid:2002315; rev:7;)

#By Mark Tombaugh
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET EXPLOIT Outgoing Electronic Mail for UNIX Expires Header Buffer Overflow Exploit"; flow:established; content:"Expires|3a|";
content:"|40 60 6e 63|"; distance:52; within:300; content:"|2d 70|"; distance:2; within:20; classtype:misc-attack; reference:url,www.frsirt.com/exploits/20050822.elmexploit.c.php;
reference:url,www.instinct.org/elm/; reference:url,doc.emergingthreats.net/bin/view/Main/2002316; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Elm;
sid:2002316; rev:7;)

#by Akash Mahajan
#
alert udp $EXTERNAL_NET any -> $HOME_NET 427 (msg:"ET EXPLOIT ExtremeZ-IP File and Print Server Multiple Vulnerabilities - udp"; content:"language"; content:"|65 7a 69 70 3a 2f 2f 62 6c
61 2f 62 6c 61 3f 53 4e 3d 62 6c 61 3f 50 4e 3d 62 6c 61 3f 55 4e 3d 62 6c 61|"; classtype:successful-dos; reference:bugtraq,27718; reference:url,aluigi.altervista.org/adv/ezipirla-
adv.txt; reference:cve,CVE-2008-0767; reference:url,doc.emergingthreats.net/bin/view/Main/2007876; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_ExtremeZ-IP; sid:2007876; rev:2;)

#by Akash Mahajan
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 548 (msg:"ET EXPLOIT ExtremeZ-IP File and Print Server Multiple Vulnerabilities - tcp"; flow:established,to_server; content:"|12 06 41 46 50 33
2e 31|"; pcre:"/[a-zA-Z0-9]{5,}/i"; classtype:successful-dos; reference:bugtraq,27718; reference:url,aluigi.altervista.org/adv/ezipirla-adv.txt; reference:cve,CVE-2008-0759;
reference:url,doc.emergingthreats.net/bin/view/Main/2007877; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_ExtremeZ-IP; sid:2007877; rev:3;)

#by Kevin Ross
#disabling for falses...
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET FTP FTP CWD command attempt without login"; flow:established,to_server; flowbits:isnotset,ET.ftp.user.login; content:!"USER";
depth:4; content:"CWD"; nocase; classtype:attempted-recon; reference:url,www.nsftools.com/tips/RawFTP.htm; reference:url,doc.emergingthreats.net/2010731;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_FTP; sid:2010731; rev:2;)

#by Kevin Ross
#disabling for falses...
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET FTP FTP SITE command attempt without login"; flow:established,to_server; flowbits:isnotset,ET.ftp.user.login; content:!"USER";
depth:4; content:"SITE"; nocase; classtype:attempted-recon; reference:url,www.nsftools.com/tips/RawFTP.htm; reference:url,doc.emergingthreats.net/2010732;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_FTP; sid:2010732; rev:2;)

#by Kevin Ross
#disabling for falses...
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET FTP FTP RMDIR command attempt without login"; flow:established,to_server; flowbits:isnotset,ET.ftp.user.login; content:!"USER";
depth:4; content:"RMDIR"; nocase; classtype:attempted-recon; reference:url,www.nsftools.com/tips/RawFTP.htm; reference:url,doc.emergingthreats.net/2010733;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_FTP; sid:2010733; rev:2;)

#by Kevin Ross
#disabling for falses...
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET FTP FTP MKDIR command attempt without login"; flow:established,to_server; flowbits:isnotset,ET.ftp.user.login; content:!"USER";
depth:4; content:"MKDIR"; nocase; classtype:attempted-recon; reference:url,www.nsftools.com/tips/RawFTP.htm; reference:url,doc.emergingthreats.net/2010734;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_FTP; sid:2010734; rev:2;)

#by Kevin Ross
#disabling for falses...
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET FTP FTP PWD command attempt without login"; flow:established,to_server; flowbits:isnotset,ET.ftp.user.login; content:!"USER";
depth:4; content:"PWD"; nocase; classtype:attempted-recon; reference:url,www.nsftools.com/tips/RawFTP.htm; reference:url,doc.emergingthreats.net/2010735;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_FTP; sid:2010735; rev:2;)

#by Kevin Ross
#disabling for falses...
#
```

```
#alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET FTP FTP RETR command attempt without login"; flow:established,to_server; flowbits:isnotset,ET.ftp.user.login; content:!"USER";
depth:4; content:"RETR"; nocase; classtype:attempted-recon; reference:url,www.nsftools.com/tips/RawFTP.htm; reference:url,doc.emergingthreats.net/2010736;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_FTP; sid:2010736; rev:2;)

#by Kevin Ross
#disabling for falses...
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET FTP FTP NLST command attempt without login"; flow:established,to_server; flowbits:isnotset,ET.ftp.user.login; content:!"USER";
depth:4; content:"NLST"; nocase; classtype:attempted-recon; reference:url,www.nsftools.com/tips/RawFTP.htm; reference:url,doc.emergingthreats.net/2010737;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_FTP; sid:2010737; rev:2;)

#by Kevin Ross
#disabling for falses...
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET FTP FTP RNTO command attempt without login"; flow:established,to_server; flowbits:isnotset,ET.ftp.user.login; content:!"USER";
depth:4; content:"RNTO"; nocase; classtype:attempted-recon; reference:url,www.nsftools.com/tips/RawFTP.htm; reference:url,doc.emergingthreats.net/2010738;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_FTP; sid:2010738; rev:2;)

#by Kevin Ross
#disabling for falses...
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET FTP FTP RNFR command attempt without login"; flow:established,to_server; flowbits:isnotset,ET.ftp.user.login; content:!"USER";
depth:4; content:"RNFR"; nocase; classtype:attempted-recon; reference:url,www.nsftools.com/tips/RawFTP.htm; reference:url,doc.emergingthreats.net/2010739;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_FTP; sid:2010739; rev:2;)

#by Kevin Ross
#disabling for falses...
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET FTP FTP STOR command attempt without login"; flow:established,to_server; flowbits:isnotset,ET.ftp.user.login; content:!"USER";
depth:4; content:"STOR"; nocase; classtype:attempted-recon; reference:url,www.nsftools.com/tips/RawFTP.htm; reference:url,doc.emergingthreats.net/2010740;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_FTP; sid:2010740; rev:2;)

#by Anonymous Researchers(tm)
#Intended to catch common shellcode encoding in exploit scripts coming to clients in web sessions
#high load. use these if you need them!
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET SHELLCODE Possible UTF-8 encoded Shellcode Detected"; flow:from_server,established; content:"%u"; nocase; isdataat:2;
content:!"|0a|"; within:2; content:!"|20|"; within:2; pcre:"/(%U([0-9a-f]{2})){6}/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003173;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Generic_Shellcode; sid:2003173; rev:7;)

#by Anonymous Researchers(tm)
#Intended to catch common shellcode encoding in exploit scripts coming to clients in web sessions
#high load. use these if you need them!
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET SHELLCODE Possible UTF-16 encoded Shellcode Detected"; flow:from_server,established; content:"%u"; nocase; isdataat:4;
content:!"|0a|"; within:4; content:!"|20|"; within:4; pcre:"/(%U([0-9a-f]{4})){6}/i"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003174;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Generic_Shellcode; sid:2003174; rev:8;)

#by rich rumble
#GsecDump rule
#
alert tcp any any -> $HOME_NET [139,445] (msg:"ET EXPLOIT GsecDump executed"; flow:to_server,established; content:"|67 00 73 00 65 00 63 00 64 00 75 00 6d 00 70 00 2e 00 65 00 78 00
65|"; classtype:suspicious-filename-detect; reference:url,xinn.org/Snort-gsecdump.html; reference:url,doc.emergingthreats.net/2010783; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Gsecdump; sid:2010783; rev:3;)

#by Veerendra
#10/11/2008 GuildFTPd CWD and LIST Command Heap Overflow Attack.
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET EXPLOIT GuildFTPd CWD and LIST Command Heap Overflow - POC-1"; flow:established; content:"cwd"; depth:4; nocase; dsize:>74;
pcre:"/(\/\.){70,}/i"; classtype:web-application-attack; reference:url,milw0rm.com/exploits/6738; reference:cve,CVE-2008-4572; reference:bugtraq,31729;
reference:url,doc.emergingthreats.net/bin/view/Main/2008776; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_GuidFTP; sid:2008776; rev:3;)

#by Veerendra
#10/11/2008 GuildFTPd CWD and LIST Command Heap Overflow Attack.
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET EXPLOIT GuildFTPd CWD and LIST Command Heap Overflow - POC-2"; flow:established; content:"list"; depth:5; nocase; dsize:>74;
pcre:"/[\w]{70,}/i"; classtype:web-application-attack; reference:url,milw0rm.com/exploits/6738; reference:cve,CVE-2008-4572; reference:bugtraq,31729;
reference:url,doc.emergingthreats.net/bin/view/Main/2008777; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_GuidFTP; sid:2008777; rev:3;)

#by Veerendra
#10/11/2008 GuildFTPd CWD and LIST Command Heap Overflow Attack.
#
#alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET EXPLOIT GuppY error.php Arbitrary Remote Code Execution"; flow: to_server,established; uricontent:"/error.php?";
nocase; uricontent:"err="; nocase; uricontent:"_SERVER[REMOTE_ADDR]="; nocase; classtype: web-application-attack; reference:bugtraq,15609;
reference:url,doc.emergingthreats.net/bin/view/Main/2002703; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Guppy; sid:2002703; rev:4;)

#by David Maciejak
#
#alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET EXPLOIT GuppY error.php POST Arbitrary Remote Code Execution"; flow: to_server,established; content:"POST "; depth:5;
nocase; uricontent:"/error.php?"; nocase; uricontent:"err="; nocase; pcre:"/Cookie\:\ +REMOTE_ADDR=/i"; classtype:web-application-attack; reference:bugtraq,15609;
reference:url,doc.emergingthreats.net/bin/view/Main/2003332; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Guppy; sid:2003332; rev:4;)

#by mike cox
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 1530 (msg:"ET EXPLOIT HP Open View Data Protector Buffer Overflow Attempt"; flow:established,to_server; content:"|B6 29 8C 23 FF FF FF|";
pcre:"/\xB6\x29\x8C\x23\xFF\xFF\xFF[\xF8-\xFF]/"; classtype:attempted-admin; reference:url,dvlabs.tippingpoint.com/advisory/TPTI-09-15; reference:url,doc.emergingthreats.net/2010546;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_HP; reference:cve,2007-2281; sid:2010546; rev:3;)

#by Blake Hartstein of Demarc
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET FTP USER login flowbit"; flow:established,to_server; content:"USER "; nocase; depth:5; flowbits:set,ET.ftp.user.login;
flowbits:noalert; classtype:not-suspicious; reference:url,doc.emergingthreats.net/bin/view/Main/2002850; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_HP-UX; sid:2002850; rev:4;)

#by Blake Hartstein of Demarc
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET FTP HP-UX LIST command without login"; flow:established,to_server; flowbits:isnotset,ET.ftp.user.login; content:"LIST "; nocase;
depth:5; classtype:attempted-recon; reference:cve,2005-3296; reference:bugtraq,15138; reference:url,doc.emergingthreats.net/bin/view/Main/2002851;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_HP-UX; sid:2002851; rev:5;)

#by Blake Hartstein of Demarc
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 515 (msg:"ET EXPLOIT HP-UX Printer LPD Command Insertion"; flow:established,to_server; content:"|02|msf28|30|"; depth:7; content:"|60|";
distance:0; within:20; classtype:attempted-user; reference:cve,2005-3277; reference:bugtraq,15136; reference:url,doc.emergingthreats.net/bin/view/Main/2002852;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_HP-UX; sid:2002852; rev:5;)

#By Frank Knobbe
#disabled by default as the ftp preproc will catch this now
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET EXPLOIT Possible IIS FTP Exploit attempt - Large SITE command"; flow:established,to_server; content:"SITE "; nocase;
isdataat:150,relative; content:!"|0d 0a|"; within:150; classtype:attempted-admin; reference:url,www.milw0rm.com/exploits/9541; reference:url,doc.emergingthreats.net/2009828;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_IISFTP; reference:cve,2009-3023; sid:2009828; rev:6;)

#By evilghost
#disabled by default as the ftp preproc will catch this now
#
```

```
#alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET EXPLOIT IIS FTP Exploit - NLST Globbing Exploit"; flow:established,to_server; content:"NLST "; nocase; content:"|2a 2f 2e 2e 2f|";
classtype:attempted-admin; reference:url,www.milw0rm.com/exploits/9541; reference:url,doc.emergingthreats.net/2009860; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_IISFTP; reference:cve,2009-3023; sid:2009860; rev:5;)

#Submitted by Joseph Gama
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET EXPLOIT Invalid non-fragmented packet with fragment offset>0"; fragbits: !M; fragoffset: >0; classtype: bad-unknown;
reference:url,doc.emergingthreats.net/bin/view/Main/2001022; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Invalid_TCP_Fragments; sid:2001022; rev:5;)

#Submitted by Joseph Gama
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET EXPLOIT Invalid fragment - ACK reset"; fragbits: M; flags: !A,12; classtype: bad-unknown;
reference:url,doc.emergingthreats.net/bin/view/Main/2001023; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Invalid_TCP_Fragments; sid:2001023; rev:5;)

#Submitted by Joseph Gama
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET EXPLOIT Invalid fragment - illegal flags"; fragbits: M; flags: *FSR,12; classtype: bad-unknown;
reference:url,doc.emergingthreats.net/bin/view/Main/2001024; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Invalid_TCP_Fragments; sid:2001024; rev:5;)

#by David Maciejak
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET EXPLOIT JamMail Jammail.pl Remote Command Execution Attempt"; flow: to_server,established; uricontent:"/cgi-
bin/jammail.pl?"; nocase; pcre:"/(mail=\|.+\|)/"; classtype: web-application-attack; reference:bugtraq,13937; reference:url,doc.emergingthreats.net/bin/view/Main/2001990;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Jammail; sid:2001990; rev:5;)

#
alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"ET NETBIOS MS04011 Lsasrv.dll RPC exploit (Win2k)"; flow: to_server,established; content:"|00 00 00 00 9A A8 40 00 01 00 00 00 00 00
00 00|"; content:"|01 0000 00 00 00 00 00 9A A8 40 00 01 00 00 00|"; classtype: misc-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2000046;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_LSASRV_DLL_RPC_Exploit_win2k; reference:cve,2003-0533; sid:2000046; rev:9;)

#
alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"ET NETBIOS MS04011 Lsasrv.dll RPC exploit (WinXP)"; flow: to_server,established; content:"|95 14 40 00 03 00 00 00 7C 70 40 00 01|";
content:"|78 85 13 00 AB5B A6 E9 31 31|"; classtype: misc-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2000033; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_LSASRV_DLL_RPC_Exploit_winXP; reference:cve,2003-0533; sid:2000033; rev:9;)

#Submitted by Joseph Gama
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT libPNG - Possible NULL-pointer crash in png_handle_iCCP"; flow: established; content:"|89 50 4E 47 0D 0A 1A 0A|";
depth:8; byte_test:4,>,0x80000000,0,relative,big,string,hex; classtype:misc-activity; reference:url,www.securiteam.com/unixfocus/5ZP0C0KDPG.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001190; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_LibPNG; sid:2001190; rev:10;)

#Submitted by Joseph Gama
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT libPNG - Width exceeds limit"; flow: established; content:"|89 50 4E 47 0D 0A 1A 0A|"; depth:8;
byte_test:4,>,0x80000000,8,relative,big,string,hex; classtype: misc-activity; reference:url,www.securiteam.com/unixfocus/5ZP0C0KDPG.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001191; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_LibPNG; sid:2001191; rev:10;)

#Submitted by Joseph Gama
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT libPNG - Height exceeds limit"; flow: established; content:"|89 50 4E 47 0D 0A 1A 0A|"; depth:8;
byte_test:4,>,0x80000000,12,relative,big,string,hex; classtype: misc-activity; reference:url,www.securiteam.com/unixfocus/5ZP0C0KDPG.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001192; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_LibPNG; sid:2001192; rev:10;)

#Submitted by Joseph Gama
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT libPNG - Possible integer overflow in allocation in png_handle_sPLT"; flow: established; content:"|89 50 4E 47 0D
0A 1A 0A|"; depth:8; content:"sPLT"; isdataat:80,relative; content:!"|00|"; distance: 0; classtype: misc-activity; reference:url,www.securiteam.com/unixfocus/5ZP0C0KDPG.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001195; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_LibPNG; sid:2001195; rev:9;)

#Submitted by Joe Stewart
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT libpng tRNS overflow attempt"; flow: established,to_client; content:"|89|PNG|0D 0A 1A 0A|"; content:!"PLTE";
content:"tRNS"; byte_test:4,>,256,-8,relative,big; classtype:attempted-admin; reference:cve,CAN-2004-0597; reference:url,doc.emergingthreats.net/bin/view/Main/2001058;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_LibPNG; sid:2001058; rev:8;)

#by Blake Hartstein
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET EXPLOIT Linksys WRT54g Authentication Bypass Attempt"; flow:established,to_server; uricontent:"/Security.tri"; nocase;
content:"SecurityMode=0"; nocase; classtype:attempted-admin; reference:url,secunia.com/advisories/21372/; reference:url,doc.emergingthreats.net/bin/view/Main/2003072;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Linksys; sid:2003072; rev:4;)

#by evilghost
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET EXPLOIT Linksys WAP54G debug.cgi Shell Access as Gemtek"; flow:established,to_server; content:"|0d 0a|Authorization|3a|
Basic R2VtdGVrOmdlbXRla3N3ZA==|0d 0a|"; uricontent:"/debug.cgi"; classtype:attempted-admin; reference:url,seclists.org/fulldisclosure/2010/Jun/176;
reference:url,doc.emergingthreats.net/2011669; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Linksys; sid:2011669; rev:4;)

#
alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"ET NETBIOS MS04-007 Kill-Bill ASN1 exploit attempt"; flow: established,to_server; content:"CCCC|20f0fd7f|SVWf"; classtype:attempted-
admin; reference:url,www.phreedom.org/solar/exploits/msasn1-bitstring/; reference:url,www.microsoft.com/technet/security/bulletin/MS04-007.mspx; reference:cve,CAN-2003-0818;
reference:url,doc.emergingthreats.net/bin/view/Main/2001944; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS04-007; sid:2001944; rev:7;)

#Submitted by Chris Norton and Woofz
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET EXPLOIT MS04-032 Windows Metafile (.emf) Heap Overflow Exploit"; flow: established; content:"|45 4D 46|"; content:"|EB 12 90 90 90
90 90 90|"; content:"|9e 5c 05 78|"; nocase; classtype: shellcode-detect; reference:url,www.k-otik.com/exploits/20041020.HOD-ms04032-emf-expl2.c.php;
reference:url,doc.emergingthreats.net/bin/view/Main/2001369; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS04-032; sid:2001369; rev:7;)

#Submitted by Chris Norton and Woofz
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET EXPLOIT Possible MS04-032 Windows Metafile (.emf) Heap Overflow Portbind Attempt"; flow: established; content:"|45 4D 46|";
content:"|23 6A 75 4E|"; classtype: shellcode-detect; reference:url,www.microsoft.com/technet/security/bulletin/ms04-032.mspx;
reference:url,doc.emergingthreats.net/bin/view/Main/2001363; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS04-032; sid:2001363; rev:7;)

#Submitted by Chris Norton and Woofz
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET EXPLOIT MS04-032 Windows Metafile (.emf) Heap Overflow Connectback Attempt"; flow: established; content:"|45 4D 46|"; content:"|5E
79 72 63|"; content:"|48 4F 44 21|"; classtype: shellcode-detect; reference:url,www.microsoft.com/technet/security/bulletin/ms04-032.mspx;
reference:url,doc.emergingthreats.net/bin/view/Main/2001364; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS04-032; sid:2001364; rev:7;)

#From Erik Fichtner
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT MS04-032 Bad EMF file"; flow: from_server,established; content:"|01 00 00 00|"; depth: 4; content:"|20 45 4d 46|";
offset: 40; depth: 44; byte_test:4, >, 256, 60, little; classtype: misc-activity; reference:url,www.sygate.com/alerts/SSR20041013-0001.htm;
reference:url,doc.emergingthreats.net/bin/view/Main/2001374; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS04-032; sid:2001374; rev:8;)

#By Erik Fichtner
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT Exploit MS05-002 Malformed .ANI stack overflow attack"; flow: to_client,established; content:"RIFF";
content:"ACON"; distance: 8; content:"anih"; distance: 160; byte_test:4,>,36,0,relative,little; classtype: misc-attack; reference:url,doc.emergingthreats.net/bin/view/Main/2001668;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS05-002_ANI_Stack_Overflow; sid:2001668; rev:6;)

#by Chris Ries of Vigilant Minds
#
alert tcp $HOME_NET 445 -> $EXTERNAL_NET any (msg:"ET NETBIOS ms05-011 exploit"; flow:from_server,established; content:"|00|"; depth:1; content:"|FF|SMB|32|"; depth:9; offset:4;
content: "|ff ff ff ff 00 00 00 00 ff|"; offset: 132; depth: 141; classtype:attempted-admin; reference:bugtraq,12484; reference:url,www.frsirt.com/exploits/20050623.mssmb_poc.c.php;
reference:url,doc.emergingthreats.net/bin/view/Main/2002064; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS05-011; sid:2002064; rev:7;)

#These should be dropped. Disabling till we hear if anyone wants to keep them
#Erik Fichtner
#
```

```
#alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET EXPLOIT MS05-021 Exchange Link State - Possible Attack (1)"; flow: to_server,established; content:"X-LINK2STATE"; nocase;
classtype: misc-activity; reference:cve,CAN-2005-0560; reference:url,isc.sans.org/diary.php?date=2005-04-12; reference:url,www.microsoft.com/technet/security/bulletin/MS05-021.mspx;
reference:url,doc.emergingthreats.net/bin/view/Main/2001848; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS05-021; sid:2001848; rev:7;)

#These should be dropped. Disabling till we hear if anyone wants to keep them
#Erik Fichtner
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 691 (msg:"ET EXPLOIT MS05-021 Exchange Link State - Possible Attack (2)"; flow: to_server,established; content:"X-LSA-2"; nocase; classtype:
misc-activity; reference:cve,CAN-2005-0560; reference:url,isc.sans.org/diary.php?date=2005-04-12; reference:url,www.microsoft.com/technet/security/bulletin/MS05-021.mspx;
reference:url,doc.emergingthreats.net/bin/view/Main/2001849; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS05-021; sid:2001849; rev:7;)

#These should be dropped. Disabling till we hear if anyone wants to keep them
#Erik Fichtner
#
#alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"ET EXPLOIT MS Exchange Link State Routing Chunk (maybe MS05-021)"; flow: to_server, established; content:"X-LINK2STATE"; nocase;
content:"CHUNK="; nocase; threshold: type limit, track by_src, count 1, seconds 60; flowbits:set,msxlsa; classtype: misc-activity; reference:cve,CAN-2005-0560;
reference:url,isc.sans.org/diary.php?date=2005-04-12; reference:url,www.microsoft.com/technet/security/bulletin/MS05-021.mspx;
reference:url,doc.emergingthreats.net/bin/view/Main/2001873; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS05-021; sid:2001873; rev:9;)

#since this could be variable length chunks, we can't tell if we had
#enough data to blow the server up or not, so we have to read the
#chicken bones to see if it looks like exchange sh!t the bed or not.
#
#alert tcp $SMTP_SERVERS 25 -> $EXTERNAL_NET any (msg:"ET EXPLOIT TCP Reset from MS Exchange after chunked data, probably crashed it (MS05-021)"; flags: R; flowbits:isset,msxlsa;
flowbits: unset,msxlsa; classtype: misc-activity; reference:cve,CAN-2005-0560; reference:url,isc.sans.org/diary.php?date=2005-04-12;
reference:url,www.microsoft.com/technet/security/bulletin/MS05-021.mspx; reference:url,doc.emergingthreats.net/bin/view/Main/2001874; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS05-021; sid:2001874; rev:8;)

#Added 2005/08/14 as found on SANS ISC web site, by AlertLogic
#Replaced by sigs below
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"ET NETBIOS SMB-DS Microsoft Windows 2000 Plug and Play Vulnerability"; flow:to_server,established; content:"|FF|SMB%"; depth:5;
offset:4; nocase; content:"|2600|"; depth:2; offset:65; content:"|67157a76|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS05-039.mspx;
reference:url,isc.sans.org/diary.php?date=2005-08-14; reference:url,doc.emergingthreats.net/bin/view/Main/2002186; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS05-039; sid:2002186; rev:4;)

#Added 2005/08/14 as found on SANS ISC web site, by AlertLogic
#Replaced by sigs below
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 139 (msg:"ET NETBIOS NETBIOS SMB Microsoft Windows 2000 PNP Vuln"; flow:to_server,established; content:"|FF|SMB%"; depth:5; offset:4; nocase;
content:"|2600|"; depth:2; offset:65; content:"|3600|"; offset:110; within:5; content:"|F6387A76|"; classtype:attempted-admin;
reference:url,www.microsoft.com/technet/security/Bulletin/MS05-039.mspx; reference:url,isc.sans.org/diary.php?date=2005-08-14;
reference:url,doc.emergingthreats.net/bin/view/Main/2002187; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS05-039; sid:2002187; rev:5;)

#Added 2005/08/14 as found on SANS ISC web site, by AlertLogic
#Replaced by sigs below
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"ET NETBIOS NETBIOS SMB-DS Microsoft Windows 2000 PNP Vuln"; flow:to_server,established; content:"|FF|SMB%"; depth:5; offset: 4;
nocase; content:"|2600|"; depth:2; offset:65; content:"|3600|"; offset:110; within:5; content:"|F6387A76|"; classtype:attempted-admin;
reference:url,www.microsoft.com/technet/security/Bulletin/MS05-039.mspx; reference:url,isc.sans.org/diary.php?date=2005-08-14;
reference:url,doc.emergingthreats.net/bin/view/Main/2002188; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS05-039; sid:2002188; rev:5;)

#All related to UPnP Exploit, MS05-039
#Thanks to the Alert Logic team
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"ET NETBIOS SMB-DS DCERPC PnP HOD bind attempt"; flow:to_server,established; content:"|FF|SMB%"; depth:5; offset:4; nocase;
content:"&|00|"; within:2; distance:56; content:"|5C 00|P|00|I|00|P|00|E|00 5C 00|"; within:12; distance:5; nocase; content:"|05|"; within:1; distance:4; content:"|0B|"; within:1;
distance:1; content:"|40 4E 9F 8D 3D A0 CE 11 8F 69 08 00 3E 30 05 1B|"; flowbits:set,netbios.pnp.bind.attempt; flowbits:noalert; classtype:protocol-command-decode;
reference:url,doc.emergingthreats.net/bin/view/Main/2002199; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS05-039; sid:2002199; rev:4;)

#All related to UPnP Exploit, MS05-039
#Thanks to the Alert Logic team
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"ET NETBIOS SMB-DS DCERPC PnP bind attempt"; flow:to_server,established; content:"|FF|SMB%"; depth:5; offset:4; nocase;
content:"&|00|"; within:2; distance:56; content:"|5C 00|P|00|I|00|P|00|E|00 5C 00|"; within:12; distance:5; nocase; content:"|05|"; within:1; distance:2; content:"|0B|"; within:1;
distance:1; content:"|40 4E 9F 8D 3D A0 CE 11 8F 69 08 00 3E 30 05 1B|"; flowbits:set,netbios.pnp.bind.attempt; flowbits:noalert; classtype:protocol-command-decode;
reference:url,doc.emergingthreats.net/bin/view/Main/2002200; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS05-039; sid:2002200; rev:4;)

#All related to UPnP Exploit, MS05-039
#Thanks to the Alert Logic team
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"ET NETBIOS SMB-DS DCERPC PnP QueryResConfList exploit attempt"; flow:to_server,established; content:"|FF|SMB%"; depth:5; offset:4;
nocase; content:"&|00|"; within:2; distance:56; content:"|5C 00|P|00|I|00|P|00|E|00 5C 00|"; within:12; distance:5; nocase; content:"|36 00|"; within:2; distance:26;
pcre:"/(\x00\\\x00.*?){2}\x00{2}\xFF{2}.{128,}[\x04-\xFF][\x00-\xFF]{3}\x00{4}$/Rs"; flowbits:isset,netbios.pnp.bind.attempt; classtype:attempted-admin; reference:cve,CAN-2005-1983;
reference:url,www.microsoft.com/technet/security/Bulletin/MS05-039.mspx; reference:url,doc.emergingthreats.net/bin/view/Main/2002201; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS05-039; sid:2002201; rev:4;)

#All related to UPnP Exploit, MS05-039
#Thanks to the Alert Logic team
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 139 (msg:"ET NETBIOS SMB DCERPC PnP bind attempt"; flow:to_server,established; content:"|00|"; depth:1; content:"|FF|SMB%"; depth:5; offset:4;
nocase; byte_test:2,^,1,5,relative; content:"&|00|"; within:2; distance:56; content:"|5C|PIPE|5C 00 05 00 0B|"; within:10; distance:4; byte_test:1,&,16,1,relative; content:"|40 4E 9F 8D
3D A0 CE 11 8F 69 08 00 3E 30 05 1B|"; flowbits:set,netbios.pnp.bind.attempt; flowbits:noalert; classtype:protocol-command-decode;
reference:url,doc.emergingthreats.net/bin/view/Main/2002202; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS05-039; sid:2002202; rev:4;)

#All related to UPnP Exploit, MS05-039
#Thanks to the Alert Logic team
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 139 (msg:"ET NETBIOS SMB DCERPC PnP QueryResConfList exploit attempt"; flow:to_server,established; content:"|00|"; depth:1; content:"|FF|SMB%";
depth:5; offset:4; nocase; byte_test:2,^,1,5,relative; content:"&|00|"; within:2; distance:56; content:"|5C|PIPE|5C 00 05 00 00|"; within:10; distance:4; nocase; content:"|36 00|";
within:2; distance:19; pcre:"/(\x00\\\x00.*?){2}\x00{2}\xFF{2}.{128,}[\x04-\xFF][\x00-\xFF]{3}\x00{4}$/Rs"; flowbits:isset,netbios.pnp.bind.attempt; classtype:attempted-admin;
reference:cve,CAN-2005-1983; reference:url,www.microsoft.com/technet/security/Bulletin/MS05-039.mspx; reference:url,doc.emergingthreats.net/bin/view/Main/2002203;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS05-039; sid:2002203; rev:4;)

#by Shirkdog, updated 2006-02-21, mscott
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT Windows Media Player parsing BMP file with 0 size offset to start of image"; flow:established,from_server;
content:"BM"; depth:400; byte_test:8,=,0,4,relative; classtype:attempted-user; reference:url,www.milw0rm.com/id.php?id=1500;
reference:url,www.microsoft.com/technet/security/Bulletin/MS06-005.mspx; reference:cve,2006-0006; reference:bugtraq,16633; reference:url,doc.emergingthreats.net/bin/view/Main/2002802;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS06-005; sid:2002802; rev:8;)

#by Joe Stewart of Lurhq
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT BMP with invalid bfOffBits"; flow:established,to_client; content:"|0d 0a 0d 0a|BM"; byte_test:4,>,14,0,relative;
content:"|0000000000000000|"; distance:4; within:8; classtype:attempted-user; reference:url,www.microsoft.com/technet/security/Bulletin/ms06-005.mspx; reference:cve,2006-0006;
reference:bugtraq,16633; reference:url,doc.emergingthreats.net/bin/view/Main/2002803; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS06-005;
sid:2002803; rev:8;)

#by Shirkdog
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"ET EXPLOIT DOS Microsoft Windows SRV.SYS MAILSLOT "; flow:to_server,established; content:"|00|"; depth:1; content:"|FF|SMB%";
within:5; distance:3; byte_test:1,!&,128,6,relative; pcre:"/^.{27}/sR"; content:"|03|"; distance:21; content:"|01 00 00 00 00 00|"; distance:1; within:6;
byte_test:2,=,17,0,little,relative; content:"|5C|MAILSLOT|5C|"; within:10; distance:2; classtype:attempted-dos; reference:url,www.milw0rm.com/exploits/2057;
reference:url,www.microsoft.com/technet/security/bulletin/MS06-035.mspx; reference:url,doc.emergingthreats.net/bin/view/Main/2003067; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS06-035; sid:2003067; rev:5;)

#Submitted 2006-08-11 by Joe Stewart
#
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 139 (msg:"ET NETBIOS NETBIOS SMB DCERPC NetrpPathCanonicalize request (possible MS06-040)"; flow:to_server,established; content:"|00|"; depth:1;
content:"|FF|SMB|25|"; depth:5; offset:4; nocase; byte_test:2,^,1,5,relative; content:"&|00|"; within:2; distance:56; content:"|5C|PIPE|5C 00 05 00|"; within:9; distance:4; content:"|1f
00|"; distance:20; within:2; classtype:misc-attack; reference:url,www.microsoft.com/technet/security/bulletin/MS06-040.mspx; reference:url,doc.emergingthreats.net/bin/view/Main/2003081;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS06-040; sid:2003081; rev:5;)

#Submitted 2006-08-11 by Joe Stewart
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"ET NETBIOS NETBIOS SMB-DS DCERPC NetrpPathCanonicalize request (possible MS06-040)"; flow:to_server,established; content:"|00|";
depth:1; content:"|FF|SMB|25|"; depth:5; offset:4; nocase; byte_test:2,^,1,5,relative; content:"&|00|"; within:2; distance:56; content:"|5C|PIPE|5C 00 05 00|"; within:9; distance:4;
content:"|1f 00|"; distance:20; within:2; classtype:misc-attack; reference:url,www.microsoft.com/technet/security/bulletin/MS06-040.mspx;
reference:url,doc.emergingthreats.net/bin/view/Main/2003082; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS06-040; sid:2003082; rev:5;)

#by Secureworks
#
alert udp any any -> $HOME_NET 139 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (1)"; content:"|0B|"; offset:2; depth:1; content:"|C8 4F 32 4B 70 16 D3 01
12 78 5A 47 BF 6E E1 88|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250;
reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008690; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008690; rev:5;)

#by Secureworks
#
alert udp any any -> $HOME_NET 139 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (2)"; content:"|1F 00|"; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF
6E E1 88|"; content:"..|5C|..|5C|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250;
reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008691; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008691; rev:6;)

#by Secureworks
#
alert udp any any -> $HOME_NET 139 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (3)"; content:"|1F 00|"; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF
6E E1 88|"; content:"../../"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250;
reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008692; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008692; rev:5;)

#by Secureworks
#
alert udp any any -> $HOME_NET 139 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (4)"; content:"|1F 00|"; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF
6E E1 88|"; content:"|00 2E 00 2E 00 2F 00 2E 00 2E 00 2F|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250;
reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008693; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008693; rev:5;)

#by Secureworks
#
alert udp any any -> $HOME_NET 139 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (5)"; content:"|1F 00|"; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF
6E E1 88|"; content:"|00 2E 00 2E 00 5C 00 2E 00 2E 00 5C|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250;
reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008694; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008694; rev:5;)

#by Secureworks
#
##alert udp any any -> $HOME_NET 139 (msg:"ET DELETED Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (6)"; content:"|0B|"; offset:2; depth:1; content:"|C8 4F 32 4B 70 16 D3
01 12 78 5A 47 BF 6E E1 88|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250;
reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008695; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008695; rev:5;)

#by Secureworks
#
alert udp any any -> $HOME_NET 139 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (7)"; content:"|20 00|"; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF
6E E1 88|"; content:"..|5C|..|5C|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250;
reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008696; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008696; rev:6;)

#by Secureworks
#
alert udp any any -> $HOME_NET 139 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (8)"; content:"|20 00|"; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF
6E E1 88|"; content:"../../"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250;
reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008697; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008697; rev:5;)

#by Secureworks
#
alert udp any any -> $HOME_NET 139 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (9)"; content:"|20 00|"; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF
6E E1 88|"; content:"|00 2E 00 2E 00 2F 00 2E 00 2E 00 2F|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250;
reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008698; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008698; rev:5;)

#by Secureworks
#
alert udp any any -> $HOME_NET 139 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (10)"; content:"|20 00|"; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF
6E E1 88|"; content:"|00 2E 00 2E 00 5C 00 2E 00 2E 00 5C|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250;
reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008699; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008699; rev:5;)

#by Secureworks
#
alert udp any any -> $HOME_NET 139 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 - Known Exploit Instance"; content:"|00 2e 00 2e 00 2f 00 2e 00 2e 00 2f
00 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 87|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-
4250; reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008700; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008700; rev:5;)

#by Secureworks
#
alert tcp any any -> $HOME_NET 445 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (11)"; flow:established,to_server; content:"|0B|"; offset:2; depth:1;
content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF 6E E1 88|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250;
reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008701; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008701; rev:5;)

#by Secureworks
#
alert tcp any any -> $HOME_NET 445 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (12)"; flow:established,to_server; content:"|1F 00|"; content:"|C8 4F 32
4B 70 16 D3 01 12 78 5A 47 BF 6E E1 88|"; content:"|5C|..|5C|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-
4250; reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008702; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008702; rev:6;)

#by Secureworks
#
alert tcp any any -> $HOME_NET 445 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (13)"; flow:established,to_server; content:"|1F 00|"; content:"|C8 4F 32
4B 70 16 D3 01 12 78 5A 47 BF 6E E1 88|"; content:"/../"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250;
reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008703; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008703; rev:5;)

#by Secureworks
#
alert tcp any any -> $HOME_NET 445 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (14)"; flow:established,to_server; content:"|1F 00|"; content:"|C8 4F 32
4B 70 16 D3 01 12 78 5A 47 BF 6E E1 88|"; content:"|00 2E 00 2E 00 2F 00 2E 00 2E 00 2F|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-
067.mspx; reference:cve,2008-4250; reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008704; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008704; rev:5;)

#by Secureworks
#
```

```
alert tcp any any -> $HOME_NET 445 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (15)"; flow:established,to_server; content:"|1F 00|"; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF 6E E1 88|"; content:"|00 2E 00 2E 00 5C 00 2E 00 2E 00 5C|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250; reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008705; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008705; rev:5;)

#by Secureworks
#
alert tcp any any -> $HOME_NET 139 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (16)"; flow:established,to_server; content:"|0B|"; offset:2; depth:1; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF 6E E1 88|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250; reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008706; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008706; rev:5;)

#by Secureworks
#
alert tcp any any -> $HOME_NET 139 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (17)"; flow:established,to_server; content:"|1F 00|"; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF 6E E1 88|"; content:"..|5C|..|5C|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250; reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008707; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008707; rev:6;)

#by Secureworks
#
alert tcp any any -> $HOME_NET 139 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (18)"; flow:established,to_server; content:"|1F 00|"; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF 6E E1 88|"; content:"../../"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250; reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008708; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008708; rev:5;)

#by Secureworks
#
alert tcp any any -> $HOME_NET 139 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (19)"; flow:established,to_server; content:"|1F 00|"; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF 6E E1 88|"; content:"|00 2E 00 2E 00 2F 00 2E 00 2E 00 2F|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250; reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008709; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008709; rev:5;)

#by Secureworks
#
alert tcp any any -> $HOME_NET 139 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (20)"; flow:established,to_server; content:"|1F 00|"; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF 6E E1 88|"; content:"|00 2E 00 2E 00 5C 00 2E 00 2E 00 5C|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250; reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008710; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008710; rev:5;)

#by Secureworks
#
##alert tcp any any -> $HOME_NET 445 (msg:"ET DELETED Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (21)"; flow:established,to_server; content:"|0B|"; offset:2; depth:1; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF 6E E1 88|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250; reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008711; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008711; rev:5;)

#by Secureworks
#
alert tcp any any -> $HOME_NET 445 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (22)"; flow:established,to_server; content:"|20 00|"; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF 6E E1 88|"; content:"|5C|..|5C|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250; reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008712; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008712; rev:6;)

#by Secureworks
#
alert tcp any any -> $HOME_NET 445 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (23)"; flow:established,to_server; content:"|20 00|"; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF 6E E1 88|"; content:"/../"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250; reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008713; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008713; rev:5;)

#by Secureworks
#
alert tcp any any -> $HOME_NET 445 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (24)"; flow:established,to_server; content:"|20 00|"; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF 6E E1 88|"; content:"|00 2E 00 2E 00 2F 00 2E 00 2E 00 2F|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250; reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008714; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008714; rev:5;)

#by Secureworks
#
alert tcp any any -> $HOME_NET 445 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (25)"; flow:established,to_server; content:"|20 00|"; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF 6E E1 88|"; content:"|00 2E 00 2E 00 5C 00 2E 00 2E 00 5C|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250; reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008715; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008715; rev:5;)

#by Secureworks
#
##alert tcp any any -> $HOME_NET 139 (msg:"ET DELETED Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (26)"; flow:established,to_server; content:"|0B|"; offset:2; depth:1; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF 6E E1 88|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250; reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008716; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008716; rev:5;)

#by Secureworks
#
alert tcp any any -> $HOME_NET 139 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (27)"; flow:established,to_server; content:"|20 00|"; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF 6E E1 88|"; content:"..|5C|..|5C|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250; reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008717; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008717; rev:6;)

#by Secureworks
#
alert tcp any any -> $HOME_NET 139 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (28)"; flow:established,to_server; content:"|20 00|"; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF 6E E1 88|"; content:"../../"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250; reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008718; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008718; rev:5;)

#by Secureworks
#
alert tcp any any -> $HOME_NET 139 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (29)"; flow:established,to_server; content:"|20 00|"; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF 6E E1 88|"; content:"|00 2E 00 2E 00 2F 00 2E 00 2E 00 2F|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250; reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008719; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008719; rev:5;)

#by Secureworks
#
alert tcp any any -> $HOME_NET 139 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (30)"; flow:established,to_server; content:"|20 00|"; content:"|C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF 6E E1 88|"; content:"|00 2E 00 2E 00 5C 00 2E 00 2E 00 5C|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250; reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008720; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008720; rev:5;)

#by Secureworks
#
alert tcp any any -> $HOME_NET 445 (msg:"ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 - Known Exploit Instance (2)"; flow:established,to_server; content:"|00 2e 00 2e 00 2f 00 2e 00 2e 00 2f 00 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 87|"; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; reference:cve,2008-4250; reference:url,www.kb.cert.org/vuls/id/827267; reference:url,doc.emergingthreats.net/bin/view/Main/2008721; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067; sid:2008721; rev:5;)
```

```
#by Blake Hartstein of Demarc
#
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 1433 (msg:"ET EXPLOIT MSSQL Hello Overflow Attempt"; flow:established,to_server; dsize:>400; content:"|12 01 00 34 00 00 00 00|"; offset:0;
depth:8; classtype:attempted-admin; reference:cve,2002-1123; reference:bugtraq,5411; reference:url,doc.emergingthreats.net/bin/view/Main/2002845;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MSSQL_Hello; sid:2002845; rev:5;)

#Submitted by Joseph Gama
#
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 1433 (msg:"ET EXPLOIT MS-SQL SQL Injection closing string plus line comment"; flow: to_server,established; content:"'|00|"; content:"-|00|-
|00|"; classtype: attempted-user; reference:url,www.nextgenss.com/papers/more_advanced_sql_injection.pdf; reference:url,www.securitymap.net/sdm/docs/windows/mssql-checklist.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2000488; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MSSQL_Injection; sid:2000488; rev:7;)

#Submitted by Joseph Gama
#
#alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 1433 (msg:"ET EXPLOIT MS-SQL SQL Injection running SQL statements line comment"; flow: to_server,established; content:"|3b 00|"; content:"-
|00|-|00|"; classtype: attempted-user; reference:url,www.nextgenss.com/papers/more_advanced_sql_injection.pdf; reference:url,www.securitymap.net/sdm/docs/windows/mssql-checklist.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2000372; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MSSQL_Injection; sid:2000372; rev:8;)

#Submitted by Joseph Gama
#
#alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 1433 (msg:"ET EXPLOIT MS-SQL SQL Injection line comment"; flow: to_server,established; content:"-|00|-|00|"; classtype: attempted-user;
reference:url,www.nextgenss.com/papers/more_advanced_sql_injection.pdf; reference:url,www.securitymap.net/sdm/docs/windows/mssql-checklist.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2000373; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MSSQL_Injection; sid:2000373; rev:7;)

#Submitted by Joseph Gama
#
alert udp $EXTERNAL_NET any -> $SQL_SERVERS 1434 (msg:"ET EXPLOIT MS-SQL heap overflow attempt"; content:"|08 3A 31|"; depth: 3; classtype: attempted-admin;
reference:url,www.nextgenss.com/papers/tp-SQL2000.pdf; reference:url,doc.emergingthreats.net/bin/view/Main/2000377; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MSSQL_Ping; sid:2000377; rev:7;)

#Submitted by Joseph Gama
#
alert udp $EXTERNAL_NET any -> $SQL_SERVERS 1434 (msg:"ET EXPLOIT MS-SQL DOS attempt (08)"; dsize: >1; content:"|08|"; depth: 1; content:!"|3A|"; offset: 1; depth: 1; classtype:
attempted-dos; reference:url,www.nextgenss.com/papers/tp-SQL2000.pdf; reference:url,doc.emergingthreats.net/bin/view/Main/2000378; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MSSQL_Ping; sid:2000378; rev:8;)

#Submitted by Joseph Gama
#
alert udp $EXTERNAL_NET any -> $SQL_SERVERS 1434 (msg:"ET EXPLOIT MS-SQL DOS attempt (08) 1 byte"; dsize: 1; content:"|08|"; depth: 1; classtype: attempted-dos;
reference:url,www.nextgenss.com/papers/tp-SQL2000.pdf; reference:url,doc.emergingthreats.net/bin/view/Main/2000379; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MSSQL_Ping; sid:2000379; rev:7;)

#Submitted by Joseph Gama
#
alert udp $EXTERNAL_NET any -> $SQL_SERVERS 1434 (msg:"ET EXPLOIT MS-SQL Spike buffer overflow"; content:"|12 01 00 34|"; depth: 4; classtype: attempted-admin; reference:bugtraq,5411;
reference:url,doc.emergingthreats.net/bin/view/Main/2000380; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MSSQL_Ping; sid:2000380; rev:9;)

#Submitted by Joseph Gama
#
alert udp $EXTERNAL_NET any -> $SQL_SERVERS 1434 (msg:"ET EXPLOIT MS-SQL DOS bouncing packets"; content:"|0A|"; depth: 1; classtype: attempted-dos;
reference:url,www.nextgenss.com/papers/tp-SQL2000.pdf; reference:url,doc.emergingthreats.net/bin/view/Main/2000381; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MSSQL_Ping; sid:2000381; rev:8;)

#by Jaime Blasco
#
#alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 1433 (msg:"ET EXPLOIT xp_servicecontrol access"; flow:to_server,established;
content:"x|00|p|00|_|00|s|00|e|00|r|00|v|00|i|00|c|00|e|00|c|00|o|00|n|00|t|00|r|00|o|00|l|00|"; nocase; classtype:attempted-user; reference:url,doc.emergingthreats.net/2009999;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MSSQL_Response; sid:2009999; rev:3;)

#by Jaime Blasco
#
#alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 1433 (msg:"ET EXPLOIT xp_fileexist access"; flow:to_server,established;
content:"x|00|p|00|_|00|f|00|i|00|l|00|e|00|e|00|x|00|i|00|s|00|t|00|"; nocase; classtype:attempted-user; reference:url,doc.emergingthreats.net/2010000;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MSSQL_Response; sid:2010000; rev:3;)

#by Jaime Blasco
#
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 1433 (msg:"ET EXPLOIT xp_enumerrorlogs access"; flow:to_server,established;
content:"x|00|p|00|_|00|e|00|n|00|u|00|m|00|e|00|r|00|r|00|o|00|r|00|l|00|o|00|g|00|s|00|"; nocase; classtype:attempted-user; reference:url,doc.emergingthreats.net/2010001;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MSSQL_Response; sid:2010001; rev:3;)

#by Jaime Blasco
#
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 1433 (msg:"ET EXPLOIT xp_readerrorlogs access"; flow:to_server,established;
content:"x|00|p|00|_|00|r|00|e|00|a|00|d|00|e|00|r|00|r|00|o|00|r|00|l|00|o|00|g|00|s|00|"; nocase; classtype:attempted-user; reference:url,doc.emergingthreats.net/2010002;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MSSQL_Response; sid:2010002; rev:4;)

#by Jaime Blasco
#
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 1433 (msg:"ET EXPLOIT xp_enumdsn access"; flow:to_server,established; content:"x|00|p|00|_|00|e|00|n|00|u|00|m|00|d|00|s|00|n|00|"; nocase;
classtype:attempted-user; reference:url,doc.emergingthreats.net/2010003; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MSSQL_Response; sid:2010003;
rev:4;)

#community-written, see docs. Moved from Current events, will be stable for the long term
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT MS ANI exploit"; flow:established,from_server; content:"RIFF"; nocase; content:"ACON"; nocase; content:"anih";
nocase; byte_test:4,>,36,0,relative, little; classtype:attempted-admin; reference:url,doc.emergingthreats.net/bin/view/Main/2003519; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS_ANI; sid:2003519; rev:8;)

#by Akash Mahajan of Stillsecure
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 143 (msg:"ET EXPLOIT MDAEMON (Post Auth) Remote Root IMAP FETCH Command Universal Exploit"; flow:established,to_server; content:"FLAGS BODY";
pcre:"/[0-9a-zA-Z]{200,}/R"; content:"|EB 06 90 90 8b 11 DC 64 90|"; distance:0; classtype:successful-user; reference:url,www.milw0rm.com/exploits/5248; reference:bugtraq,28245;
reference:url,doc.emergingthreats.net/bin/view/Main/2008063; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Mdaemon; reference:cve,2008-1358; sid:2008063;
rev:3;)

#By Mark Tombaugh
#
alert tcp $HOME_NET 143 -> $EXTERNAL_NET any (msg:"ET EXPLOIT Vulnerable Mercury 4.01a IMAP Banner"; flow: from_server,established; content:"IMAP4rev1 Mercury/32 v4.01a server ready";
flowbits:set,mercury.imap.401a; classtype:successful-recon-limited; reference:url,www.pmail.com/whatsnew/m32401.htm; reference:bugtraq,11775;
reference:url,doc.emergingthreats.net/bin/view/Main/2002389; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Mercury; sid:2002389; rev:4;)

#By Mark Tombaugh
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 143 (msg:"ET EXPLOIT Mercury v4.01a IMAP RENAME Buffer Overflow"; flow:established,to_server; flowbits:isset,mercury.imap.401a; content:"a001
RENAME"; pcre:"/[0-9A-Z]{240,}/smi"; classtype:misc-attack; reference:url,www.pmail.com/whatsnew/m32401.htm; reference:url,metasploit.com/projects/Framework/exploits.html#mercury_imap;
reference:bugtraq,11775; reference:url,doc.emergingthreats.net/bin/view/Main/2002390; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Mercury; sid:2002390;
rev:4;)

#by Alejandro Gramajo
##########################################################################
#x86 Pex Variable Length Fnstenv/mov/sub Double Word Xor Encoder
#D9 EE fldz
#D9 74 24 F4 fnstenv [esp - 12]
#5B pop ebx
#81 73 13 xorkey xor_xor: xor DWORD [ebx + 22], xorkey
#83 EB FC sub ebx,-4
#E2 F4 loop xor_xor
#Real traffic dump
#Content1
```

```
#98 49 F8 27 91 2F 27 48 4F 4E 6A 12 59 <D9 EE D9 .I.'./'HONj.Y...
#74 24 F4 5B 81 73 13> 2E D6 9A FE <83 EB FC E2 F4> t$.[.s..........
#Xorkey Content2
#
#alert tcp $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"ET SHELLCODE x86 PexFnstenvMov/Sub Encoder"; flow:established; content:"|D9 EE D9 74 24 F4 5B 81 73 13|"; content:"|83
EB FC E2 F4|"; distance: 4; within: 5; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/bin/view/Main/2002903; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2002903; rev:5;)

#########################################################################
#x86 Skylined\'s Alpha2 Alphanumeric Encoder
#
#alert tcp $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"ET SHELLCODE x86 Alpha2 GetEIPs Encoder"; flow:established; content:"|EB 03 59 EB 05 E8 F8 FF FF FF|";
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/bin/view/Main/2002904; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2002904; rev:5;)

#########################################################################
#x86 Call $+4 countdown xor encoder
#E8 FF FF FF call $+4
#FF C1 inc ecx
#5E pop esi
#30 4C 0E 07 xor_xor: xor [esi + ecx + 0x07], cl
#E2 FA loop xor_xor
#
#alert tcp $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"ET SHELLCODE x86 Countdown Encoder"; flow:established; content:"|E8 FF FF FF FF C1 5E 30 4C 0E 07 E2 FA|";
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/bin/view/Main/2002905; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2002905; rev:5;)

#########################################################################
#x86 Pex Alphanumeric Encoder
#VTX630VXH49HHHPhYAAQhZYYYYAAQQDDDd36FFFFTXVj0PPTUPPa301089 win32getpc
#?? JJJJJ ?? baseaddr
#VTX630VX4A0B6HH0B30BCVX2BDBH4A2AD0ADTBDQB0ADAVX4Z8BDJOM decoder
#
#alert tcp $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"ET SHELLCODE x86 PexAlphaNum Encoder"; flow:established;
content:"VTX630VXH49HHHPhYAAQhZYYYYAAQQDDDd36FFFFTXVj0PPTUPPa301089"; content:"JJJJJ"; distance: 2; within: 5; content:"VTX630VX4A0B6HH0B30BCVX2BDBH4A2AD0ADTBDQB0ADAVX4Z8BDJOM";
distance: 2; within: 55; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/bin/view/Main/2002906; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2002906; rev:5;)

#########################################################################
#x86 Pex Call $+4 Double Word Xor Encoder
#E8 FF FF FF call $+4
#FF C0 inc eax
#5E pop esi
#81 76 0E xorkey xor_xor: xor [esi + 0x0e], xorkey
#83 EE FC sub esi, -4
#E2 F4 loop xor_xor
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE x86 PexCall Encoder"; flow:established; content:"|E8 FF FF FF FF C0 5E 81 76 0E|"; content:"|82 EE FC E2 F4|"; distance:
4; within: 5; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/bin/view/Main/2002907; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2002907; rev:5;)

#########################################################################
#x86 IA32 Jmp/Call XOR Additive Feedback Decoder
#FC cld
#BB key mov ebx, key
#EB 0C jmp short 0x14
#5E pop esi
#56 push esi
#31 1E xor [esi], ebx
#AD lodsd
#01 C3 add ebx, eax
#85 C0 test eax, eax
#75 F7 jnz 0xa
#C3 ret
#E8 EF FF FF FF call 0x8
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE x86 JmpCallAdditive Encoder"; flow:established; content:"|FC BB|"; content:"|EB 0C 5E 56 31 1E AD 01 C3 85 C0 75 F7 C3
E8 EF FF FF FF|"; distance: 4; within: 19; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/bin/view/Main/2002908; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2002908; rev:5;)

#Metasploit BSD shellcode detect rules by h0f - Jennylab
#Alberto Garcia de Dios
#albertogdedios@andaluciajunta.es
#http://www.jennylab.org
#####
#METASPLOIT SHELLCODE RULES
#####
#BSD METASPLOIT RULES
#### BSD BIND SHELL #######
#BSD Bind Shell - ENCODE: PexFnstenvSub
#
#alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell"; content:"|83 e9 ec d9 ee d9 74 24 f4 5b 81 73 13|"; classtype:shellcode-detect;
reference:url,doc.emergingthreats.net/2010383; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010383; rev:2;)

#BSD Bind Shell - ENCODE: CountDown
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Countdown Encoded 2)"; content:"|82 ed 5f 4c 5d 52 43 78 03 d9 95 8f 84 49 4a 48 71 74 45
d3|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010385; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010385; rev:4;)

#BSD Bind Shell - ENCODE: CountDown
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Countdown Encoded 3)"; content:"|9f 90 4b ef a3 76 76 74 97 36 e4 aa bc 46 2f 77 45 6a 69
63|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010386; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010386; rev:3;)

#BSD Bind Shell - ENCODE: CountDown
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Countdown Encoded 4)"; content:"|64 65 f8 b6 7e 41 cc 6a 53 13 12 4d 57 28 6e 20 2a 2a cc
a5|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010387; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010387; rev:3;)

#BSD Bind Shell - ENCODE: CountDown
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Countdown Encoded 5)"; content:"|17 1c 1a 19 fb 77 80 ce|"; classtype:shellcode-detect;
reference:url,doc.emergingthreats.net/2010388; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010388; rev:3;)

#BSD Bind Shell - ENCODE: Pex
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Pex Encoded 1)"; content:"|c9 83 e9 ec e8 ff ff ff ff c0 5e 81 76 0e|"; classtype:shellcode-
detect; reference:url,doc.emergingthreats.net/2010389; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010389; rev:3;)

#BSD Bind Shell - ENCODE: Pex
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Pex Encoded 2)"; content:"|83 ee fc e2 f4|"; classtype:shellcode-detect;
reference:url,doc.emergingthreats.net/2010390; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010390; rev:3;)

#BSD Bind Shell - ENCODE: None
```

```
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Not Encoded 1)"; content:"|6a 61 58 99 52 68 10 02|"; classtype:shellcode-detect;
reference:url,doc.emergingthreats.net/2010391; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010391; rev:3;)

#BSD Bind Shell - ENCODE: None
#
#alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Not Encoded 2)"; content:"|89 e1 52 42 52 42 52 6a 10 cd 80 99 93 51 53 52 6a 68
58 cd|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010392; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010392; rev:2;)

#BSD Bind Shell - ENCODE: None
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Not Encoded 3)"; content:"|80 b0 6a cd 80 52 53 52 b0 1e cd 80 97 6a 02 59 6a 5a 58 51|";
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010393; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010393; rev:3;)

#BSD Bind Shell - ENCODE: None
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Not Encoded 4)"; content:"|57 51 cd 80 49 79 f5 50 68 2f 2f 73 68 68 2f 62 69 6e 89 e3|";
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010394; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010394; rev:3;)

#BSD Bind Shell - ENCODE: None
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Not Encoded 5)"; content:"|50 54 53 53 b0 3b cd 80|"; classtype:shellcode-detect;
reference:url,doc.emergingthreats.net/2010395; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010395; rev:3;)

#BSD Bind Shell - ENCODE: PexAlphaNum
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Pex Alphanumeric Encoded 1)"; content:"|eb 03 59 eb 05 e8 f8 ff ff ff 4f 49 49 49 49 49 51
5a 56|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010396; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010396; rev:3;)

#BSD Bind Shell - ENCODE: PexAlphaNum
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Pex Alphanumeric Encoded 2)"; content:"|54 58 36 33 30 56 58 34 41 30 42 36 48 48 30 42 33 30
42 43|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010397; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010397; rev:3;)

#BSD Bind Shell - ENCODE: PexAlphaNum
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Pex Alphanumeric Encoded 3)"; content:"|56 58 32 42 44 42 48 34 41 32 41 44 30 41 44 54 42 44
51 42|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010398; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010398; rev:3;)

#BSD Bind Shell - ENCODE: PexAlphaNum
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Pex Alphanumeric Encoded 4)"; content:"|30 41 44 41 56 58 34 5a 38 42 44 4a 4f 4d 4c 36 41|";
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010399; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010399; rev:3;)

#BSD Bind Shell - ENCODE: PexAlphaNum
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Pex Alphanumeric Encoded 5)"; content:"|41 4e 44 35 44 34 44|"; classtype:shellcode-detect;
reference:url,doc.emergingthreats.net/2010400; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010400; rev:3;)

#BSD Bind Shell - ENCODE: PexFstEnvMov
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (PexFstEnvMov Encoded 1)"; content:"|6a 14 59 d9 ee d9 74 24 f4 5b 81 73 13|";
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010401; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010401; rev:3;)

#BSD Bind Shell - ENCODE: PexFstEnvMov
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (PexFstEnvMov Encoded 2)"; content:"|83 eb fc e2 f4|"; classtype:shellcode-detect;
reference:url,doc.emergingthreats.net/2010402; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010402; rev:3;)

#BSD Bind Shell - ENCODE: JmpCallAditive
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (JmpCallAdditive Encoded)"; content:"|eb 0c 5e 56 31 1e ad 01 c3 85 c0 75 f7 c3 e8 ef ff ff
ff|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010403; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010403; rev:3;)

#BSD Bind Shell - ENCODE: Alpha2
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Alpha2 Encoded 1)"; content:"|eb 03 59 eb 05 e8 f8 ff ff ff 49 49 49 49 49 49 49 49 49|";
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010404; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010404; rev:3;)

#BSD Bind Shell - ENCODE: Alpha2
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Alpha2 Encoded 2)"; content:"|41 42 32 42 41 32 41 41 30 41 41 58|"; classtype:shellcode-
detect; reference:url,doc.emergingthreats.net/2010405; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010405; rev:3;)

#BSD Bind Shell - ENCODE: Alpha2
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Alpha2 Encoded 3)"; content:"|49 72 4e 4e 69 6b 53|"; classtype:shellcode-detect;
reference:url,doc.emergingthreats.net/2010406; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010406; rev:3;)

#BSD Reverse Shell - ENCODE: PexFnstenvSub
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Reverse shell (PexFnstenvSub Encoded 1)"; content:"|c9 83 e9 ef d9 ee d9 74 24 f4 5b 81 73 13|";
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010407; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010407; rev:3;)

#### EOF BSD BIND SHELL ######
### BSD REVERSE SHELL #######
#BSD Reverse Shell - ENCODE: PexFnstenvSub
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Reverse shell (PexFnstenvSub Encoded 2)"; content:"|83 eb fc e2 f4|"; classtype:shellcode-detect;
reference:url,doc.emergingthreats.net/2010408; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010408; rev:3;)

#BSD Reverse Shell - ENCODE: Countdown
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Reverse shell (Countdown Encoded 1)"; content:"|6a 43 59 e8 ff ff ff ff c1 5e 30 4c 0e 07 e2 fa 6b 63 5b
9d|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010409; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010409; rev:3;)

#BSD Reverse Shell - ENCODE: Countdown
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Reverse shell (Countdown Encoded 2)"; content:"|9f f6 72 09 4b 4b 4d 8a 74 7d 78 ec a2 49 26 7c 96 7d 79
7e|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010410; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010410; rev:3;)

#BSD Reverse Shell - ENCODE: Countdown
#
```

```
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Reverse shell (Countdown Encoded 3)"; content:"|7b e6 ac 64 57 d9 60 59 1d 1c 47 5d 5e 18 5a 50 54 b2 df
6d|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010411; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010411; rev:3;)

#BSD Reverse Shell - ENCODE: Countdown
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Reverse shell (Countdown Encoded 4)"; content:"|57 44 55 4a 5b 62|"; classtype:shellcode-detect;
reference:url,doc.emergingthreats.net/2010412; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010412; rev:3;)

#BSD Reverse Shell - ENCODE: Pex
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Reverse shell (Pex Encoded 1)"; content:"|c9 83 e9 ef e8 ff ff ff ff c0 5e 81 76 0e|";
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010413; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010413; rev:3;)

#BSD Reverse Shell - ENCODE: Pex
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Reverse shell (Pex Encoded 2)"; content:"|83 ee fc e2 f4|"; classtype:shellcode-detect;
reference:url,doc.emergingthreats.net/2010414; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010414; rev:3;)

#BSD Reverse Shell - ENCODE: None
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Reverse shell (Not Encoded 1)"; content:"|51 cd 80 49 79 f6 50 68 2f 2f 73 68 68 2f 62 69 6e 89 e3 50|";
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010415; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010415; rev:3;)

#BSD Reverse Shell - ENCODE: None
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Reverse shell (Not Encoded 2)"; content:"|6a 61 58 99 52 42 52 42 52 68|"; classtype:shellcode-detect;
reference:url,doc.emergingthreats.net/2010416; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010416; rev:3;)

#BSD Reverse Shell - ENCODE: None
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Reverse shell (Not Encoded 3)"; content:"|89 e1 6a 10 51 50 51 97 6a 62 58 cd 80 6a 02 59 b0 5a 51 57|";
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010417; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010417; rev:3;)

#BSD Reverse Shell - ENCODE: PexAlphaNum
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Reverse shell (Pex Alphanumeric Encoded 1)"; content:"|44 32 4d 4c 42 48 4a 46 42 31 44 50 50 41 4e 4f 49
38 41 4e|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010418; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010418; rev:3;)

#BSD Reverse Shell - ENCODE: PexAlphaNum
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Reverse shell (Pex Alphanumeric Encoded 2)"; content:"|4c 36 42 41 41 35 42 45 41 35 47 59 4c 36 44 56 4a
35 4d 4c|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010419; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010419; rev:3;)

#BSD Reverse Shell - ENCODE: PexAlphaNum
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Reverse shell (Pex Alphanumeric Encoded 3)"; content:"|56 58 32 42 44 42 48 34 41 32 41 44 30 41 44 54 42
44 51 42|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010420; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010420; rev:3;)

#BSD Reverse Shell - ENCODE: PexFnstenvMov
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Reverse shell (PexFnstenvMov Encoded 1)"; content:"|6a 11 59 d9 ee d9 74 24 f4 5b 81 73 13|";
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010421; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010421; rev:3;)

#BSD Reverse Shell - ENCODE: PexFnstenvMov
#
#alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Reverse shell (PexFnstenvMov Encoded 2)"; content:"|83 eb fc e2 f4|"; classtype:shellcode-detect;
reference:url,doc.emergingthreats.net/2010422; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010422; rev:3;)

#BSD Reverse Shell - ENCODE: JmpCallAditive
#
#alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Reverse shell (JmpCallAdditive Encoded 1)"; content:"|eb 0c 5e 56 31 1e ad 01 c3 85 c0 75 f7
c3 e8 ef ff ff ff|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010423; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010423; rev:2;)

#BSD Reverse Shell - ENCODE: Alpha2
#
#alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Reverse shell (Alpha2 Encoded 1)"; content:"|49 49 49 49 49 49 49 51 5a 6a|";
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010424; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010424; rev:2;)

#BSD Reverse Shell - ENCODE: Alpha2
#
#alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Reverse shell (Alpha2 Encoded 2)"; content:"|58 50 30 42 31 41 42 6b 42 41|";
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010425; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010425; rev:2;)

#BSD Reverse Shell - ENCODE: Alpha2
#
#alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Reverse shell (Alpha2 Encoded 3)"; content:"|32 41 41 30 41 41 58 50 38 42 42 75|";
classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010426; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010426; rev:2;)

##### EOF BSD Reverse Shell#####
##### BSD SPARC Bind Shell #########
#BSD SPARC Bind Shell - ENCODE: SPARC
#
#alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD SPARC Bind shell (SPARC Encoded 1)"; content:"|20 bf ff ff 20 bf ff ff 7f ff ff ff ea 03 e0
20 aa 9d 40 11|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010427; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010427; rev:2;)

##### EOF BSD Reverse Shell#####
##### BSD SPARC Bind Shell #########
#BSD SPARC Bind Shell - ENCODE: SPARC
#
#alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD SPARC Bind shell (SPARC Encoded 2)"; content:"|ea 23 e0 20 a2 04 40 15 81 db e0 20 12 bf ff
fb 9e 03 e0 04|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010428; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010428; rev:2;)

#BSD SPARC Bind Shell - ENCODE: None
#
#alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD SPARC Bind shell (Not Encoded 1)"; content:"|e0 23 bf f0 c0 23 bf f4 92 23 a0 10 94 10 20 10
82 10 20 68|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010429; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010429; rev:2;)

#BSD SPARC Bind Shell - ENCODE: None
#
#alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD SPARC Bind shell (Not Encoded 2)"; content:"|91 d0 20 08 d0 03 bf f8 92 10 20 01 82 10 20 6a
91 d0 20 08|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010430; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010430; rev:2;)

#BSD SPARC Bind Shell - ENCODE: None
#
```

```
#alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD SPARC Bind shell (Not Encoded 3)"; content:"|d0 03 bf f8 92 1a 40 09 94 12 40 09 82 10 20 1e
91 d0 20 08|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010431; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010431; rev:2;)

#BSD SPARC Bind Shell - ENCODE: None
#
#alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD SPARC Bind shell (Not Encoded 4)"; content:"|23 0b dc da 90 23 a0 10 92 23 a0 08 e0 3b bf f0
d0 23 bf f8|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010432; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010432; rev:2;)

#### EOF BSD SPARC Bind Shell #########4
### BSD SPARC Reverse Shell ########
#BSD SPARC Reverse Shell - ENCODE: None
#
#alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD SPARC Reverse shell (Not Encoded 1)"; content:"|9c 2b a0 07 94 1a c0 0b 92 10 20 01 90 10 20
02 82 10 20 61|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010433; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010433; rev:2;)

#### EOF BSD SPARC Bind Shell #########4
### BSD SPARC Reverse Shell ########
#BSD SPARC Reverse Shell - ENCODE: None
#
#alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD SPARC Reverse shell (Not Encoded 2)"; content:"|91 d0 20 08 d0 23 bf f8 92 10 20 03 92 a2 60
01 82 10 20 5a|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010434; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010434; rev:2;)

#### EOF BSD SPARC Bind Shell #########4
### BSD SPARC Reverse Shell ########
#BSD SPARC Reverse Shell - ENCODE: None
#
#alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD SPARC Reverse shell (Not Encoded 3)"; content:"|91 d0 20 08 12 bf ff fd d0 03 bf f8 21 3f
c0|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010437; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders;
sid:2010437; rev:2;)

#BSD SPARC Reverse Shell - ENCODE: SPARC
#
#alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD SPARC Reverse shell (SPARC Encoded 1)"; content:"|20 bf ff ff 20 bf ff ff 7f ff ff ff ea 03
e0 20 aa 9d 40 11|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010435; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010435; rev:2;)

#BSD SPARC Reverse Shell - ENCODE: SPARC
#
#alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD SPARC Reverse shell (SPARC Encoded 2)"; content:"|ea 23 e0 20 a2 04 40 15 81 db e0 20 12 bf
ff fb 9e 03 e0 04|"; classtype:shellcode-detect; reference:url,doc.emergingthreats.net/2010436; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Metasploit_Encoders; sid:2010436; rev:2;)

#### EOF BSD SPARC Reverse Shell ####
#Erik Fichtner
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT CAN-2005-0399 Gif Vuln via http"; flow: from_server,established; content:"GIF89a"; content:"|21 ff 0b|NETSCAPE2.0";
byte_test:1,!=,3,0,relative; classtype: attempted-admin; reference:cve,2005-0399; reference:url,doc.emergingthreats.net/bin/view/Main/2001807; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Mozilla-Firefox; sid:2001807; rev:8;)

#By Joel Esler
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 9999 (msg:"ET EXPLOIT MySQL MaxDB Buffer Overflow"; flow: to_server,established; content:"GET"; content:"|31 c9 83 e9 af d9 ee|";
pcre:"/(GET).\/%.{1586,}/i"; classtype: attempted-admin; reference:url,doc.emergingthreats.net/bin/view/Main/2001988; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MySQL_MaxDB; sid:2001988; rev:4;)

#
alert tcp $EXTERNAL_NET any -> $HOME_NET 139 (msg:"ET NETBIOS NII Microsoft ASN.1 Library Buffer Overflow Exploit"; flow: to_server,established; content:"|A1 05 23 03 03 01 07|";
classtype: bad-unknown; reference:url,www.microsoft.com/technet/security/bulletin/ms04-007.asp; reference:url,doc.emergingthreats.net/bin/view/Main/2000017;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_NETBIOS_ASN1_Overflow; sid:2000017; rev:6;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 143 (msg:"ET EXPLOIT Possible Novell Groupwise Internet Agent CREATE Verb Stack Overflow Attempt"; flow:established,to_server; content:"|41 30
30 31|"; depth:4; content:"CREATE "; within:10; isdataat:500,relative; content:!"|0A|"; within:500; classtype:attempted-admin; reference:url,www.exploit-db.com/exploits/14379/;
reference:url,www.zerodayinitiative.com/advisories/ZDI-10-129/; reference:url,www.novell.com/support/php/search.do?
cmd=displayKC&docType=kc&externalId=7006374&sliceId=2&docTypeID=DT_TID_1_1&dialogID=155271264&stateId=0 0 155267598; reference:url,doc.emergingthreats.net/2011235;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Novell; sid:2011235; rev:2;)

#By Michael Hale Ligh and Ryan Smith
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 8028 (msg:"ET EXPLOIT Novell HttpStk Remote Code Execution Attempt /nds"; flow:to_server,established; content:"/nds"; depth:10; nocase;
content:"|0d0a|Host|3a|"; nocase; content:!"|0d0a|"; within:56; classtype:web-application-attack; reference:url,doc.emergingthreats.net/bin/view/Main/2003145;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Novell_HTTPSTK; sid:2003145; rev:3;)

#By Michael Hale Ligh and Ryan Smith
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 8028 (msg:"ET EXPLOIT Novell HttpStk Remote Code Execution Attempt /dhost"; flow:to_server,established; content:"/dhost"; depth:10; nocase;
content:"|0d0a|Host|3a|"; nocase; content:!"|0d0a|"; within:56; classtype:web-application-attack; reference:url,doc.emergingthreats.net/bin/view/Main/2003146;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Novell_HTTPSTK; sid:2003146; rev:3;)

#By Michael Hale Ligh and Ryan Smith
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 8028 (msg:"ET EXPLOIT Novell HttpStk Remote Code Execution Attempt /nds (linewrap)"; flow:to_server,established; content:"/nds"; depth:10;
nocase; content:"|0d0a|Host|3a|"; nocase; content:"|0d0a20|"; within:56; classtype:web-application-attack; reference:url,doc.emergingthreats.net/bin/view/Main/2003148;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Novell_HTTPSTK; sid:2003148; rev:3;)

#By Michael Hale Ligh and Ryan Smith
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 8028 (msg:"ET EXPLOIT Novell HttpStk Remote Code Execution Attempt /dhost (linewrap)"; flow:to_server,established; content:"/dhost"; depth:10;
nocase; content:"|0d0a|Host|3a|"; nocase; content:"|0d0a20|"; within:56; classtype:web-application-attack; reference:url,doc.emergingthreats.net/bin/view/Main/2003147;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Novell_HTTPSTK; sid:2003147; rev:3;)

#by Akash Mahajan
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 8800 (msg:"ET EXPLOIT Now SMS/MMS Gateway HTTP BOF Vulnerability"; flow:established,to_server; content:"GET "; depth:4;
content:"Authorization|3a|"; distance:0; content:"Basic"; distance:0; pcre:"/Authorization\x3a\s*Basic\s*[a-zA-Z0-9]{255,}==/i"; classtype:web-application-attack;
reference:bugtraq,27896; reference:url,aluigi.altervista.org/adv/nowsmsz-adv.txt; reference:url,doc.emergingthreats.net/bin/view/Main/2007874; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Now_SMS; sid:2007874; rev:6;)

#by Akash Mahajan
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 2775 (msg:"ET EXPLOIT Now SMS/MMS Gateway SMPP BOF Vulnerability"; flow:established,to_server; content:"|00 00 00 04|"; content:"|00 00 00
01|"; distance:1; pcre:"/[a-zA-Z0-9]{1000,}/i"; classtype:web-application-attack; reference:bugtraq,27896; reference:url,aluigi.altervista.org/adv/nowsmsz-adv.txt;
reference:url,doc.emergingthreats.net/bin/view/Main/2007875; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Now_SMS; sid:2007875; rev:4;)

#by Fabien Bourdaire of ECSC Security
#Re: http://www.internetdefence.net/2007/02/06/Javascript-payload
#bc d3 c3 d2 c9 d0 d4 <SCRIPT
#bc f3 e3 f2 e9 f0 f4 <script
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT US-ASCII Obfuscated script"; flow:established,from_server; content:"US-ASCII"; nocase; pcre:"/\xbc[\xf3\xd3]
[\xe3\xc3][\xf2\xd2][\xe9\xc9][\xf0\xd0][\xf4\xd4]/"; classtype:web-application-attack; reference:url,www.internetdefence.net/2007/02/06/Javascript-payload; reference:cve,2006-3227;
reference:url,www.securityfocus.com/archive/1/437948/30/0/threaded; reference:url,doc.emergingthreats.net/bin/view/Main/2003400; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Obfuscated_Scripting; sid:2003400; rev:3;)
```

```
#ae ef f0 e5 ee a0 a2 e7 e5 f4 a2 .open "get"
#ae cf d0 c5 ce a0 a2 c7 c5 d4 a2 .OPEN "GET"
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT US-ASCII Obfuscated VBScript download file"; flow:established,from_server; content:"US-ASCII"; nocase;
pcre:"/\xae[\xef\xcf][\xf0\xd0][\xe5\xc5][\xee\xce]\xa0\xa2[\xe7\xc7][\xe5\xc5][\xf4\xd4]\xa2/"; classtype:web-application-attack;
reference:url,www.internetdefence.net/2007/02/06/Javascript-payload; reference:cve,2006-3227; reference:url,www.securityfocus.com/archive/1/437948/30/0/threaded;
reference:url,doc.emergingthreats.net/bin/view/Main/2003401; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Obfuscated_Scripting; sid:2003401; rev:4;)

#f3 e8 e5 ec ec e5 f8 e5 e3 f5 f4 e5 shellexecute
#d3 c8 c5 cc cc c5 d8 c5 c3 d5 d4 c5
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT US-ASCII Obfuscated VBScript execute command"; flow:established,from_server; content:"US-ASCII"; nocase;
pcre:"/[\xf3\xd3][\xe8\xc8][\xe5\xc5][\xec\xcc][\xec\xcc][\xe5\xc5][\xf8\xd8][\xe5\xc5][\xe3\xc3][\xf5\xd5][\xf4\xd4][\xe5\xc5]/"; classtype:web-application-attack;
reference:url,www.internetdefence.net/2007/02/06/Javascript-payload; reference:cve,2006-3227; reference:url,www.securityfocus.com/archive/1/437948/30/0/threaded;
reference:url,doc.emergingthreats.net/bin/view/Main/2003402; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Obfuscated_Scripting; sid:2003402; rev:4;)

#f6 e2 f3 e3 f2 e9 f0 f4
#d6 c2 d3 c3 d2 c9 d0 d4 VBSCRIPT
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT US-ASCII Obfuscated VBScript"; flow:established,from_server; content:"US-ASCII"; nocase; pcre:"/[\xf6\xd6]
[\xe2\xc2][\xf3\xd3][\xe3\xc3][\xf2\xd2][\xe9\xc9][\xf0\xd0][\xf4\xd4]/"; classtype:web-application-attack; reference:url,www.internetdefence.net/2007/02/06/Javascript-payload;
reference:cve,2006-3227; reference:url,www.securityfocus.com/archive/1/437948/30/0/threaded; reference:url,doc.emergingthreats.net/bin/view/Main/2003403;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Obfuscated_Scripting; sid:2003403; rev:3;)

#by Blake Hartstein of Demarc
#
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS $ORACLE_PORTS (msg:"ET EXPLOIT SYS get_domain_index_metadata Privilege Escalation Attempt"; flow:established,to_server;
content:"ODCIIndexMetadata"; nocase; content:"sys.dbms_export_extension.get_domain_index_metadata"; nocase; classtype:attempted-admin; reference:bugtraq,17699;
reference:url,doc.emergingthreats.net/bin/view/Main/2002886; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Oracle; sid:2002886; rev:3;)

#by Blake Hartstein of Demarc
#
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS $ORACLE_PORTS (msg:"ET EXPLOIT SYS get_domain_index_tables Access"; flow:established,to_server;
content:"sys.dbms_export_extension.get_domain_index_tables"; nocase; classtype:attempted-admin; reference:bugtraq,17699; reference:url,doc.emergingthreats.net/bin/view/Main/2002887;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Oracle; sid:2002887; rev:4;)

#by Blake Hartstein of Demarc
#
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS $ORACLE_PORTS (msg:"ET EXPLOIT SYS get_v2_domain_index_tables Privilege Escalation Attempt"; flow:established,to_server;
content:"ODCIIndexUtilGetTableNames"; nocase; content:"sys.dbms_export_extension.get_v2_domain_index_tables"; nocase; classtype:attempted-admin; reference:bugtraq,17699;
reference:url,doc.emergingthreats.net/bin/view/Main/2002888; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Oracle; sid:2002888; rev:4;)

#by Greg Martin
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET EXPLOIT Oracle WebLogic IIS connector JSESSIONID Remote Overflow Exploit"; flow:to_server,established; uricontent:".jsp?";
nocase; uricontent:"JSESSIONID="; nocase; isdataat:5132; classtype:attempted-admin; reference:cve,2008-5457; reference:url,infosec20.blogspot.com/2009/04/oracle-weblogic-iis-remote-
buffer.html; reference:url,doc.emergingthreats.net/2009216; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Oracle; sid:2009216; rev:6;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $ORACLE_PORTS (msg:"ET EXPLOIT Possible Oracle Database Text Component ctxsys.drvxtabc.create_tables Remote SQL Injection Attempt";
flow:established,to_server; content:"ctxsys|2E|drvxtabc|2E|create|5F|tables"; nocase; content:"dbms|5F|sql|2E|execute"; nocase; distance:0;
pcre:"/ctxsys\x2Edrvxtabc\x2Ecreate\x5Ftables.+(SELECT|DELETE|CREATE|INSERT|UPDATE|OUTFILE)/si"; classtype:attempted-admin; reference:url,www.securityfocus.com/bid/36748;
reference:cve,2009-1991; reference:url,doc.emergingthreats.net/2010375; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Oracle; sid:2010375; rev:2;)

#Mark Tombaugh
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET EXPLOIT XML-RPC for PHP Remote Code Injection"; flow:established,to_server; content:"POST "; depth:5; nocase;
uricontent:"xmlrpc.php"; content:"methodCall"; nocase; pcre:"/>.*\'\s*\)\s*\)*\s*\;/"; classtype: web-application-attack; reference:url,www.securityfocus.com/bid/14088/exploit;
reference:cve,2005-1921; reference:url,doc.emergingthreats.net/bin/view/Main/2002158; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_PHP; sid:2002158;
rev:7;)

#by Steve Adair steven@securityzone - 11/28/2006, updates from Mat Rowley
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET EXPLOIT FTP .message file write"; flow:to_server,established; content:"STOR "; nocase; depth:5; content:".message|0d 0a|";
distance:0; pcre:"/[^a-zA-Z0-9]+\.message/"; flowbits:set,BE.ftp.message; classtype:misc-attack; reference:url,www.milw0rm.com/exploits/2856;
reference:url,doc.emergingthreats.net/bin/view/Main/2003196; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_ProFTPD; sid:2003196; rev:7;)

#by Steve Adair steven@securityzone - 11/28/2006, updates from Mat Rowley
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET EXPLOIT ProFTPD .message file overflow attempt"; flowbits:isset,BE.ftp.message; flow:to_server,established; content:"CWD "; depth:4;
nocase; flowbits:unset,BE.ftp.message; classtype:misc-attack; reference:url,www.milw0rm.com/exploits/2856; reference:url,doc.emergingthreats.net/bin/view/Main/2003197;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_ProFTPD; sid:2003197; rev:6;)

#Submitted by Matt Jonkman, Updated by Abe and Matt Sheridan
#
alert tcp any any -> $HOME_NET 139 (msg:"ET EXPLOIT Pwdump3e Session Established Reg-Entry port 139"; flow: to_server,established; content:"|53 00 4f 00 46 00 54 00 57 00 41 00 52 00 45
00 5c 00 45 00 62 00 69 00 7a 00 5c 00 68 00 61 00 73 00 68|"; classtype: suspicious-login; reference:url,doc.emergingthreats.net/bin/view/Main/2000565;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Pwdump_Fgdump; sid:2000565; rev:8;)

#Submitted by Matt Jonkman, Updated by Abe and Matt Sheridan
#
alert tcp any any -> $HOME_NET 445 (msg:"ET EXPLOIT Pwdump3e Session Established Reg-Entry port 445"; flow: to_server,established; content:"|53 00 4f 00 46 00 54 00 57 00 41 00 52 00 45
00 5c 00 45 00 62 00 69 00 7a 00 5c 00 68 00 61 00 73 00 68|"; classtype: suspicious-login; reference:url,doc.emergingthreats.net/bin/view/Main/2000566;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Pwdump_Fgdump; sid:2000566; rev:8;)

#Submitted by Matt Jonkman, Updated by Abe and Matt Sheridan
#
alert tcp any any -> $HOME_NET 445 (msg:"ET EXPLOIT Pwdump3e pwservice.exe Access port 445"; flow: to_server,established;
content:"p|00|w|00|s|00|e|00|r|00|v|00|i|00|c|00|e|00|.|00|e|00|x|00|e"; classtype: misc-attack; reference:url,doc.emergingthreats.net/bin/view/Main/2000564;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Pwdump_Fgdump; sid:2000564; rev:9;)

#Submitted by Matt Jonkman, Updated by Abe and Matt Sheridan
#
alert tcp any any -> $HOME_NET 139 (msg:"ET EXPLOIT Pwdump3e pwservice.exe Access port 139"; flow: to_server,established;
content:"p|00|w|00|s|00|e|00|r|00|v|00|i|00|c|00|e|00|.|00|e|00|x|00|e"; classtype: misc-attack; reference:url,doc.emergingthreats.net/bin/view/Main/2000567;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Pwdump_Fgdump; sid:2000567; rev:8;)

#Submitted by Matt Jonkman, Updated by Abe and Matt Sheridan
#
alert tcp $HOME_NET 445 -> any any (msg:"ET EXPLOIT Pwdump3e Password Hash Retrieval port 445"; flow: from_server,established; content:"|3a 00|5|00|0|00|0|3a|"; classtype: misc-attack;
reference:url,doc.emergingthreats.net/bin/view/Main/2000563; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Pwdump_Fgdump; sid:2000563; rev:11;)

#Submitted by Matt Jonkman, Updated by Abe and Matt Sheridan
#
alert tcp $HOME_NET 139 -> any any (msg:"ET EXPLOIT Pwdump3e Password Hash Retrieval port 139"; flow: from_server,established; content:"|3a 00|5|00|0|00|0|3a|"; classtype: misc-attack;
reference:url,doc.emergingthreats.net/bin/view/Main/2000568; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Pwdump_Fgdump; sid:2000568; rev:10;)

#Submitted by Abe Use
#
alert tcp any any -> $HOME_NET 139 (msg:"ET EXPLOIT NTDump.exe Service Started port 139"; flow: to_server,established; content:"|4e 00 74 00 44 00 75 00 6d 00 70 00 53 00 76 00 63 00 2e
00 65 00 78 00 65 00|"; classtype: misc-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001053; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Pwdump_Fgdump; sid:2001053; rev:7;)

#Submitted by Abe Use
#
alert tcp any any -> $HOME_NET 445 (msg:"ET EXPLOIT NTDump.exe Service Started port 445"; flow: to_server,established; content:"|4e 00 74 00 44 00 75 00 6d 00 70 00 53 00 76 00 63 00 2e
00 65 00 78 00 65 00|"; classtype: misc-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001544; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Pwdump_Fgdump; sid:2001544; rev:7;)
```

```
#Submitted by Abe Use
#
alert tcp any any -> $HOME_NET 139 (msg:"ET EXPLOIT NTDump Session Established Reg-Entry port 139"; flow: to_server,established; content:"|53 00 4f 00 46 00 54 00 57 00 41 00 52 00 45
00 5c 00 4e 00 74 00 44 00 75 00 6d 00 70 00|"; classtype: misc-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001052; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Pwdump_Fgdump; sid:2001052; rev:8;)

#Submitted by Abe Use
#
alert tcp any any -> $HOME_NET 445 (msg:"ET EXPLOIT NTDump Session Established Reg-Entry port 445"; flow: to_server,established; content:"|53 00 4f 00 46 00 54 00 57 00 41 00 52 00 45
00 5c 00 4e 00 74 00 44 00 75 00 6d 00 70 00|"; classtype: misc-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001543; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Pwdump_Fgdump; sid:2001543; rev:7;)

#Submitted by Abe Use
#
alert tcp any any -> $HOME_NET 139 (msg:"ET EXPLOIT Pwdump4 Session Established GetHash port 139"; flow: to_server,established; content:"|50 57 44 75 6d 70 34 2e 64 6c 6c 00 47 65 74 48
61 73 68|"; classtype: suspicious-login; reference:url,doc.emergingthreats.net/bin/view/Main/2001753; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Pwdump_Fgdump; sid:2001753; rev:4;)

#Submitted by Abe Use
#
alert tcp any any -> $HOME_NET 445 (msg:"ET EXPLOIT Pwdump4 Session Established GetHash port 445"; flow: to_server,established; content:"|50 57 44 75 6d 70 34 2e 64 6c 6c 00 47 65 74 48
61 73 68|"; classtype: suspicious-login; reference:url,doc.emergingthreats.net/bin/view/Main/2001754; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Pwdump_Fgdump; sid:2001754; rev:4;)

#by Rich Rumble
#
alert tcp any any -> $HOME_NET 139:445 (msg:"ET EXPLOIT PWDump4 Password dumping exe copied to victim"; flow:to_server,established; content:"|4F 00 72 00 69 00 67 00 69 00 6E 00 61 00
6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 50 00 57 00 44 00 55 00 4D 00 50 00 34 00 2E 00 65 00 78 00 65|"; classtype:suspicious-filename-detect;
reference:url,xinn.org/Snort-pwdump4.html; reference:url,doc.emergingthreats.net/bin/view/Main/2008444; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Pwdump_Fgdump; sid:2008444; rev:2;)

#PWDump6
#
alert tcp any any -> $HOME_NET 139:445 (msg:"ET EXPLOIT Pwdump6 Session Established test file created on victim"; flow:to_server,established; content:"|5c 00 74 00 65 00 73 00 74 00 2e
00 70 00 77 00 64|"; classtype:suspicious-filename-detect; reference:url,xinn.org/Snort-pwdump6.html; reference:url,doc.emergingthreats.net/bin/view/Main/2008445;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Pwdump_Fgdump; sid:2008445; rev:2;)

#This should catch both FGDump and PWDump
#
alert tcp any any -> $HOME_NET 139:445 (msg:"ET EXPLOIT Foofus.net Password dumping, dll injection"; flow:to_server,established; content:"|6c 00 73 00 72 00 65 00 6d 00 6f 00 72 00
61|"; classtype:suspicious-filename-detect; reference:url,xinn.org/Snort-fgdump.html; reference:url,doc.emergingthreats.net/bin/view/Main/2008476;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Pwdump_Fgdump; sid:2008476; rev:2;)

#by Kyle Haugsness, Erik Fichtner, and Matt Jonkman
#VNC State Machine, good for other uses
#VNC is easy to run on any port, so ranges are not in use for now...
#Server offers version
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET EXPLOIT VNC Possible Vulnerable Server Response"; flow:established; dsize:12; content:"RFB 003.00"; depth:11; flowbits:noalert;
flowbits:set,BSposs.vuln.vnc.svr; classtype:misc-activity; reference:url,www.realvnc.com/docs/rfbproto.pdf; reference:cve,2006-2369;
reference:url,doc.emergingthreats.net/bin/view/Main/2002912; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_RealVNC; sid:2002912; rev:7;)

#Client replies in kind
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET EXPLOIT VNC Client response"; flowbits:isset,BSposs.vuln.vnc.svr; flow:established; dsize:12; content:"RFB 003.0"; depth:9;
flowbits:noalert; flowbits:set,BSis.vnc.setup; classtype:misc-activity; reference:url,www.realvnc.com/docs/rfbproto.pdf; reference:url,doc.emergingthreats.net/bin/view/Main/2002913;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_RealVNC; sid:2002913; rev:7;)

#Server says it requires VNC auth, and sends 16 byte salt
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET EXPLOIT VNC Server VNC Auth Offer"; flowbits:isset,BSis.vnc.setup; flow:established; dsize:20; content:"|00 00 00 02|"; depth:4;
flowbits:noalert; flowbits:set,BSvnc.auth.offered; classtype:misc-activity; reference:url,www.realvnc.com/docs/rfbproto.pdf; reference:url,doc.emergingthreats.net/bin/view/Main/2002914;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_RealVNC; sid:2002914; rev:6;)

#or server replies like so, same thing as above, different method. For some reason some servers do not send the challenge with the auth offer
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET EXPLOIT VNC Server VNC Auth Offer - No Challenge string"; flowbits:isset,BSis.vnc.setup; flow:established; dsize:2; content:"|01
02|"; depth:2; flowbits:noalert; flowbits:set,BSvnc.auth.offered; classtype:misc-activity; reference:url,www.realvnc.com/docs/rfbproto.pdf;
reference:url,doc.emergingthreats.net/bin/view/Main/2002918; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_RealVNC; sid:2002918; rev:6;)

#or, unrelated, if server says it allows no auth. Could be a compromised server
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET EXPLOIT VNC Server Not Requiring Authentication"; flowbits:isset,BSis.vnc.setup; flow:established; content:"|01 01|"; depth:2;
flowbits:set,BSvnc.auth.offered; flowbits:unset,BSis.vnc.setup; flowbits:unset,BSvnc.auth.offered; classtype:misc-activity; reference:url,www.realvnc.com/docs/rfbproto.pdf;
reference:cve,2006-2369; reference:url,doc.emergingthreats.net/bin/view/Main/2002924; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_RealVNC; sid:2002924;
rev:7;)

#and in the other client style case
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET EXPLOIT VNC Server Not Requiring Authentication (case 2)"; flowbits:isset,BSis.vnc.setup; dsize:4; flow:established; content:"|00
00 00 01|"; depth:4; flowbits:set,BSvnc.auth.offered; classtype:misc-activity; reference:url,www.realvnc.com/docs/rfbproto.pdf; reference:cve,2006-2369;
reference:url,doc.emergingthreats.net/bin/view/Main/2002923; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_RealVNC; sid:2002923; rev:6;)

#and the client in this scenario replies with a |02| to ask for normal pass auth, this ends the chain as a good exchange
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET EXPLOIT VNC Good Authentication Reply"; flowbits:isset,BSvnc.auth.offered; flow:established; dsize:2; content:"|02|";
flowbits:unset,BSvnc.auth.offered; flowbits:noalert; flowbits:set,BSvnc.auth.agreed; classtype:attempted-admin; reference:url,www.realvnc.com/docs/rfbproto.pdf;
reference:url,doc.emergingthreats.net/bin/view/Main/2002919; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_RealVNC; sid:2002919; rev:7;)

#if client replies with hashed salt chain ends, this is not an exploit attempt
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET EXPLOIT VNC Authentication Reply"; flowbits:isset,BSvnc.auth.offered; flow:established; dsize:16;
flowbits:unset,BSvnc.auth.offered; flowbits:noalert; flowbits:set,BSvnc.auth.agreed; classtype:attempted-admin; reference:url,www.realvnc.com/docs/rfbproto.pdf;
reference:url,doc.emergingthreats.net/bin/view/Main/2002915; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_RealVNC; sid:2002915; rev:6;)

#if client replies it wants null auth, this is an exploit ATTEMPT
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET EXPLOIT RealVNC Authentication Bypass Attempt"; flowbits:isset,BSvnc.auth.offered; flow:established; dsize:1; content:"|01|";
depth:1; flowbits:set,BSvnc.null.auth.sent; classtype:attempted-admin; reference:url,secunia.com/advisories/20107/; reference:url,archives.neohapsis.com/archives/fulldisclosure/2006-
05/0356.html; reference:cve,2006-2369; reference:url,doc.emergingthreats.net/bin/view/Main/2002916; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_RealVNC; sid:2002916; rev:6;)

#if server replies with auth successful this is a successful exploit
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET EXPLOIT RealVNC Server Authentication Bypass Successful"; flowbits:isset,BSvnc.null.auth.sent; flow:established; dsize:4;
content:"|00 00 00 00|"; depth:4; classtype:successful-admin; flowbits:unset,BSis.vnc.setup; flowbits:unset,BSvnc.auth.offered; reference:url,secunia.com/advisories/20107/;
reference:url,archives.neohapsis.com/archives/fulldisclosure/2006-05/0356.html; reference:cve,2006-2369; reference:url,doc.emergingthreats.net/bin/view/Main/2002917;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_RealVNC; sid:2002917; rev:6;)

#This is a good auth back from the server, in 2002922 in the policy ruleset
#this is for a server saying auth failed, in 2002920 in the policy ruleset
#This is for too many failures
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET EXPLOIT VNC Multiple Authentication Failures"; flowbits:isset,BSvnc.auth.agreed; flow:established; dsize:<50; content:"|00 00 00
02|"; depth:4; classtype:attempted-admin; reference:url,www.realvnc.com/docs/rfbproto.pdf; reference:url,doc.emergingthreats.net/bin/view/Main/2002921;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_RealVNC; sid:2002921; rev:6;)
```

```
#by Adam Pointon at sentinelsecurity.com.au
#
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 1433 (msg:"ET EXPLOIT SQL sp_configure - configuration change"; flow:to_server,established;
content:"s|00|p|00|_|00|c|00|o|00|n|00|f|00|i|00|g|00|u|00|r|00|e|00|"; nocase; classtype:attempted-user; reference:url,msdn.microsoft.com/en-us/library/ms190693.aspx;
reference:url,doc.emergingthreats.net/bin/view/Main/2008517; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_SQL_XP_cmdshell; sid:2008517; rev:2;)

#by Adam Pointon at sentinelsecurity.com.au
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET EXPLOIT SQL sp_configure attempt"; flow:to_server,established; content:"sp_configure"; nocase; classtype:attempted-
user; reference:url,msdn.microsoft.com/en-us/library/ms190693.aspx; reference:url,doc.emergingthreats.net/bin/view/Main/2008518; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_SQL_XP_cmdshell; sid:2008518; rev:2;)

#
alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"ET NETBIOS LSA exploit"; flow: to_server,established;
content:"|31313131313131313131313131313131313131313131313131313131313131313131313131313131313131313131313131313131313131313131313131313131313131313131313131313131313131313131313131313131313131313131313131313131313131313131313131313131313
13131313131313131|"; offset: 78; depth: 192; classtype: misc-activity; reference:url,www.eeye.com/html/research/advisories/AD20040501.html;
reference:url,www.upenn.edu/computing/virus/04/w32.sasser.worm.html; reference:url,doc.emergingthreats.net/bin/view/Main/2000032; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Sasser_LSA; sid:2000032; rev:9;)

#by Chandan at Secpod.com
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 4000 (msg:"ET EXPLOIT SecurityGateway 1.0.1 Remote Buffer Overflow"; flow:to_server,established; content:"POST "; depth:5; nocase;
content:"/SecurityGateway.dll"; nocase; distance:0; content:"logon"; nocase; distance:0; content:"&username"; nocase; distance:0; pcre:"/\x3d[^\x26]{720}/R"; classtype:misc-attack;
reference:url,frsirt.com/english/advisories/2008/1717; reference:url,milw0rm.com/exploits/5718; reference:url,doc.emergingthreats.net/bin/view/Main/2008426;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_SecurityGateway; reference:cve,2008-4193; sid:2008426; rev:4;)

#Submitted by Cooljay
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET EXPLOIT Possible ShixxNote buffer-overflow + remote shell attempt"; flow: established,to_server; content:"|68 61 63 6b 75|";
offset: 126; depth: 5; content:"|68 61 63 6b 90 61 61 61 61|"; offset: 519; depth: 9; classtype: shellcode-detect; reference:url,aluigi.altervista.org/adv/shixxbof-adv.txt;
reference:url,doc.emergingthreats.net/bin/view/Main/2001385; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_ShixxNote; sid:2001385; rev:6;)

#by Nagaraj S
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 1723 (msg:"ET EXPLOIT Siemens Gigaset SE361 WLAN Data Flood Denial of Service Vulnerability"; flow:to_server; content:"|90 90 90 90 90|";
depth:5; content:"|90 90 90 90 90|"; distance:0; content:"|90 90 90 90 90|"; distance:0; pcre:"/\x90{200,}/"; classtype:denial-of-service; reference:cve,CVE-2009-3322;
reference:bugtraq,36366; reference:url,www.milw0rm.com/exploits/9646; reference:url,doc.emergingthreats.net/2009976; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Siemens; sid:2009976; rev:2;)

#by Summit Siddharth
#
alert tcp $EXTERNAL_NET 31337 -> $HOME_NET 64876 (msg:"ET EXPLOIT malformed Sack - Snort DoS-by-$um$id"; seq:0; ack:0; window:65535; dsize:0; classtype:attempted-dos;
reference:url,doc.emergingthreats.net/bin/view/Main/2002656; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Snort; sid:2002656; rev:4;)

#submitted by bdoctor
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 23 (msg:"ET EXPLOIT Solaris TTYPROMPT environment variable set"; flow: established,to_server; content:"|00 54 54 59 50 52 4F 4D 50 54|";
classtype: attempted-admin; reference:url,online.securityfocus.com/archive/1/293844; reference:url,doc.emergingthreats.net/bin/view/Main/2001780;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Solaris_TTYPROMPT; sid:2001780; rev:6;)

#Submitted 2007-02-12 by Chris Byrd
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 23 (msg:"ET EXPLOIT Solaris telnet USER environment vuln Attack inbound"; flow:to_server,established; content: "|ff fa 27 00 00 55 53 45 52 01
2d 66|"; rawbytes; classtype:attempted-user; reference:url,riosec.com/solaris-telnet-0-day; reference:url,isc.sans.org/diary.html?n&storyid=2220;
reference:url,doc.emergingthreats.net/bin/view/Main/2003411; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Solaris_TelnetUserEnv; reference:cve,2007-
0882; sid:2003411; rev:8;)

#Submitted 2007-02-12 by Chris Byrd
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 23 (msg:"ET EXPLOIT Solaris telnet USER environment vuln Attack outbound"; flow:to_server,established; content: "|ff fa 27 00 00 55 53 45 52 01
2d 66|"; rawbytes; classtype:attempted-user; reference:url,riosec.com/solaris-telnet-0-day; reference:url,isc.sans.org/diary.html?n&storyid=2220;
reference:url,doc.emergingthreats.net/bin/view/Main/2003412; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Solaris_TelnetUserEnv; reference:cve,2007-
0882; sid:2003412; rev:4;)

#by Akash Mahajan of Stillsecure
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Sony ImageStation (SonyISUpload.cab 1.0.0.38) ActiveX Buffer Overflow Exploit"; flow:to_client,established;
content:"0x40000"; nocase; content:"E9A7F56F-C40F-4928-8C6F-7A72F2A25222"; nocase; content:"SetLogging"; nocase; classtype:web-application-attack;
reference:url,www.milw0rm.com/exploits/5086; reference:url,www.milw0rm.com/exploits/5100; reference:url,doc.emergingthreats.net/bin/view/Main/2007847;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Sony_Imagestation; sid:2007847; rev:2;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET EXPLOIT Possible SpamAssassin Milter Plugin Remote Arbitrary Command Injection Attempt"; flow:established,to_server;
content:"to|3A|"; depth:10; nocase; content:"+|3A|\"|7C|"; distance:0; classtype:attempted-user; reference:url,www.securityfocus.com/bid/38578;
reference:url,seclists.org/fulldisclosure/2010/Mar/140; reference:url,doc.emergingthreats.net/2010877; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Spamassassin; sid:2010877; rev:3;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET EXPLOIT Possible Sendmail SpamAssassin Milter Plugin Remote Arbitrary Command Injection Attempt"; flow:established,to_server;
content:"to|3A|"; depth:10; nocase; content:"+\"|7C|"; distance:0; classtype:attempted-user; reference:url,www.securityfocus.com/bid/38578;
reference:url,seclists.org/fulldisclosure/2010/Mar/140; reference:url,doc.emergingthreats.net/2010941; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Spamassassin; sid:2010941; rev:1;)

#
alert tcp $EXTERNAL_NET any -> $HOME_NET 3128 (msg:"ET EXPLOIT Squid NTLM Auth Overflow Exploit"; flow: to_server; content:"|4141 414a 4351 6b4a 4351 6b4a 4351 6b4a|"; offset: 96;
classtype: misc-attack; reference:url,www.idefense.com/application/poi/display?id=107; reference:cve,CAN-2004-0541; reference:url,doc.emergingthreats.net/bin/view/Main/2000342;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Squid_NTLM_Overflow; sid:2000342; rev:6;)

#by Matt Richard
#
#alert tcp any $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT Java runtime.exec() call"; flow:from_server,established; content:"|52 75 6e 74 69 6d 65 3b 01 00 04 65 78 65 63 01 00|";
classtype:trojan-activity; reference:url,www.mullingsecurity.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002783; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Sun_Javascript; sid:2002783; rev:3;)

#Disabled by default. Used in several major sites...
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT Java private function call sun.misc.unsafe"; flow:from_server,established; content:"sun/misc/Unsafe";
classtype:trojan-activity; reference:url,www.mullingsecurity.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002784; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Sun_Javascript; sid:2002784; rev:3;)

#Disabled by default. Used in several major sites...
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT Java field reflector call java.lang.reflect.field"; flow:from_server,established;
content:"java/lang/reflect/Field"; classtype:trojan-activity; reference:url,www.mullingsecurity.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002785;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Sun_Javascript; sid:2002785; rev:3;)

#Disabled by default. Used in several major sites...
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT Javascript unsafe applet call"; flow:from_server,established; content: "sun.misc.Unsafe"; classtype:trojan-
activity; reference:url,www.mullingsecurity.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002786; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Sun_Javascript; sid:2002786; rev:3;)

#Disabled by default. Used in several major sites...
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT Javascript Securitymanager class applet call"; flow:from_server,established; content: "java.lang.SecurityManager";
classtype:trojan-activity; reference:url,www.mullingsecurity.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002787; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Sun_Javascript; sid:2002787; rev:3;)
```

```
#Submitted on 2006-05-01 by Blake Hartstein
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 8004 (msg:"ET EXPLOIT Symantec Scan Engine Request Password Hash"; flow:established,to_server; content:"POST"; nocase; depth:4;
content:"/xml.xml"; nocase; distance:1; within:10; content:"<request"; nocase; distance:0; content:"<key "; distance:0; classtype:attempted-recon; reference:cve,2006-0230;
reference:bugtraq,17637; reference:url,doc.emergingthreats.net/bin/view/Main/2002896; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Symantec;
sid:2002896; rev:5;)

#Matt Jonkman
#limited info, but the exploit requires the data type to be 0x10, the command to be 0x24, then a null, and there is a backslash (0x5c) in the body, and the body is over 0x17c or 0x17a.
More detail in the reference
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 2967:2968 (msg:"ET EXPLOIT Symantec Remote Management RTVScan Exploit"; flow:established,to_server; content:"|10|"; depth:2; content:"|00 24
00|"; distance:0; within:20; content:"|5c|"; distance:0; isdataat:380,relative; classtype:attempted-admin; reference:cve,2006-3455;
reference:url,research.eeye.com/html/advisories/published/AD20060612.html; reference:url,doc.emergingthreats.net/bin/view/Main/2003250; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Symantec; sid:2003250; rev:4;)

#These rules are mostly for malformed tftp related to, but not for any one specific exploit.
#The tftp get or put should be opcode(\x01 or \x02)\x00filename\x00mode\x00. Mode is either netascii, binary or mail.
#by Matt Jonkman
#These look for write or get that does not have the correct mode. Will catch many of the tftp exploits, like the 3com stuff of late.
#
alert udp $EXTERNAL_NET any -> $HOME_NET 69 (msg:"ET EXPLOIT TFTP Invalid Mode in file Get"; content:"|01|"; depth:1; content:"|00|"; distance:1; content:"|00|"; distance:0;
content:!"|00|binary|00|"; nocase; content:!"|00|netascii|00|"; nocase; content:!"|00|mail|00|"; nocase; classtype:non-standard-protocol;
reference:url,doc.emergingthreats.net/bin/view/Main/2003198; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_TFTP_Mode; sid:2003198; rev:4;)

#These rules are mostly for malformed tftp related to, but not for any one specific exploit.
#The tftp get or put should be opcode(\x01 or \x02)\x00filename\x00mode\x00. Mode is either netascii, binary or mail.
#by Matt Jonkman
#These look for write or get that does not have the correct mode. Will catch many of the tftp exploits, like the 3com stuff of late.
#
alert udp $EXTERNAL_NET any -> $HOME_NET 69 (msg:"ET EXPLOIT TFTP Invalid Mode in file Put"; content:"|02|"; depth:1; content:"|00|"; distance:1; content:"|00|"; distance:0;
content:!"|00|binary|00|"; nocase; content:!"|00|netascii|00|"; nocase; content:!"|00|mail|00|"; nocase; classtype:non-standard-protocol;
reference:url,doc.emergingthreats.net/bin/view/Main/2003199; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_TFTP_Mode; sid:2003199; rev:4;)

#By Blake Hartstein
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET EXPLOIT TAC Attack Directory Traversal"; flow:established,to_server; uricontent:"/ISALogin.dll?"; nocase;
pcre:"/Template=.*\.\./UGi"; classtype:attempted-recon; reference:cve,2005-3040; reference:url,secunia.com/advisories/16854; reference:url,cirt.dk/advisories/cirt-37-advisory.pdf;
reference:url,doc.emergingthreats.net/bin/view/Main/2002406; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Tac; sid:2002406; rev:4;)

#Matt Jonkman
#Issue is fixed by patch, and all http traffic is now redirected to https. So anything on this
#port in the clear using the bad cookie name is suspect. Thanks for the reference Jose
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 14942 (msg:"ET EXPLOIT Trend Micro Web Interface Auth Bypass Vulnerable Cookie Attempt"; flow:established,to_server; content:"splx_2376_info";
classtype:attempted-admin; reference:url,labs.idefense.com/intelligence/vulnerabilities/display.php?id=477; reference:url,www.trendmicro.com/download/product.asp?productid=20;
reference:url,doc.emergingthreats.net/bin/view/Main/2003434; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Trend_Micro; sid:2003434; rev:3;)

#by Shirkdog and Scott Melnick
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 5168 (msg:"ET EXPLOIT TrendMicro ServerProtect Exploit possible worma(little-endian DCERPC Request)"; flow:established,to_server; dsize:>1000;
content:"|05|"; depth:1; content:"|10 00 00 00|"; distance:3; within:4; content:"|00 00 88 88 28 25 5b bd d1 11 9d 53 00 80 c8 3a 5c 2c|"; distance:14; within:18; content:"|04 00 03
00|"; distance:0; within:4; content:"|1c 13 74 65|"; distance:500; classtype:misc-attack; reference:url,isc.sans.org/diary.html?storyid=3310;
reference:url,doc.emergingthreats.net/bin/view/Main/2007584; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Trend_Micro; sid:2007584; rev:5;)

#by David Wharton
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 8080 (msg:"ET EXPLOIT VLC web interface buffer overflow attempt"; flow:to_server,established; uricontent:"|2F|requests|2F|status|2E|xml|3F|";
nocase; uricontent:"input|3D|smb|3A 2F 2F|"; nocase; pcre:"/\x2Frequests\x2Fstatus\x2Exml\x3F[^\x0A\x0D]*input\x3D[^\x0A\x0D\x26\x3B]{1000}/iU"; classtype:web-application-attack;
reference:url,milw0rm.org/exploits/9029; reference:url,doc.emergingthreats.net/2009511; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_VLC; sid:2009511;
rev:3;)

#by kevin ross
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET EXPLOIT M3U File Request Flowbit Set"; flow:to_server,established; content:"GET "; depth:4; uricontent:".m3u";
flowbits:set,ET.m3u.download; flowbits:noalert; classtype:not-suspicious; reference:url,doc.emergingthreats.net/2011241; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_VLC; sid:2011241; rev:2;)

#by kevin ross
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT Possible VLC Medial Player M3U File FTP URL Processing Stack Buffer Overflow Attempt";
flowbits:isset,ET.m3u.download; flow:established,to_client; content:"ftp|3A|//"; nocase; content:"PRAV"; within:10; isdataat:2000,relative; content:!"|0A|"; within:2000;
classtype:attempted-user; reference:url,securitytracker.com/alerts/2010/Jul/1024172.html; reference:url,doc.emergingthreats.net/2011242; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_VLC; sid:2011242; rev:2;)

#By Paul Dokas, posted on http://isc.sans.org/diary.php?date=2005-06-27
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 10000 (msg:"ET EXPLOIT Possible BackupExec Metasploit Exploit (inbound)"; flow:established,to_server; content: "|00 00 03 00 00 02 00 58 58
58|"; offset: 24; depth: 20; classtype: attempted-admin; reference:url,isc.sans.org/diary.php?date=2005-06-27;
reference:url,www.metasploit.org/projects/Framework/modules/exploits/backupexec_agent.pm; reference:url,doc.emergingthreats.net/bin/view/Main/2002061;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Veritas_BUExec; sid:2002061; rev:4;)

#By Paul Dokas, posted on http://isc.sans.org/diary.php?date=2005-06-27
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 10000 (msg:"ET EXPLOIT Possible BackupExec Metasploit Exploit (outbound)"; flow:established,to_server; content: "|00 00 03 00 00 02 00 58 58
58|"; offset: 24; depth: 20; classtype: attempted-admin; reference:url,isc.sans.org/diary.php?date=2005-06-27;
reference:url,www.metasploit.org/projects/Framework/modules/exploits/backupexec_agent.pm; reference:url,doc.emergingthreats.net/bin/view/Main/2002062;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Veritas_BUExec; sid:2002062; rev:4;)

#By Chris Ries of Vigilant Minds. This is not specific to the exploit as previous versions
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 10000 (msg:"ET EXPLOIT Veritas backupexec_agent exploit"; flow:to_server,established; content:"|00 00 00 00 00 00 09 01|"; offset:12; depth:20;
content: "|00 00 00 03|"; offset: 28; depth: 32; byte_jump: 4, 32; byte_test: 4,>,3000,0,relative; classtype:misc-attack; reference:url,isc.sans.org/diary.php?date=2005-06-27;
reference:url,doc.emergingthreats.net/bin/view/Main/2002065; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Veritas_BUExec; sid:2002065; rev:7;)

#By Mark Tombaugh: Alerts on responses of version checks.
#
alert tcp $HOME_NET 10000 -> $EXTERNAL_NET any (msg:"ET EXPLOIT NDMP Notify Connect - Possible Backup Exec Remote Agent Recon"; flow:established,from_server; content:"|00 00 05 02|";
offset:16; depth:20; content: "|00 00 00 03|"; offset: 28; depth: 32; classtype:attempted-recon; reference:url,www.ndmp.org/download/sdk_v4/draft-skardal-ndmp4-04.txt;
reference:url,doc.emergingthreats.net/bin/view/Main/2002068; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Veritas_BUExec; sid:2002068; rev:8;)

#Added 2005/08/12 by Frank Knobbe - This version alerts if a system is vulnerable. flowbits:noalert is optional on the first rule if you don't want to detect (possibly unsuccessfull)
attempts.
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 10000 (msg:"ET EXPLOIT Backup Exec Windows Agent Remote File Access - Attempt"; flow:to_server,established; flowbits:isnotset,SID2002181;
content:"|0000 0000 0000 0901 0000 0000 0000 0000 0000 0000 0002 0000 0004 726f 6f74 b4b8 0f26 205c 4234 03fc aeee 8f91 3d6f|"; offset:8; depth:52; flowbits:set,SID2002181;
classtype:default-login-attempt; reference:url,www.frsirt.com/english/advisories/2005/1387; reference:url,www.frsirt.com/exploits/20050811.backupexec_dump.pm.php;
reference:url,doc.emergingthreats.net/bin/view/Main/2002181; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Veritas_BUExec; sid:2002181; rev:5;)

#Added 2005/08/12 by Frank Knobbe - This version alerts if a system is vulnerable. flowbits:noalert is optional on the first rule if you don't want to detect (possibly unsuccessfull)
attempts.
#
alert tcp $HOME_NET 10000 -> $EXTERNAL_NET any (msg:"ET EXPLOIT Backup Exec Windows Agent Remote File Access - Vulnerable"; flow:from_server,established; flowbits:isset,SID2002181;
content:"|0000 0001 0000 0901|"; offset:8; depth:16; content:"|0000 0000 0000 0000|"; distance:4; within:12; classtype:misc-attack;
reference:url,www.frsirt.com/english/advisories/2005/1387; reference:url,www.frsirt.com/exploits/20050811.backupexec_dump.pm.php;
reference:url,doc.emergingthreats.net/bin/view/Main/2002182; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Veritas_BUExec; sid:2002182; rev:5;)
```

```
#by mmlange
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET EXPLOIT WMF Exploit"; flow:established; content:"|01 00 09 00 00 03 52 1f 00 00 06 00 3d 00 00 00|"; content:"|00 26 06 0f 00 08
00 ff ff ff ff 01 00 00 00 03 00 00 00 00 00|"; classtype:attempted-user; reference:url,www.frsirt.com/exploits/20051228.ie_xp_pfv_metafile.pm.php;
reference:url,doc.emergingthreats.net/bin/view/Main/2002734; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_WMF; sid:2002734; rev:5;)

#By Frank Knobbe, 2005-12-28. Additional work with Blake Harstein and Brandon Franklin.
#flow_depth (of http_inspect_server) has to be set to 0. Recommend second Snort instance with that config.
#Note that these rules will fail to detect the exploit when the HTTP response is gzipped.
#There is also a possibility for evasion, but a version that catches it will incurr massive amount of FPs.
#Web Only
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT WMF Escape Record Exploit - Web Only - all versions"; flow:established,from_server;
flowbits:isnotset,emerging_wmf_http; content:"HTTP"; depth:4; nocase; flowbits:set,emerging_wmf_http; flowbits:noalert; classtype:unknown;
reference:url,www.frsirt.com/english/advisories/2005/3086; reference:url,doc.emergingthreats.net/bin/view/Main/2002743; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_WMF; sid:2002743; rev:5;)

#By Frank Knobbe, 2005-12-28. Additional work with Blake Harstein and Brandon Franklin.
#flow_depth (of http_inspect_server) has to be set to 0. Recommend second Snort instance with that config.
#Note that these rules will fail to detect the exploit when the HTTP response is gzipped.
#There is also a possibility for evasion, but a version that catches it will incurr massive amount of FPs.
#Web Only
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT WMF Escape Record Exploit - Web Only - version 3"; flow:established; flowbits:isset,emerging_wmf_http;
flowbits:isnotset,emerging_wmf_expl; flowbits:isnotset,emerging_wmf_expl_v1; content:"|00 09 00 00 03|"; content:"|00 00|"; distance:10; within:12; flowbits:set,emerging_wmf_expl;
flowbits:noalert; classtype:unknown; reference:url,www.frsirt.com/english/advisories/2005/3086; reference:url,doc.emergingthreats.net/bin/view/Main/2002741;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_WMF; sid:2002741; rev:10;)

#By Frank Knobbe, 2005-12-28. Additional work with Blake Harstein and Brandon Franklin.
#flow_depth (of http_inspect_server) has to be set to 0. Recommend second Snort instance with that config.
#Note that these rules will fail to detect the exploit when the HTTP response is gzipped.
#There is also a possibility for evasion, but a version that catches it will incurr massive amount of FPs.
#Web Only
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT WMF Escape Record Exploit - Web Only - version 1"; flow:established; flowbits:isset,emerging_wmf_http;
flowbits:isnotset,emerging_wmf_expl; flowbits:isnotset,emerging_wmf_expl_v1; content:"|00 09 00 00 01|"; content:"|00 00|"; distance:10; within:12; flowbits:set,emerging_wmf_expl_v1;
flowbits:noalert; classtype:unknown; reference:url,www.frsirt.com/english/advisories/2005/3086; reference:url,doc.emergingthreats.net/bin/view/Main/2002757;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_WMF; sid:2002757; rev:4;)

## These rules have to be there for both
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET EXPLOIT WMF Escape Record Exploit - Version 1"; flow:established; flowbits:isset,emerging_wmf_expl_v1; pcre:"/\x26[\x00-
\xff]\x09\x00/"; flowbits:unset,emerging_wmf_http; flowbits:unset,emerging_wmf_expl; flowbits:unset,emerging_wmf_expl_v1; classtype:attempted-user; threshold:type limit, track by_src,
count 1,seconds 120; reference:url,www.frsirt.com/english/advisories/2005/3086; reference:url,doc.emergingthreats.net/bin/view/Main/2002758; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_WMF; sid:2002758; rev:6;)

## These rules have to be there for both
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET EXPLOIT WMF Escape Record Exploit - Version 3"; flow:established; flowbits:isset,emerging_wmf_expl; pcre:"/\x26[\x00-
\xff]\x09\x00/"; flowbits:unset,emerging_wmf_http; flowbits:unset,emerging_wmf_expl; flowbits:unset,emerging_wmf_expl_v1; classtype:attempted-user; threshold:type limit, track by_src,
count 1,seconds 120; reference:url,www.frsirt.com/english/advisories/2005/3086; reference:url,doc.emergingthreats.net/bin/view/Main/2002742; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_WMF; sid:2002742; rev:9;)

#by kevin ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 9100 (msg:"ET EXPLOIT Xerox WorkCentre PJL Daemon Buffer Overflow Attempt"; flow:established,to_server; content:"ENTER LANGUAGE ="; depth:50;
nocase; isdataat:55,relative; content:!"|0A|"; within:55; pcre:"/ENTER\x20LANGUAGE\x20\x3D.{55}/smi"; classtype:attempted-admin; reference:url,www.securityfocus.com/bid/38010;
reference:url,doc.emergingthreats.net/2010759; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Xerox; sid:2010759; rev:2;)

#by Akash Mahajan of Stillsecure
#disabled but adding the default port for the server otherwise sig is way to generic
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 7700 (msg:"ET EXPLOIT Zilab Chat and Instant Messaging Heap Overflow Vulnerability"; flow:established; content:"|21 00 21 03|"; pcre:"/[0-9a-zA-
Z]{10,}/R"; classtype:misc-attack; reference:url,aluigi.altervista.org/adv/zilabzcsx-adv.txt; reference:bugtraq,27940; reference:url,doc.emergingthreats.net/bin/view/Main/2007933;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Zilab; sid:2007933; rev:9;)

#by Akash Mahajan of Stillsecure
#adding server default port otherwise sig is way to generic
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 7700 (msg:"ET EXPLOIT Zilab Chat and Instant Messaging User Info BoF Vulnerability"; flow:established; content:"|61 00 09 00 08 00 07 00 21
03|"; pcre:"/[0-9a-zA-Z]{10,}/R"; classtype:misc-attack; reference:url,aluigi.altervista.org/adv/zilabzcsx-adv.txt; reference:bugtraq,27940;
reference:url,doc.emergingthreats.net/bin/view/Main/2007934; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_Zilab; sid:2007934; rev:6;)

#by evilghost
#
alert udp any any -> $HOME_NET 27901 (msg:"ET GAMES Alien Arena 7.30 Remote Code Execution Attempt"; content:"print|0A 5C|"; isdataat:257,relative; pcre:"/\x5C[^\x5C\x00]{257,}/";
classtype:misc-attack; reference:url,www.packetstormsecurity.org/0910-advisories/alienarena-exec.txt; reference:url,doc.emergingthreats.net/2010156;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_AlienArena; sid:2010156; rev:5;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 6112 (msg:"ET GAMES Battle.net Starcraft login"; flow:established,to_server; content:"|FF 50|"; depth:2; content:"RATS"; offset:12; depth:12;
classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002101; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet;
sid:2002101; rev:6;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 6112 (msg:"ET GAMES Battle.net Brood War login"; flow:established,to_server; content:"|FF 50|"; depth:2; content:"PXES"; offset:12; depth:12;
classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002102; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet;
sid:2002102; rev:6;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 6112 (msg:"ET GAMES Battle.net Diablo login"; flow:established,to_server; content:"|FF 50|"; depth:2; content:"LTRD"; offset:12; depth:12;
classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002103; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet;
sid:2002103; rev:6;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 6112 (msg:"ET GAMES Battle.net Diablo 2 login"; flow:established,to_server; content:"|FF 50|"; depth:2; content:"VD2D"; offset:12; depth:12;
classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002104; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet;
sid:2002104; rev:6;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 6112 (msg:"ET GAMES Battle.net Diablo 2 Lord of Destruction login"; flow:established,to_server; content:"|FF 50|"; depth:2; content:"PX2D";
offset:12; depth:12; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002105; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet; sid:2002105; rev:6;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 6112 (msg:"ET GAMES Battle.net Warcraft 2 login"; flow:established,to_server; content:"|FF 50|"; depth:2; content:"NB2W"; offset:12; depth:12;
classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002106; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet;
sid:2002106; rev:6;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 6112 (msg:"ET GAMES Battle.net Warcraft 3 login"; flow:established,to_server; content:"|FF 50|"; depth:2; content:"3RAW"; offset:12; depth:12;
classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002107; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet;
```

```
sid:2002107; rev:6;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 6112 (msg:"ET GAMES Battle.net Warcraft 3 The Frozen throne login"; flow:established,to_server; content:"|FF 50|"; depth:2; content:"PX3W";
offset:12; depth:12; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002108; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet; sid:2002108; rev:7;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net old game version"; flow:established,from_server; content:"|FF 51|"; depth:2; content:"|00 01 00 00|"; offset:4;
depth:4; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002109; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet;
sid:2002109; rev:6;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net invalid version"; flow:established,from_server; content:"|FF 51 08 00 01 01 00 00|"; classtype: policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2002110; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet; sid:2002110; rev:5;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net invalid cdkey"; flow:established,from_server; content:"|FF 51 09 00 00 02 00 00|"; classtype: policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2002111; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet; sid:2002111; rev:5;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net cdkey in use"; flow:established,from_server; content:"|FF 51|"; depth:2; content:"|01 02 00 00|"; offset:4;
depth:4; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002112; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet;
sid:2002112; rev:6;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net banned key"; flow:established,from_server; content:"|FF 51 09 00 02 02 00 00|"; classtype: policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2002113; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet; sid:2002113; rev:5;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net wrong product"; flow:established,from_server; content:"|FF 51 09 00 03 02 00 00|"; classtype: policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2002114; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet; sid:2002114; rev:5;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net failed account login (OLS) wrong password"; flow:established,from_server; content:"|FF 3A 08 00 02 00 00 00|";
classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002115; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet;
sid:2002115; rev:6;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net failed account login (NLS) wrong password"; flow:established,from_server; content:"|FF 54 1C 00 02 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 00 00 00|"; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002116;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet; sid:2002116; rev:6;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net connection reset (possible IP-Ban)"; flags:R,12; classtype: policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2002117; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet; sid:2002117; rev:6;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net user in channel"; flow:established,from_server; content:"|FF 0F|"; depth:2; content:"|01 00 00 00|"; offset:4;
depth:4; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002118; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet;
sid:2002118; rev:6;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net user joined channel"; flow:established,from_server; content:"|FF 0F|"; depth:2; content:"|02 00 00 00|";
offset:4; depth:4; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002140; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet; sid:2002140; rev:5;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net user left channel"; flow:established,from_server; content:"|FF 0F|"; depth:2; content:"|03 00 00 00|"; offset:4;
depth:4; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002141; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet;
sid:2002141; rev:5;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net received whisper message"; flow:established,from_server; content:"|FF 0F|"; depth:2; content:"|04 00 00 00|";
offset:4; depth:4; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002142; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet; sid:2002142; rev:5;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net received server broadcast"; flow:established,from_server; content:"|FF 0F|"; depth:2; content:"|06 00 00 00|";
offset:4; depth:4; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002143; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet; sid:2002143; rev:5;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net joined channel"; flow:established,from_server; content:"|FF 0F|"; depth:2; content:"|07 00 00 00|"; offset:4;
depth:4; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002144; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet;
sid:2002144; rev:5;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net user had a flags update"; flow:established,from_server; content:"|FF 0F|"; depth:2; content:"|09 00 00 00|";
offset:4; depth:4; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002145; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet; sid:2002145; rev:5;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net sent a whisper"; flow:established,from_server; content:"|FF 0F|"; depth:2; content:"|0a 00 00 00|"; offset:4;
depth:4; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002146; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet;
sid:2002146; rev:5;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net channel full"; flow:established,from_server; content:"|FF 0F|"; depth:2; content:"|0d 00 00 00|"; offset:4;
depth:4; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002147; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet;
sid:2002147; rev:5;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net channel doesn't exist"; flow:established,from_server; content:"|FF 0F|"; depth:2; content:"|0e 00 00 00|";
offset:4; depth:4; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002148; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet; sid:2002148; rev:5;)

#All by Ron Bowes. Many thanks Ron
```

```
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net channel is restricted"; flow:established,from_server; content:"|FF 0F|"; depth:2; content:"|0f 00 00 00|";
offset:4; depth:4; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002149; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet; sid:2002149; rev:5;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net informational message"; flow:established,from_server; content:"|FF 0F|"; depth:2; content:"|12 00 00 00|";
offset:4; depth:4; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002150; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet; sid:2002150; rev:5;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net error message"; flow:established,from_server; content:"|FF 0F|"; depth:2; content:"|13 00 00 00|"; offset:4;
depth:4; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002151; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet;
sid:2002151; rev:5;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net 'emote' message"; flow:established,from_server; content:"|FF 0F|"; depth:2; content:"|17 00 00 00|"; offset:4;
depth:4; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002152; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet;
sid:2002152; rev:5;)

#All by Ron Bowes. Many thanks Ron
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 6112 (msg:"ET GAMES Battle.net outgoing chat message"; flow:established,to_server; content:"|FF 0E|"; depth:2; classtype: policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2002119; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet; sid:2002119; rev:6;)

#World of Warcraft rules, though written by Ron, are thanks to information from Justin (UserLoser)
#updated from info from Adam Ellison. New packets start with 00 06, not just 00 02.
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 3724 (msg:"ET GAMES World of Warcraft connection"; flow:established,to_server; content:"|00|"; depth:1; content:"|25 00|WoW|00|"; distance:1;
within:7; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002138; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet;
sid:2002138; rev:9;)

#World of Warcraft rules, though written by Ron, are thanks to information from Justin (UserLoser)
#updated from info from Adam Ellison. New packets start with 00 06, not just 00 02.
#
alert tcp $EXTERNAL_NET 3724 -> $HOME_NET any (msg:"ET GAMES World of Warcraft failed logon"; flow:established,from_server; content:"|01 0A|"; depth:2; classtype: policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2002139; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet; sid:2002139; rev:5;)

#Guild wars rues, again written by Ron, are thanks to information from Ian (Romi)
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 6112 (msg:"ET GAMES Guild Wars connection"; flow:established,to_server; content:"|01 00 00 00 00 F1 00 10 00 01 00 00 00 00 00 00 00 00 00 00
00|"; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002154; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet;
sid:2002154; rev:5;)

#Guild wars rues, again written by Ron, are thanks to information from Ian (Romi)
#
alert tcp $EXTERNAL_NET 6112 -> $HOME_NET any (msg:"ET GAMES Battle.net incoming chat message"; flow:established,from_server; content:"|FF 0F|"; depth:2; content:"|05 00 00 00|";
offset:4; depth:4; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002170; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/GAMES/GAMES_Battlenet; sid:2002170; rev:5;)

#by Jason Wallace. Detects blizzard game updates, p2p traffic may follow for downloads from blizzard
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET GAMES Blizzard Downloader"; flow: established,to_server; content: "User-Agent|3a| Blizzard Downloader"; nocase; classtype:policy-
violation; reference:url,www.worldofwarcraft.com/info/faq/blizzarddownloader.html; reference:url,doc.emergingthreats.net/bin/view/Main/2002855;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Blizzard; sid:2002855; rev:7;)

#by Blake Hartstein of Demarc
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET GAMES PunkBuster Server webkey Buffer Overflow"; flow:established,to_server; uricontent:"/pbsvweb"; nocase;
content:"webkey="; nocase; isdataat:500,relative; pcre:"/^[^&\n]{500}/R"; classtype:attempted-admin; reference:url,aluigi.altervista.org/adv/pbwebbof-adv.txt;
reference:url,doc.emergingthreats.net/2002947; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB/WEB_Punkbuster; sid:2002947; rev:4;)

#By Ron Iago
#
alert udp $HOME_NET any -> $EXTERNAL_NET 27015 (msg:"ET GAMES Steam connection"; content:"getchallengesteam"; classtype:policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2002155; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Steam; sid:2002155; rev:4;)

#by Sean Calista
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 27020:27050 (msg:"ET GAMES STEAM Connection (v2)"; flow:established,to_server; content:"|00 00 00 03|"; dsize:4; classtype:policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2003089; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Steam; sid:2003089; rev:4;)

#by Philipp Seidel
#
alert udp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET GAMES TeamSpeak3 Connect"; content:"|00 00 00 00 02 9d 74 8b 45 aa 7b ef b9 9e fe ad 08 19 ba cf 41 e0 16 a2|"; offset:8;
depth:24; classtype:policy-violation; reference:url,teamspeak.com; reference:url,doc.emergingthreats.net/2011733; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/GAMES/GAMES_TeamSpeak; sid:2011733; rev:3;)

#by Philipp Seidel
#
alert udp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET GAMES TeamSpeak2 Connection/Login"; content:"|f4 be 03 00|"; depth:4; classtype:policy-violation; reference:url,teamspeak.com;
reference:url,doc.emergingthreats.net/2011734; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_TeamSpeak; sid:2011734; rev:3;)

#by Philipp Seidel
#
alert udp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET GAMES TeamSpeak2 Connection/Login Replay"; content:"|f4 be 04 00|"; depth:4; classtype:policy-violation;
reference:url,teamspeak.com; reference:url,doc.emergingthreats.net/2011735; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_TeamSpeak; sid:2011735; rev:3;)

#be careful with the following two rules, they produce at least 1 alert per second on an active TeamSpeak 2 connection
#
alert udp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET GAMES TeamSpeak2 Connection/Ping"; content:"|f4 be 01 00|"; depth:4; threshold:type limit, count 1, seconds 300, track by_src;
classtype:policy-violation; reference:url,teamspeak.com; reference:url,doc.emergingthreats.net/2011736; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/GAMES/GAMES_TeamSpeak; sid:2011736; rev:3;)

#be careful with the following two rules, they produce at least 1 alert per second on an active TeamSpeak 2 connection
#
alert udp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET GAMES TeamSpeak2 Connection/Ping Reply"; content:"|f4 be 02 00|"; depth:4; threshold:type limit, count 1, seconds 300, track
by_src; classtype:policy-violation; reference:url,teamspeak.com; reference:url,doc.emergingthreats.net/2011737; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/GAMES/GAMES_TeamSpeak; sid:2011737; rev:3;)

#be careful with the following two rules, they produce at least 1 alert per second on an active TeamSpeak 2 connection
#
alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET GAMES TeamSpeak2 Standard/Login Part 2"; content:"|f0 be 05 00|"; depth:4; classtype:policy-violation;
reference:url,teamspeak.com; reference:url,doc.emergingthreats.net/2011738; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_TeamSpeak; sid:2011738; rev:3;)

#be careful with the following two rules, they produce at least 1 alert per second on an active TeamSpeak 2 connection
#
alert udp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET GAMES TeamSpeak2 Standard/Channel List"; content:"|f0 be 06 00|"; depth:4; classtype:policy-violation;
reference:url,teamspeak.com; reference:url,doc.emergingthreats.net/2011739; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_TeamSpeak; sid:2011739; rev:3;)

#be careful with the following two rules, they produce at least 1 alert per second on an active TeamSpeak 2 connection
#
alert udp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET GAMES TeamSpeak2 Standard/Player List"; content:"|f0 be 07 00|"; depth:4; classtype:policy-violation;
reference:url,teamspeak.com; reference:url,doc.emergingthreats.net/2011740; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_TeamSpeak; sid:2011740; rev:3;)
```

```
#be careful with the following two rules, they produce at least 1 alert per second on an active TeamSpeak 2 connection
#
alert udp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET GAMES TeamSpeak2 Standard/Login End"; content:"|f0 be 08 00|"; depth:4; classtype:policy-violation;
reference:url,teamspeak.com; reference:url,doc.emergingthreats.net/2011741; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_TeamSpeak; sid:2011741; rev:3;)

#be careful with the following two rules, they produce at least 1 alert per second on an active TeamSpeak 2 connection
#
alert udp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET GAMES TeamSpeak2 Standard/New Player Joined"; content:"|f0 be 64 00|"; depth:4; classtype:policy-violation;
reference:url,teamspeak.com; reference:url,doc.emergingthreats.net/2011742; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_TeamSpeak; sid:2011742; rev:3;)

#be careful with the following two rules, they produce at least 1 alert per second on an active TeamSpeak 2 connection
#
alert udp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET GAMES TeamSpeak2 Standard/Player Left"; content:"|f0 be 65 00|"; depth:4; classtype:policy-violation;
reference:url,teamspeak.com; reference:url,doc.emergingthreats.net/2011743; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_TeamSpeak; sid:2011743; rev:3;)

#be careful with the following two rules, they produce at least 1 alert per second on an active TeamSpeak 2 connection
#
alert udp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET GAMES TeamSpeak2 Standard/Change Status"; content:"|f0 be 30 01|"; depth:4; classtype:policy-violation;
reference:url,teamspeak.com; reference:url,doc.emergingthreats.net/2011744; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_TeamSpeak; sid:2011744; rev:3;)

#be careful with the following two rules, they produce at least 1 alert per second on an active TeamSpeak 2 connection
#
alert udp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET GAMES TeamSpeak2 Standard/Known Player Update"; content:"|f0 be 68 00|"; depth:4; classtype:policy-violation;
reference:url,teamspeak.com; reference:url,doc.emergingthreats.net/2011745; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_TeamSpeak; sid:2011745; rev:3;)

#be careful with the following two rules, they produce at least 1 alert per second on an active TeamSpeak 2 connection
#
alert udp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET GAMES TeamSpeak2 Standard/Disconnect"; content:"|f0 be 2c 01|"; depth:4; classtype:policy-violation;
reference:url,teamspeak.com; reference:url,doc.emergingthreats.net/2011746; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_TeamSpeak; sid:2011746; rev:3;)

#be careful with the following two rules, they produce at least 1 alert per second on an active TeamSpeak 2 connection
#
alert udp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET GAMES TeamSpeak2 ACK"; content:"|f1 be|"; depth:2; dsize:16; classtype:policy-violation; reference:url,teamspeak.com;
reference:url,doc.emergingthreats.net/2011747; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_TeamSpeak; sid:2011747; rev:3;)

#by philipp seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET GAMES TrackMania Game Launch"; flow:to_server,established; content:"GET"; offset:0; depth:3;
uricontent:"/online_game/launcher_init.php?"; content:"|0d 0a|User-Agent|3a| GameBox"; uricontent:"game="; uricontent:"lang="; uricontent:"protocol="; uricontent:"distro=";
uricontent:"osdesc="; classtype:policy-violation; reference:url,www.trackmania.com; reference:url,doc.emergingthreats.net/2011748; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/GAMES/GAMES_Trackmania; sid:2011748; rev:3;)

#by philipp seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET GAMES TrackMania Game Check for Patch"; flow:to_server,established; content:"GET"; offset:0; depth:3;
uricontent:"/online_game/patch.php?"; uricontent:"game="; uricontent:"lang="; uricontent:"protocol="; uricontent:"distro="; uricontent:"osdesc="; classtype:policy-violation;
reference:url,www.trackmania.com; reference:url,doc.emergingthreats.net/2011749; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Trackmania; sid:2011749;
rev:2;)

#by philipp seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET GAMES TrackMania Request GetConnectionAndGameParams"; flow:to_server,established; content:"POST"; offset:0; depth:4;
uricontent:"/online_game/request.php"; content:"|0d 0a|User-Agent|3a| GameBox"; content:"<request><name>GetConnectionAndGameParams</name>"; nocase; classtype:policy-violation;
reference:url,www.trackmania.com; reference:url,doc.emergingthreats.net/2011750; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Trackmania; sid:2011750;
rev:3;)

#by philipp seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET GAMES TrackMania Request OpenSession"; flow:to_server,established; content:"POST"; offset:0; depth:4;
uricontent:"/online_game/request.php"; content:"|0d 0a|User-Agent|3a| GameBox"; content:"<request><name>OpenSession</name>"; nocase; classtype:policy-violation;
reference:url,www.trackmania.com; reference:url,doc.emergingthreats.net/2011751; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Trackmania; sid:2011751;
rev:3;)

#by philipp seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET GAMES TrackMania Request Connect"; flow:to_server,established; content:"POST "; nocase; depth:5;
uricontent:"/online_game/request.php"; content:"User-Agent|3a| GameBox"; content:"<request><name>Connect</name>"; nocase; classtype:policy-violation; reference:url,www.trackmania.com;
reference:url,doc.emergingthreats.net/2011752; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Trackmania; sid:2011752; rev:5;)

#by philipp seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET GAMES TrackMania Request Disconnect"; flow:to_server,established; content:"POST"; offset:0; depth:4;
uricontent:"/online_game/request.php"; content:"|0d 0a|User-Agent|3a| GameBox"; content:"<request><name>Disconnect</name>"; nocase; classtype:policy-violation;
reference:url,www.trackmania.com; reference:url,doc.emergingthreats.net/2011753; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Trackmania; sid:2011753;
rev:3;)

#by philipp seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET GAMES TrackMania Request GetOnlineProfile"; flow:to_server,established; content:"POST"; offset:0; depth:4;
uricontent:"/online_game/request.php"; content:"|0d 0a|User-Agent|3a| GameBox"; content:"<request><name>GetOnlineProfile</name>"; nocase; classtype:policy-violation;
reference:url,www.trackmania.com; reference:url,doc.emergingthreats.net/2011754; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Trackmania; sid:2011754;
rev:3;)

#by philipp seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET GAMES TrackMania Request GetBuddies"; flow:to_server,established; content:"POST"; offset:0; depth:4;
uricontent:"/online_game/request.php"; content:"|0d 0a|User-Agent|3a| GameBox"; content:"<request><name>GetBuddies</name>"; nocase; classtype:policy-violation;
reference:url,www.trackmania.com; reference:url,doc.emergingthreats.net/2011755; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Trackmania; sid:2011755;
rev:3;)

#by philipp seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET GAMES TrackMania Request SearchNew"; flow:to_server,established; content:"POST"; offset:0; depth:4;
uricontent:"/online_game/request.php"; content:"|0d 0a|User-Agent|3a| GameBox"; content:"<request><name>SearchNew</name>"; nocase; classtype:policy-violation;
reference:url,www.trackmania.com; reference:url,doc.emergingthreats.net/2011756; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Trackmania; sid:2011756;
rev:3;)

#by philipp seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET GAMES TrackMania Request LiveUpdate"; flow:to_server,established; content:"POST"; offset:0; depth:4;
uricontent:"/online_game/request.php"; content:"|0d 0a|User-Agent|3a| GameBox"; content:"<request><name>LiveUpdate</name>"; nocase; classtype:policy-violation;
reference:url,www.trackmania.com; reference:url,doc.emergingthreats.net/2011757; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/GAMES/GAMES_Trackmania; sid:2011757;
rev:3;)

#by philipp seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET GAMES TrackMania Ad Report"; flow:to_server,established; content:"GET"; offset:0; depth:3;
uricontent:"/online_game/ad_report.php"; content:"|0d 0a|User-Agent|3a| GameBox"; uricontent:"protocol="; uricontent:"author="; uricontent:"login="; uricontent:"zone=";
classtype:policy-violation; reference:url,www.trackmania.com; reference:url,doc.emergingthreats.net/2011758; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/GAMES/GAMES_Trackmania; sid:2011758; rev:3;)

#Google Image Search, Safe Mode Off
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET INAPPROPRIATE Google Image Search, Safe Mode Off"; flow:established,to_server; uricontent:"&safe=off"; content:"|0d
0a|Host|3a| images.google.com|0d 0a|"; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002925; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/INAPPROPRIATE/INAPPROPRIATE_Google; sid:2002925; rev:4;)

#Info for these sigs from Gary Kalbfleisch
#
```

```
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET INAPPROPRIATE Kiddy Porn preteen"; flow: from_server,established; content:"preteen"; nocase; threshold: type threshold,
track by_dst,count 5, seconds 360; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2001346; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/INAPPROPRIATE/INAPPROPRIATE_Kiddy_Porn; sid:2001346; rev:8;)

#Info for these sigs from Gary Kalbfleisch
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET INAPPROPRIATE Kiddy Porn pre-teen"; flow: from_server,established; content:"pre-teen"; nocase; threshold: type threshold,
track by_dst,count 5, seconds 360; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2001347; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/INAPPROPRIATE/INAPPROPRIATE_Kiddy_Porn; sid:2001347; rev:8;)

#Info for these sigs from Gary Kalbfleisch
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET INAPPROPRIATE Kiddy Porn early teen"; flow: from_server,established; content:"early teen"; nocase; threshold: type
threshold, track by_dst,count 5, seconds 360; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2001348; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/INAPPROPRIATE/INAPPROPRIATE_Kiddy_Porn; sid:2001348; rev:8;)

#From Patrick Harper
#Commenting out by default. Enable these if needed
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET INAPPROPRIATE Kiddy Porn pthc"; flow: from_server,established; content:" pthc "; nocase; classtype: policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2001386; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/INAPPROPRIATE/INAPPROPRIATE_Kiddy_Porn; sid:2001386; rev:6;)

#From Patrick Harper
#Commenting out by default. Enable these if needed
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET INAPPROPRIATE Kiddy Porn zeps"; flow: from_server,established; content:" zeps "; nocase; classtype: policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2001387; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/INAPPROPRIATE/INAPPROPRIATE_Kiddy_Porn; sid:2001387; rev:6;)

#From Patrick Harper
#Commenting out by default. Enable these if needed
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET INAPPROPRIATE Kiddy Porn r@ygold"; flow: from_server,established; content:" r@ygold "; nocase; classtype: policy-
violation; reference:url,doc.emergingthreats.net/bin/view/Main/2001388; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/INAPPROPRIATE/INAPPROPRIATE_Kiddy_Porn;
sid:2001388; rev:6;)

#From Patrick Harper
#Commenting out by default. Enable these if needed
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET INAPPROPRIATE Kiddy Porn childlover"; flow: from_server,established; content:" childlover "; nocase; classtype: policy-
violation; reference:url,doc.emergingthreats.net/bin/view/Main/2001389; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/INAPPROPRIATE/INAPPROPRIATE_Kiddy_Porn;
sid:2001389; rev:6;)

#From Patrick Harper
#Commenting out by default. Enable these if needed
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET INAPPROPRIATE free XXX"; flow: to_client,established; content:"FREE XXX"; nocase; threshold: type threshold, track
by_dst,count 5, seconds 360; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2001349; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/INAPPROPRIATE/INAPPROPRIATE_Porn; sid:2001349; rev:8;)

#From Patrick Harper
#Commenting out by default. Enable these if needed
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET INAPPROPRIATE hardcore anal"; flow: to_client,established; content:"hardcore anal"; nocase; threshold: type threshold,
track by_dst,count 5, seconds 360; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2001350; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/INAPPROPRIATE/INAPPROPRIATE_Porn; sid:2001350; rev:8;)

#From Patrick Harper
#Commenting out by default. Enable these if needed
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET INAPPROPRIATE masturbation"; flow: to_client,established; content:"masturbat"; nocase; threshold: type threshold, track
by_dst,count 5, seconds 360; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2001351; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/INAPPROPRIATE/INAPPROPRIATE_Porn; sid:2001351; rev:8;)

#From Patrick Harper
#Commenting out by default. Enable these if needed
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET INAPPROPRIATE ejaculation"; flow: to_client,established; content:"ejaculat"; nocase; threshold: type threshold, track
by_dst,count 5, seconds 360; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2001352; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/INAPPROPRIATE/INAPPROPRIATE_Porn; sid:2001352; rev:8;)

#From Patrick Harper
#Commenting out by default. Enable these if needed
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET INAPPROPRIATE BDSM"; flow: to_client,established; content:"BDSM"; nocase; threshold: type threshold, track by_dst,count 5,
seconds 360; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2001353; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/INAPPROPRIATE/INAPPROPRIATE_Porn; sid:2001353; rev:8;)

#Experiment by Matt Jonkman
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET INAPPROPRIATE Sextracker Tracking Code Detected (1)"; flow: from_server,established; content:"BEGIN SEXLIST REFERRER-STATS
CODE"; nocase; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2001392; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/INAPPROPRIATE/INAPPROPRIATE_Porn; sid:2001392; rev:10;)

#Experiment by Matt Jonkman
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET INAPPROPRIATE Sextracker Tracking Code Detected (2)"; flow: from_server,established; content:"BEGIN SEXTRACKER CODE";
nocase; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2001393; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/INAPPROPRIATE/INAPPROPRIATE_Porn; sid:2001393; rev:10;)

#By Jeffrey Lowe
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET INAPPROPRIATE Likely Porn"; flow: established,from_server; pcre:"/ (FREE XXX|dildo|masturbat|oral sex|ejaculat|up
skirt|tits|bondage|lolita|clitoris|cock suck|hardcore (teen|anal|sex|porn)|raw sex|((fuck|sex|porn|xxx) (movies|dvd))|((naked|nude) (celeb|lesbian)))\b/i"; classtype:policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2001608; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/INAPPROPRIATE/INAPPROPRIATE_Porn; sid:2001608; rev:8;)

#Submitted by Jason Haar
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET DELETED 180solutions Update Engine"; flow: to_server,established; content:"GET "; depth:4; content:"Host|3a|"; within:
300; content:".180solutions.com"; within: 40; classtype: trojan-activity; reference:url,www.safer-networking.org/index.php?page=threats&detail=212;
reference:url,doc.emergingthreats.net/bin/view/Main/2000930; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_180Solutions; sid:2000930; rev:10;)

#Submitted by Jason Haar
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET DELETED 180solutions Spyware (tracked event reported)"; flow: to_server,established; uricontent:"/TrackedEvent.aspx?";
nocase; uricontent:"eid="; nocase; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/pf/adware.180search.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001397; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_180Solutions; sid:2001397; rev:9;)

#Submitted by Jason Haar
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET DELETED 180solutions Spyware (action url reported)"; flow: to_server,established; uricontent:"/actionurls/ActionUrl";
nocase; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/pf/adware.180search.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001399;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_180Solutions; sid:2001399; rev:9;)

#Submitted by Jason Haar
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE 180solutions Spyware Reporting"; flow: to_server,established; uricontent:"/showme.aspx?"; nocase;
uricontent:"partner_id="; nocase; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/pf/adware.180search.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001400; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_180Solutions; sid:2001400; rev:10;)
```

```
#Matt Jonkman
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE 180solutions Spyware Keywords Download"; flow: to_server,established; uricontent:"keywords/kyf"; nocase;
content:"partner_id="; nocase; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/pf/adware.180search.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2002001; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_180Solutions; sid:2002001; rev:6;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE 180solutions Spyware Install"; flow: to_server,established; uricontent:"/downloads/installers/"; nocase;
content:"simpleinternet/180sainstaller.exe"; nocase; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/pf/adware.180search.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2002003; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_180Solutions; sid:2002003; rev:6;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE 180solutions Spyware Defs Download"; flow: to_server,established; uricontent:"/geodefs/gdf"; nocase; classtype:
trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/pf/adware.180search.html; reference:url,doc.emergingthreats.net/bin/view/Main/2002048;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_180Solutions; sid:2002048; rev:5;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE 180solutions Spyware config Download"; flow: to_server,established; uricontent:"/config.aspx?did="; nocase;
classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/pf/adware.180search.html; reference:url,doc.emergingthreats.net/bin/view/Main/2002099;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_180Solutions; sid:2002099; rev:4;)

#By M Shirk from Listening Post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE 180solutions Spyware versionconfig POST"; flow:to_server,established; uricontent:"/versionconfig.aspx?";
uricontent:"&ver="; nocase; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/pf/adware.180search.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2002354; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_180Solutions; sid:2002354; rev:4;)

#Matt Jonkman. Bundled from Warner Brothers Kids site.. can you believe that crap? Guess where my kids WON'T be spending my money....
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE 180solutions Spyware Actionlibs Download"; flow:to_server,established; uricontent:"/actionurls/ActionUrlb"; nocase;
uricontent:"partnerid="; nocase; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/pf/adware.180search.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2003057; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_180Solutions; sid:2003057; rev:4;)

#Matt Jonkman. Bundled from Warner Brothers Kids site.. can you believe that crap? Guess where my kids WON'T be spending my money....
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE 180solutions (Zango) Spyware Installer Download"; flow:to_server,established;
uricontent:"/Zango/ZangoInstaller.exe"; nocase; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/pf/adware.180search.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2003058; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_180Solutions; sid:2003058; rev:4;)

#Matt Jonkman. Bundled from Warner Brothers Kids site.. can you believe that crap? Guess where my kids WON'T be spending my money....
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE 180solutions (Zango) Spyware TB Installer Download"; flow:to_server,established;
uricontent:"/ZangoTBInstaller.exe"; nocase; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/pf/adware.180search.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2003059; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_180Solutions; sid:2003059; rev:4;)

#Matt Jonkman. Bundled from Warner Brothers Kids site.. can you believe that crap? Guess where my kids WON'T be spending my money....
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE 180solutions (Zango) Spyware Local Stats Post"; flow:to_server,established; uricontent:"/php/rpc_uci.php"; nocase;
classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/pf/adware.180search.html; reference:url,doc.emergingthreats.net/bin/view/Main/2003060;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_180Solutions; sid:2003060; rev:4;)

#Matt Jonkman. Bundled from Warner Brothers Kids site.. can you believe that crap? Guess where my kids WON'T be spending my money....
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE 180solutions (Zango) Spyware Event Activity Post"; flow:to_server,established; uricontent:"/php/uci.php"; nocase;
classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/pf/adware.180search.html; reference:url,doc.emergingthreats.net/bin/view/Main/2003061;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_180Solutions; sid:2003061; rev:3;)

#New zango url
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Zango Spyware Activity"; flow:to_server,established; uricontent:"/banman/banman.asp?ZoneID="; nocase;
uricontent:"&Task="; nocase; uricontent:"&X="; nocase; classtype:trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/pf/adware.180search.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2003170; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_180Solutions; sid:2003170; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE 180solutions (Zango) Spyware Installer Config 2"; flow:to_server,established; uricontent:"config.aspx"; nocase;
uricontent:"?ver="; nocase; content:"HTTP"; nocase; content:!"User-Agent|3a| "; classtype: trojan-activity;
reference:url,securityresponse.symantec.com/avcenter/venc/data/pf/adware.180search.html; reference:url,doc.emergingthreats.net/bin/view/Main/2003217;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_180Solutions; sid:2003217; rev:6;)

#more from the spywarelp
#Matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE 180solutions Spyware (tracked event 2 reporting)"; flow: to_server,established; uricontent:"/trackedevent.aspx?";
nocase; uricontent:"ver="; nocase; uricontent:"&pkg_ver="; nocase; uricontent:"&rnd="; nocase; classtype: trojan-activity;
reference:url,securityresponse.symantec.com/avcenter/venc/data/pf/adware.180search.html; reference:url,doc.emergingthreats.net/bin/view/Main/2003306;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_180Solutions; sid:2003306; rev:6;)

#more from the spywarelp
#Matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Zango Spyware (tbrequest data post)"; flow: to_server,established; uricontent:"/tbrequest"; nocase;
uricontent:"&q="; nocase; pcre:"/\/tbrequest\d+\.php/Ui"; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/pf/adware.180search.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2003610; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_180Solutions; sid:2003610; rev:3;)

#by Russ McRee
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Zango Spyware Post"; flow:to_server,established; uricontent:"/te.aspx?ver="; nocase; pcre:"/ver=[\v\d]+/Ui";
classtype:trojan-activity; reference:url,usa.kaspersky.com/about-us/news-press-releases.php?smnr_id=900000045; reference:url,doc.emergingthreats.net/bin/view/Main/2007607;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_180Solutions; sid:2007607; rev:4;)

#Submitted by Joel Esler
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Spyware 2020"; flow: to_server,established; content:"|48 6F 73 74 3A 20 77 77 77 2E 32 30 32 30 73 65 61 72 63 68
2E 63 6F 6D|"; content:"|49 70 41 64 64 72|"; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/spyware.2020search.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2000327; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_2020search; sid:2000327; rev:9;)

#Submitted by Jason Haar
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE 2020search Update Engine"; flow: to_server,established; content:"POST"; depth: 4; content:"srng/reg.php HTTP";
within: 50; content:"|0d0a|Host|3a|"; content:"2020search.com"; within: 40; content:"IpAddr="; nocase; within: 100; classtype: trojan-activity; reference:url,www.safer-
networking.org/index.php?page=updatehistory&detail=2004-03-04; reference:url,doc.emergingthreats.net/bin/view/Main/2000934; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_2020search; sid:2000934; rev:7;)

#by: Jeremy Conway at sudosecure.net
#ref: 2b8175726f2dde727132299992dafbe9
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE 2020search/PowerSearch Toolbar Adware/Spyware - GET"; flow:established,to_server; content:"GET "; depth:4;
uricontent:"IpAddr="; nocase; uricontent:"&OS="; nocase; uricontent:"&RegistryChanged="; nocase; uricontent:"&RegistryUpdate="; nocase; uricontent:"&NewInstallation="; nocase;
uricontent:"&utilMissing="; nocase; uricontent:"&Basedir="; nocase; uricontent:"&BundleID="; nocase; uricontent:"&InitInstalled="; nocase; uricontent:"&Interval="; nocase;
uricontent:"&LastInitRun="; nocase; uricontent:"&LastInitVer="; nocase; uricontent:"&LastSrngRun="; nocase; uricontent:"&LastUtilRun="; nocase; uricontent:"&SrngInstalled="; nocase;
uricontent:"&SrngVer="; nocase; uricontent:"&UtilInstalled="; nocase; uricontent:"&UtilVer="; nocase; uricontent:"&PCID"; nocase; classtype:trojan-activity;
reference:url,vil.nai.com/vil/content/v_103738.htm; reference:url,www.sunbeltsecurity.com/ThreatDisplay.aspx?tid=13811&cs=1437A28B7A90C4C502B683CE6DE23C4E;
reference:url,www.symantec.com/security_response/writeup.jsp?docid=2004-111918-0210-99; reference:url,doc.emergingthreats.net/2009807; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_2020search; sid:2009807; rev:2;)
```

```
#Submitted by Chris Norton
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET MALWARE 2nd-thought (W32.Daqa.C) Download"; flow: from_server,established; content:"|67 6f 69 64 72 2e 63 61 62|"; nocase;
content:"|48 6f 73 74 3a 20 77 77 77 2e 77 65 62 6e 65 74 69 6e 66 6f 2e 6e 65 74|"; nocase; classtype: trojan-activity;
reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.secondthought.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001447;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_2nd-Thought; sid:2001447; rev:7;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE 360safe.com related Fake Security Product Update"; flow:established,to_server; uricontent:"/?fixtool="; nocase;
content:"GET /?fixtool="; offset:0; depth:16; content:!"|0d 0a|User-Agent|3a| "; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008036;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_360safe.com; sid:2008036; rev:4;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE 360safe.com related Fake Security Product Update (KillerSet)"; flow:established,to_server; uricontent:"/?
KillerSet="; nocase; content:"GET /?KillerSet="; offset:0; depth:16; content:!"|0d 0a|User-Agent|3a| "; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2008149; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_360safe.com; sid:2008149; rev:4;)

#from spyware listening post data, by matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE 51yes.com Spyware Reporting User Activity"; flow:established,to_server; uricontent:"/sa.aspx?id="; nocase;
uricontent:"&refe=http"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003620; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_51yes.com; sid:2003620; rev:3;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE A-d-w-a-r-e.com Activity (popup)"; flow: established,to_server; uricontent:"/cgi-bin/PopupV"; nocase; uricontent:"?
ID={"; nocase; classtype: trojan-activity; reference:url,www.a-d-w-a-r-e.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001730; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_A-d-w-a-r-e.com; sid:2001730; rev:8;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE A-d-w-a-r-e.com Activity (cmd)"; flow: established,to_server; uricontent:"/app/VT00/ucmd.php?V="; nocase;
classtype: trojan-activity; reference:url,www.a-d-w-a-r-e.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001735; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_A-d-w-a-r-e.com; sid:2001735; rev:7;)

#By Mark Tombaugh
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE ABX Toolbar ActiveX Install"; flow: to_server,established; uricontent:"/abx_search_webinstall/abx_search.cab";
nocase; classtype: trojan-activity; reference:url,isc.sans.org/diary.php?date=2005-03-04; reference:url,doc.emergingthreats.net/bin/view/Main/2001761;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_ABX_Toolbar; sid:2001761; rev:5;)

#By Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Abcsearch.com Spyware Reporting"; flow:established,to_server; uricontent:"/cgi-bin/search/mxml.fcgi?"; nocase;
uricontent:"Terms="; nocase; uricontent:"&affiliate="; nocase; uricontent:"&subid="; nocase; uricontent:"&Hits_Per_Page="; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2003438; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Abcsearch.com; sid:2003438; rev:3;)

#Submitted by cooljay
#
#alert tcp $EXTERNAL_NET 20 -> $HOME_NET any (msg:"ET MALWARE Abox Download"; flow:established,to_server; content:"|5c 00 43 00 61 00 72 00 6d 00 65 00 6e 00 00 00 16 00 00 00 73 00 75
00 63|"; nocase; offset:160; depth:26; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001440; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Abox; sid:2001440; rev:7;)

#Submitted by cooljay
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Abox Install Report"; flow: to_server,established; uricontent:"&time="; nocase; uricontent:"/new_install?id=";
classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.adultbox.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001441;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Abox; sid:2001441; rev:11;)

#by Matt Jonkman from Listening Post Data
#Disabling, obsoleting. To be delleted in a month or so
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Adultfriendfinder.com Spyware Iframe Download"; flow:to_server,established; uricontent:"/promo/affiframe.jsp?
Pid="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002353; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Adultfriendfinder.com; sid:2002353; rev:4;)

#by Philipp Bescht
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Advert-network.com Related Spyware Updating"; flow:established,to_server; uricontent:"/cnconfig.gz?ct=";
uricontent:"&bp="; uricontent:"&vs="; uricontent:"&country="; uricontent:"&grp="; uricontent:"&tcpc="; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2008419; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Advert-network.com; sid:2008419; rev:2;)

#by Philipp Bescht
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Advert-network.com Related Spyware Checking for Updates"; flow:established,to_server; content:"POST "; depth:5;
uricontent:"/check.php?tcpc="; content:!"|0d 0a|User-Agent|3a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008425;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Advert-network.com; sid:2008425; rev:3;)

#by Matt Jonkman
#spyware, from the sandnet
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Advertisementserver.com Spyware Initial Checkin"; flow:to_server,established; uricontent:"?UID="; nocase;
uricontent:"&DIST="; nocase; uricontent:"&NPR="; nocase; content:"User-Agent|3a| Microsoft URL Control"; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2007601; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Advertisementserver.com; sid:2007601; rev:4;)

#by Matt Jonkman
#spyware, from the sandnet
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Advertisementserver.com Spyware Checkin"; flow:to_server,established; uricontent:"monitor.php"; nocase;
uricontent:"?UID="; nocase; pcre:"/UID=\d+/Ui"; content:"User-Agent|3a| Microsoft URL Control"; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2007602; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Advertisementserver.com; sid:2007602; rev:5;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Advertising.com Data Post (villains)"; flow: to_server,established; uricontent:"/Games/villains.aspx"; nocase;
classtype: policy-violation; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.fastseek.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001228;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Advertising.com_Bot; sid:2001228; rev:8;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Advertising.com Data Post (cakedeal)"; flow: to_server,established; uricontent:"/Games/cakedeal.aspx"; nocase;
classtype: policy-violation; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.fastseek.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001230;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Advertising.com_Bot; sid:2001230; rev:8;)

#From Listening Post data
#Hits on normal ads, not reporting data
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Advertising.com Reporting Data"; flow: to_server,established; uricontent:"/site="; uricontent:"/mnum=";
uricontent:"/bins="; uricontent:"/rich="; uricontent:"/logs="; uricontent:"/betr="; classtype: policy-violation;
reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.fastseek.html; reference:url,doc.emergingthreats.net/bin/view/Main/2002304;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Advertising.com_Bot; sid:2002304; rev:6;)

#by Matt Jonkman
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Adware Command Client Checkin"; flow: to_server,established; uricontent:"/client.php?str="; nocase; content:"User-
Agent|3a| "; nocase; content:"Indy Library)"; within:30; nocase; classtype: policy-violation; reference:url,www.nuker.com/container/details/adware_command.php;
reference:url,doc.emergingthreats.net/bin/view/Main/2003446; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Adware_Command; sid:2003446; rev:5;)

#by pedro Marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Generic Adware Install Report"; flow:established,to_server; content:"GET "; depth:4; uricontent:"/nsi_install.php?
inst_result=success&aff_id="; uricontent:"&id="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010630; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Adware_Command; sid:2010630; rev:3;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Adwave Agent Access"; flow: to_server,established; uricontent:"/search_404.aspx?aff="; nocase; classtype: policy-
violation; reference:url,www.intermute.com/spyware/HuntBar.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001318; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Adwave; sid:2001318; rev:7;)

#Submitted by Chris Norton
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Wintools Download/Configure"; flow: to_server,established; uricontent:"/WTools"; nocase; uricontent:".cab"; nocase;
classtype: trojan-activity; reference:url,www.intermute.com/spyware/HuntBar.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001450; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Adwave; sid:2001450; rev:11;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Casalemedia Access, Likely Spyware"; flow: to_server,established; content:"Host|3a|"; nocase; content:".ak-
networks.com"; nocase; within: 30; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001529; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Ak-networks.com; sid:2001529; rev:10;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE ak-networks.com Spyware Code Download"; flow: to_server,established; uricontent:"/SyncAkSoft.da_"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001530; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Ak-networks.com;
sid:2001530; rev:8;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE ak-networks.com Spyware Code Install"; flow: to_server,established; uricontent:"/akcore.dl_"; nocase; classtype:
trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001737; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Ak-networks.com; sid:2001737;
rev:6;)

#by Matt Jonkman from listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Alexa Spyware Reporting URL"; flow:established,to_server; uricontent:"/image_server.cgi?size=small&url=http|3a|/";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002349; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Alexa;
sid:2002349; rev:5;)

#by Matt Jonkman from listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Alexa Spyware Reporting"; flow:established,to_server; uricontent:"/data?"; nocase; uricontent:"cli="; nocase;
uricontent:"&dat="; nocase; uricontent:"&ver="; nocase; uricontent:"&uid="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003219;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Alexa; sid:2003219; rev:3;)

#by Matt Jonkman from listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Alexa Spyware Reporting URL Visited"; flow:established,to_server; uricontent:"/data/"; nocase; uricontent:"&cli=";
nocase; uricontent:"&dat="; nocase; uricontent:"&ver="; nocase; uricontent:"&url="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003606;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Alexa; sid:2003606; rev:3;)

#by Matt Jonkman from listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Alexa Spyware Redirecting User"; flow:established,to_server; uricontent:"/redirect?http"; nocase; content:"Host|3a|
redirect.alexa.com"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003619; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Alexa; sid:2003619; rev:4;)

#Modified and added to by Matt Jonkman (Original author missing)
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Altnet PeerPoints Manager Start"; flow: to_server,established; uricontent:"/pm/start.asp"; nocase; classtype:
policy-violation; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.topsearch.html; reference:url,doc.emergingthreats.net/bin/view/Main/2000906;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Altnet_Peerpoint_Manager_Traffic; sid:2000906; rev:8;)

#Modified and added to by Matt Jonkman (Original author missing)
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Altnet PeerPoints Manager Data Submission"; flow: to_server,established;
uricontent:"/backoffice.net/stats/Add.aspx"; nocase; classtype: policy-violation; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.topsearch.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2000598; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Altnet_Peerpoint_Manager_Traffic; sid:2000598;
rev:8;)

#Modified and added to by Matt Jonkman (Original author missing)
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Altnet PeerPoints Manager Settings Download"; flow: to_server,established;
uricontent:"/pointsmanager/settings.cab?"; nocase; classtype: policy-violation; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.topsearch.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2000907; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Altnet_Peerpoint_Manager_Traffic; sid:2000907;
rev:9;)

#fake antispyware package, sig by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Anti-virus-pro.com Fake AV Checkin"; flow:established,to_server; uricontent:"/stat.php?machine_id={"; nocase;
pcre:"/machine_id={[A-F0-9]+-[A-F0-9]+-[A-F0-9]+-[A-F0-9]+-[A-F0-9]+}/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007886;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Anti-virus-pro.com; sid:2007886; rev:2;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Avres Agent Receiving Instructions"; flow: to_server,established; uricontent:"/ie/updatenew/"; content:"CONFIG";
nocase; classtype: trojan-activity; reference:url,www.avres.net; reference:url,ar.avres.net/ie/updatenew/; reference:url,doc.emergingthreats.net/bin/view/Main/2000903;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Avres; sid:2000903; rev:6;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE BTGrab.com Spyware Downloading Ads"; flow: to_server,established; uricontent:"/a/Drk.syn?"; nocase;
uricontent:"adcontext="; nocase; classtype: trojan-activity; reference:url,www.btgrab.com; reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=453090726;
reference:url,doc.emergingthreats.net/bin/view/Main/2001999; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_BTGrab.com; sid:2001999; rev:7;)

#Matt Jonkman from spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Baidu.com Spyware Bar Reporting"; flow:to_server,established; uricontent:"/update/barcab/"; nocase;
classtype:policy-violation; reference:url,www.pctools.com/mrc/infections/id/BaiDu/; reference:url,doc.emergingthreats.net/bin/view/Main/2003340;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Baidu.com; sid:2003340; rev:3;)

#Matt Jonkman from spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Baidu.com Spyware Bar Pulling Content"; flow:to_server,established; uricontent:"/update/cab/loadmovie.swf"; nocase;
content:"bar.baidu.com"; nocase; classtype:policy-violation; reference:url,www.pctools.com/mrc/infections/id/BaiDu/; reference:url,doc.emergingthreats.net/bin/view/Main/2003341;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Baidu.com; sid:2003341; rev:3;)

#Matt Jonkman from spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Baidu.com Spyware Bar Pulling Data"; flow:to_server,established; uricontent:"/cpro/ui/ui"; nocase;
content:"baidu.com"; nocase; content:!"Referer|3a| "; nocase; classtype:trojan-activity; reference:url,www.pctools.com/mrc/infections/id/BaiDu/;
reference:url,doc.emergingthreats.net/bin/view/Main/2003578; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Baidu.com; sid:2003578; rev:6;)
```

```
#Matt Jonkman from spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Baidu.com Spyware Bar Activity"; flow:to_server,established; uricontent:"/n?cmd="; nocase; uricontent:"&class=";
nocase; uricontent:"&pn="; nocase; uricontent:"&tn"; nocase; classtype:trojan-activity; reference:url,www.pctools.com/mrc/infections/id/BaiDu/;
reference:url,doc.emergingthreats.net/bin/view/Main/2003605; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Baidu.com; sid:2003605; rev:3;)

#Matt Jonkman from spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Baidu.com Spyware Sobar Bar Activity"; flow:to_server,established; uricontent:"/sobar/sobar"; nocase;
classtype:trojan-activity; reference:url,www.pctools.com/mrc/infections/id/BaiDu/; reference:url,doc.emergingthreats.net/bin/view/Main/2003630;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Baidu.com; sid:2003630; rev:3;)

#by Jeremy at sudosecure.net
#ref: c182bfbaff0a5187c95020d4ae602ac0
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Adaware.BarACE Checkin and Update"; flow:established,to_server; content:"GET "; depth:4;
uricontent:"|2E|php|3F|zone="; nocase; uricontent:"|26|name="; nocase; uricontent:"|26|bpid="; nocase; uricontent:"|26|bnum="; nocase; uricontent:"|26|pid="; nocase; classtype:trojan-
activity; reference:url,www.symantec.com/security_response/writeup.jsp?docid=2007-021714-2431-99&tabid=2; reference:url,doc.emergingthreats.net/bin/view/Main/2008318;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_BarAce; sid:2008318; rev:3;)

#Submitted by Jonathan Miner
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Bargain Buddy"; flow: to_server,established; uricontent:"/download/bargin_buddy"; nocase; classtype: trojan-
activity; reference:url,www.doxdesk.com/parasite/BargainBuddy.html; reference:url,doc.emergingthreats.net/bin/view/Main/2000574; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Bargain_Buddy; sid:2000574; rev:9;)

#By John Stewart
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Begin2Search.com Spyware"; flow: to_server,established; content:"/cgi-bin/fav_del.fcgi?id"; nocase; classtype:
policy-violation; reference:url,sarc.com/avcenter/venc/data/adware.begin2search.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001885;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Begin2Search; sid:2001885; rev:6;)

#Matt Jonkman, caught off of fastmp3search.com.ar
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Best-targeted-traffic.com Spyware Checkin"; flow:established,to_server; uricontent:"/checkin.php?"; nocase;
uricontent:"unq="; nocase; uricontent:"version="; nocase; content:"User-Agent|3a| Opera "; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2003209; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Best-Targeted-Traffic.com; sid:2003209;
rev:4;)

#Matt Jonkman, caught off of fastmp3search.com.ar
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Best-targeted-traffic.com Spyware Install"; flow:established,to_server; uricontent:"/install.php?"; nocase;
uricontent:"&pais="; nocase; uricontent:"unq="; nocase; content:"User-Agent|3a| Opera "; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003210;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Best-Targeted-Traffic.com; sid:2003210; rev:4;)

#Matt Jonkman, caught off of fastmp3search.com.ar
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Best-targeted-traffic.com Spyware Ping"; flow:established,to_server; uricontent:"/ping.php?"; nocase;
uricontent:"ul=http"; nocase; uricontent:"unq="; nocase; content:"User-Agent|3a| Opera "; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003211;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Best-Targeted-Traffic.com; sid:2003211; rev:4;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Bestcount.net Spyware Checkin"; flow:established,to_server; uricontent:"/adv/"; nocase; uricontent:"/adload.php?
a1="; nocase; uricontent:"&a2=Type of Processor|3a|"; nocase; uricontent:"&a3=Windows version is "; nocase; uricontent:"&a4=Build|3a|"; nocase; classtype:trojan-activity;
reference:url,reports.internic.net/cgi/whois?whois_nic=bestcount.net&type=domain; reference:url,doc.emergingthreats.net/bin/view/Main/2002955; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Bestcount.net; sid:2002955; rev:4;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Bestcount.net Spyware Downloading vxgame"; flow:established,to_server; uricontent:"/vxgame1/vxv.php"; nocase;
classtype:trojan-activity; reference:url,reports.internic.net/cgi/whois?whois_nic=bestcount.net&type=domain; reference:url,doc.emergingthreats.net/bin/view/Main/2002956;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Bestcount.net; sid:2002956; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Bestcount.net Spyware Initial Infection Download"; flow:established,to_server; uricontent:"/win32.exe"; nocase;
pcre:"/\/adv\/\d+\/win32\.exe/Ui"; classtype:trojan-activity; reference:url,reports.internic.net/cgi/whois?whois_nic=bestcount.net&type=domain;
reference:url,doc.emergingthreats.net/bin/view/Main/2002957; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Bestcount.net; sid:2002957; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Bestcount.net Spyware Exploit Download"; flow:established,to_server; uricontent:"/sploit.anr"; nocase;
classtype:trojan-activity; reference:url,reports.internic.net/cgi/whois?whois_nic=bestcount.net&type=domain; reference:url,doc.emergingthreats.net/bin/view/Main/2003153;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Bestcount.net; sid:2003153; rev:3;)

#Matt Jonkman
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Bestcount.net Spyware Data Upload"; flow:established,to_server; uricontent:"/objects/ocget.dll"; nocase;
content:"mybest"; nocase; depth:150; classtype:trojan-activity; reference:url,reports.internic.net/cgi/whois?whois_nic=bestcount.net&type=domain;
reference:url,doc.emergingthreats.net/bin/view/Main/2003154; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Bestcount.net; sid:2003154; rev:5;)

#Submitted by Jonathan Miner
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Binet (download complete)"; flow: to_server,established; uricontent:"/download/cabs/"; nocase;
uricontent:"download_complete.htm"; nocase; classtype: trojan-activity; reference:url,sarc.com/avcenter/venc/data/pf/adware.betterinternet.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2000366; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Betterinternet; sid:2000366; rev:12;)

#Submitted by Jonathan Miner
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Binet (set_pix)"; flow: to_server,established; uricontent:"/download/cabs/set_pix.php"; nocase;
content:"abetterinternet.com"; nocase; classtype: trojan-activity; reference:url,sarc.com/avcenter/venc/data/pf/adware.betterinternet.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2000367; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Betterinternet; sid:2000367; rev:9;)

#Submitted by Jonathan Miner
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Binet (randreco.exe)"; flow: to_server,established; uricontent:"/download/cabs/RANDRECO/randreco.exe"; nocase;
content:"abetterinternet.com"; nocase; classtype: trojan-activity; reference:url,sarc.com/avcenter/venc/data/pf/adware.betterinternet.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2000371; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Betterinternet; sid:2000371; rev:9;)

#Submitted by Jonathan Miner
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Binet Ad Retrieval"; flow: to_server,established; uricontent:"/bba/flashimages/"; nocase; classtype: trojan-
activity; reference:url,sarc.com/avcenter/venc/data/pf/adware.betterinternet.html; reference:url,doc.emergingthreats.net/bin/view/Main/2000593;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Betterinternet; sid:2000593; rev:7;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Twaintec Download Attempt"; flow: to_server,established; uricontent:"/downloads/cabs/TWTDLL/twaintec.cab"; nocase;
classtype: trojan-activity; reference:url,www.pestpatrol.com/PestInfo/t/twain-tech.asp; reference:url,doc.emergingthreats.net/bin/view/Main/2001198;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Betterinternet; sid:2001198; rev:6;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Twaintec Ad Retrieval"; flow: to_server,established; uricontent:"/twain/servlet/Twain?adcontext="; nocase;
classtype: trojan-activity; reference:url,www.pestpatrol.com/PestInfo/t/twain-tech.asp; reference:url,doc.emergingthreats.net/bin/view/Main/2001199;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Betterinternet; sid:2001199; rev:6;)
```

```
#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Twaintec Reporting Data"; flow: to_server,established; uricontent:"/downloads/record_download.asp"; nocase;
classtype: trojan-activity; reference:url,www.pestpatrol.com/PestInfo/t/twain-tech.asp; reference:url,doc.emergingthreats.net/bin/view/Main/2001216;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Betterinternet; sid:2001216; rev:6;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE BInet Information Upload"; flow: to_server,established; uricontent:"/bi/servlet/ThinstallPre"; nocase; classtype:
trojan-activity; reference:url,sarc.com/avcenter/venc/data/pf/adware.betterinternet.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001339;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Betterinternet; sid:2001339; rev:7;)

#Data from Allison Macfarland
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE BInet Information Install Report"; flow: to_server,established; uricontent:"/bi/servlet/ThinstallPost"; nocase;
classtype: trojan-activity; reference:url,sarc.com/avcenter/venc/data/pf/adware.betterinternet.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001576;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Betterinternet; sid:2001576; rev:6;)

#Submitted by Matt Jonkman
#Disabling this rule, it needs work. It's hitting on legit ad referrals
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Bfast.com Spyware"; flow: to_server,established; uricontent:"/bfast/serve?bfmid"; nocase; classtype: policy-
violation; reference:url,doc.emergingthreats.net/bin/view/Main/2001398; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Bfast.com; sid:2001398; rev:7;)

#from spyware LP data, by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Bizconcept.info Spyware Checkin"; flow:to_server,established; content:"POST "; depth:5; nocase;
uricontent:"/zuzu.php?&r="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2005319; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Bizconcept.info; sid:2005319; rev:3;)

#Submitted by Allison MacFarlan
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Bonziportal Traffic"; flow: to_server,established; uricontent:"/bonziportal/bin/"; classtype: trojan-activity;
reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=59256; reference:url,doc.emergingthreats.net/bin/view/Main/2001345; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Bonzi; sid:2001345; rev:7;)

#by Jeffrey Brown
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Borlander Adware Checkin"; flow:to_server,established; content:"GET "; depth:4; nocase; uricontent:"?t="; nocase;
uricontent:"&i="; nocase; uricontent:"&v="; nocase; uricontent:"&d="; nocase; uricontent:"&a="; nocase; uricontent:"&n="; classtype:bad-unknown;
reference:url,doc.emergingthreats.net/bin/view/Main/2008736; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Borlander.com.cn; sid:2008736; rev:2;)

#Matt Jonkman
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Bravesentry.com Fake Antispyware Download"; flow:established,to_server; uricontent:"/bravesentry.exe"; nocase;
classtype:trojan-activity; reference:url,www.bravesentry.com; reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=BraveSentry&threatid=44152;
reference:url,doc.emergingthreats.net/bin/view/Main/2002954; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Bravesentry; sid:2002954; rev:4;)

#Matt Jonkman
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Bravesentry.com Fake Antispyware Updating"; flow:established,to_server; uricontent:"/update.php?v="; nocase;
uricontent:"&d="; nocase; uricontent:"&vs="; nocase; content:!"User-Agent|3a| "; content:"Host|3a| "; content:".bravesentry.com"; distance:0; nocase; classtype:trojan-activity;
reference:url,www.bravesentry.com; reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=BraveSentry&threatid=44152;
reference:url,doc.emergingthreats.net/bin/view/Main/2003541; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Bravesentry; sid:2003541; rev:5;)

#Matt Jonkman
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Bravesentry.com/Protectwin.com Fake Antispyware Reporting"; flow:established,to_server; uricontent:"/download.php?
&advid="; nocase; uricontent:"&u="; nocase; uricontent:"&p="; nocase; content:!"User-Agent|3a| "; content:"Host|3a| "; content:".bravesentry.com"; distance:0; nocase; classtype:trojan-
activity; reference:url,www.bravesentry.com; reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=BraveSentry&threatid=44152;
reference:url,doc.emergingthreats.net/bin/view/Main/2003542; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Bravesentry; sid:2003542; rev:4;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Browseraid.com Agent Reporting Data"; flow: to_server,established; uricontent:"/perl/ads.pl"; nocase; classtype:
trojan-activity; reference:url,www.browseraid.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001266; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Browseraid; sid:2001266; rev:12;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Browseraid.com Agent Updating"; flow: to_server,established; uricontent:"/perl/uptodate.pl"; nocase;
content:"uptodate.browseraid.com"; nocase; classtype: trojan-activity; reference:url,www.browseraid.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001304;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Browseraid; sid:2001304; rev:7;)

#By Matt Jonkman
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Clickspring.net Spyware Reporting"; flow: to_server,established; content:"Host|3a| www.bullseye-network.com";
nocase; classtype: trojan-activity; reference:url,sarc.com/avcenter/venc/data/adware.bargainbuddy.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001501;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Bullseye-Network.com; sid:2001501; rev:7;)

#Submitted by Chris Norton
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Bundleware Spyware Download"; flow: to_server,established; uricontent:"/app/InternetFuel/AppWrap.exe"; nocase;
classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2001451; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Bundleware;
sid:2001451; rev:6;)

#Submitted by Chris Norton
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Bundleware Spyware CHM Download"; flow: to_server,established; content:"Referer|3a| ms-
its|3a|mhtml|3a|file|3a|//C|3a|counter.mht!http|3a|//"; nocase; content:"/counter/HELP3.CHM|3a 3a|/help.htm"; nocase; classtype: trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2001452; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Bundleware; sid:2001452; rev:6;)

#Submitted by Chris Norton
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Bundleware Spyware cab Download"; flow: to_server,established; uricontent:"/counter/counter_v3.cab"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001458; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Bundleware;
sid:2001458; rev:5;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE C4tdownload.com Access, Likely Spyware"; flow: to_server,established; content:"Host|3a|"; nocase;
content:".c4tdownload.com"; within:26; nocase; classtype: trojan-activity; reference:url,sarc.com/avcenter/venc/data/adware.clickdloader.b.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001531; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_C4tdownload.com; sid:2001531; rev:13;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE C4tdownload.com Spyware Activity"; flow: to_server,established; uricontent:"/js.php?event_type=onload&recurrence=";
nocase; classtype: trojan-activity; reference:url,sarc.com/avcenter/venc/data/adware.clickdloader.b.html; reference:url,doc.emergingthreats.net/bin/view/Main/2002088;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_C4tdownload.com; sid:2002088; rev:5;)

#from sandnet analysis, called CASClient by Kaspersky
#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE CASClient Spyware/Adware Install Checkin"; flow:established,to_server; content:"POST "; depth:5;
uricontent:"/ctrl/chkmac.php?mac="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2006403; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_CASClient; sid:2006403; rev:3;)

#from sandnet analysis, called CASClient by Kaspersky
#by Matt Jonkman
```

```
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE CASClient Spyware/Adware Checkin"; flow:established,to_server; content:"POST "; depth:5;
uricontent:"/ctrl/ctrv.php"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2006404; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_CASClient; sid:2006404; rev:3;)

#By Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE CNSMIN (3721.com) Spyware Activity"; flow:established,to_server; uricontent:"/download/CnsMin"; nocase;
uricontent:"?t="; nocase; classtype:trojan-activity; reference:url,www.spyany.com/program/article_spy_rm_CnsMin.html; reference:url,doc.emergingthreats.net/bin/view/Main/2003417;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_CNSMIN; sid:2003417; rev:3;)

#By Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE CNSMIN (3721.com) Spyware Activity 2"; flow:established,to_server; uricontent:"/download/CnsUp"; nocase;
uricontent:"?t="; nocase; classtype:trojan-activity; reference:url,www.spyany.com/program/article_spy_rm_CnsMin.html; reference:url,doc.emergingthreats.net/bin/view/Main/2003418;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_CNSMIN; sid:2003418; rev:3;)

#By Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE CNSMIN (3721.com) Spyware Activity 3"; flow:established,to_server; uricontent:"/download/autolvsw.ini?"; nocase;
uricontent:"?t="; nocase; classtype:trojan-activity; reference:url,www.spyany.com/program/article_spy_rm_CnsMin.html; reference:url,doc.emergingthreats.net/bin/view/Main/2003419;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_CNSMIN; sid:2003419; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE CWS qck.cc Spyware Installer (in.php)"; flow:established,to_server; uricontent:"/x/in.php?wm="; nocase;
classtype:trojan-activity; reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=453076035; reference:url,doc.emergingthreats.net/bin/view/Main/2002089;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_CWS; sid:2002089; rev:7;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE CWS qck.cc Spyware Installer (web.php)"; flow:established,to_server; uricontent:"/x/tbd_web.php?wm="; nocase;
classtype:trojan-activity; reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=453076035; reference:url,doc.emergingthreats.net/bin/view/Main/2002095;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_CWS; sid:2002095; rev:5;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE CWS Trafcool.biz Related Installer"; flow:established,to_server; uricontent:"/progs_traff/"; nocase;
classtype:trojan-activity; reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=453076035; reference:url,doc.emergingthreats.net/bin/view/Main/2002931;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_CWS; sid:2002931; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE CWS Related Installer"; flow:established,to_server; uricontent:"/livesupport/image_tracker.php?"; nocase;
uricontent:"l=support&"; nocase; uricontent:"x=1&"; nocase; uricontent:"deptid=1&"; nocase; uricontent:"&page=http"; nocase; uricontent:"&unique="; nocase; classtype:trojan-activity;
reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=453076035; reference:url,doc.emergingthreats.net/bin/view/Main/2002932; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_CWS; sid:2002932; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE CWS Spy-Sheriff.com Infeced Buy Page Request"; flow:established,to_server; uricontent:"/?advid="; nocase;
content:"spy-sheriff.com"; nocase; classtype:trojan-activity; reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=453076035;
reference:url,doc.emergingthreats.net/bin/view/Main/2002933; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_CWS; sid:2002933; rev:3;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Spywaremover Activity"; flow: to_server,established; uricontent:"/download/cabs/THNALL1L/thnall1l.exe"; classtype:
trojan-activity; reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=453087903; reference:url,doc.emergingthreats.net/bin/view/Main/2001521;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Callinghome.biz; sid:2001521; rev:10;)

#by Deapesh Misra
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Casalemedia Spyware Reporting URL Visited 3"; flow: to_server,established; uricontent:"/sd?"; nocase; pcre:"/\/sd\?
s=\d+&f=\d&C=\d/Ui"; classtype: trojan-activity; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Casalemedia.com;
reference:url,doc.emergingthreats.net/2009880; sid:2009880; rev:3;)

#by Deapesh Misra
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Casalemedia Spyware Reporting URL Visited 2"; flow: to_server,established; uricontent:"/sd?"; nocase; pcre:"/\/sd\?
s=\d+&f=\d/Ui"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002196; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Casalemedia.com; sid:2002196; rev:1;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Casino on Net Install"; flow: to_server,established; uricontent:"/newdownload/newsetup/"; nocase;
content:"casinone"; nocase; classtype: trojan-activity; reference:url,www.888casino.net; reference:url,doc.emergingthreats.net/bin/view/Main/2001041;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_CasinoonNet; sid:2001041; rev:7;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Casino on Net Reporting Data"; flow: to_server,established; uricontent:"/logs.asp?MSGID=100"; nocase; classtype:
trojan-activity; reference:url,www.888casino.net; reference:url,doc.emergingthreats.net/bin/view/Main/2001031; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_CasinoonNet; sid:2001031; rev:7;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Casino on Net Ping Hit"; flow: to_server,established; uricontent:"/Ping/Ping.txt"; nocase; classtype: trojan-
activity; reference:url,www.888casino.net; reference:url,doc.emergingthreats.net/bin/view/Main/2001032; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_CasinoonNet; sid:2001032; rev:7;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Casino on Net Data Download"; flow: to_server,established; uricontent:"/sdl/casinov"; nocase; classtype: trojan-
activity; reference:url,www.888casino.net; reference:url,doc.emergingthreats.net/bin/view/Main/2001033; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_CasinoonNet; sid:2001033; rev:7;)

#Matt Jonkman from spywarelp data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Catchonlife.com Spyware"; flow: to_server,established; uricontent:"/nw3/r1.txt?"; content:"catchonlife"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003358; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Catchonlife.com;
sid:2003358; rev:3;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Clickspring.net Spyware Reporting Successful Install"; flow: to_server,established; uricontent:"/notify.php?
pid=remupd&module=install&v="; nocase; content:"&result=1&message=Success"; nocase; classtype: trojan-activity; reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=453082745;
reference:url,doc.emergingthreats.net/bin/view/Main/2001494; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Clickspring.net; sid:2001494; rev:6;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Clickspring.net Spyware Reporting"; flow: to_server,established; uricontent:"/notify.php?
pid=ctxad&module=NDrvExe&v="; nocase; classtype: trojan-activity; reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=453082745;
reference:url,doc.emergingthreats.net/bin/view/Main/2001500; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Clickspring.net; sid:2001500; rev:6;)

#by Matt Jonkman from spyware listeningpost data
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Cnzz.com/Baidu Related Spyware Stat Reporting"; flow:established,to_server; uricontent:"/stat.php?id="; nocase;
uricontent:"&web_id="; nocase; content:"Host|3a|"; nocase; content:!"Referer|3a| "; nocase; classtype:trojan-activity; reference:url,vil.nai.com/vil/content/v_140364.htm;
reference:url,doc.emergingthreats.net/bin/view/Main/2003607; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Cnzz.com; sid:2003607; rev:8;)

#Submitted by Jason Haar, modified
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Comet Systems Spyware Traffic"; flow: to_server,established; uricontent:"/cc/"; content:"Host|3a|
update.cc.cometsystems.com"; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2000931; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Comet_Cursor_Spyware; sid:2000931; rev:8;)

#Submitted by Jonathan Miner
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE CometSystems Spyware"; flow: to_server,established; uricontent:"/comet/request"; nocase; classtype: policy-
violation; reference:url,doc.emergingthreats.net/bin/view/Main/2001050; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Comet_Cursor_Spyware; sid:2001050;
rev:7;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Comet Systems Spyware Traffic (context.xml)"; flow: to_server,established;
uricontent:"/context/1/up_context_1.xml"; nocase; classtype: policy-violation; reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=453083029;
reference:url,doc.emergingthreats.net/bin/view/Main/2001655; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Comet_Cursor_Spyware; sid:2001655; rev:6;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Comet Systems Spyware Reporting"; flow: to_server,established; content:"Host|3a| log.cc.cometsystems.com"; nocase;
classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2001658; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Comet_Cursor_Spyware; sid:2001658; rev:6;)

#from Listening Post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Comet Systems Spyware Update Download"; flow: to_server,established; uricontent:"/cc/5/masterconfig/"; nocase;
uricontent:"/update.xml?v="; nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002351; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Comet_Cursor_Spyware; sid:2002351; rev:3;)

#from Listening Post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Comet Systems Spyware Context Report"; flow: to_server,established; uricontent:"/context/1/up_context_1.xml?v=";
nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002352; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Comet_Cursor_Spyware; sid:2002352; rev:3;)

#from spywarelp data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Comet Systems Spyware Cursor DL"; flow: to_server,established; uricontent:"/czcontent/cursor"; nocase; classtype:
policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2003307; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Comet_Cursor_Spyware;
sid:2003307; rev:3;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Conduit Connect Toolbar Message Download(Many report to be benign)"; flow: to_server,established;
uricontent:"/Message/"; content:"User-Agent|3a| EI"; nocase; pcre:"/\/Message\/\S+\/\S+\.xml/Ui"; classtype: trojan-activity; reference:url,www.conduit.com;
reference:url,doc.emergingthreats.net/bin/view/Main/2003218; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Conduit_Connect; sid:2003218; rev:4;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Content-loader.com Spyware Install"; flow: to_server,established; uricontent:"/getexe/?wmid="; nocase; classtype:
trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003074; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Contentloader.com;
sid:2003074; rev:3;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Content-loader.com Spyware Install 2"; flow: to_server,established; uricontent:"/getdata/getdata.php?wmid=";
nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003075; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Contentloader.com; sid:2003075; rev:3;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Content-loader.com (ownusa.info) Spyware Install"; flow: to_server,established; uricontent:"/fdial2.php?o=";
nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003076; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Contentloader.com; sid:2003076; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Context Plus Spyware Install"; flow: established,to_server; uricontent:"/AproposClientInstaller.exe"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001704; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_ContextPlus.net;
sid:2001704; rev:6;)

#Submitted by Chris Norton
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE ContextPanel Reporting"; flow: to_server,established; uricontent:"/cplog/?logtype="; nocase;
content:"contextpanel.com"; nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2001456; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Contextpanel; sid:2001456; rev:5;)

#by Jacob Kitchel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE CoolDeskAlert Spyware Activity"; flow:to_server,established; uricontent:"/alert/get_xml"; nocase;
content:"deskbar_id={"; nocase; classtype:trojan-activity; reference:url,cooldeskalert.com; reference:url,www.benedelman.org/spyware/images/bannerfarms-ad_w_a_r_e-globalstore-log-
061006.html; reference:url,doc.emergingthreats.net/bin/view/Main/2003462; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_CoolDeskAlert; sid:2003462;
rev:3;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Coolsearch Spyware Install"; flow: to_server,established; content:"coolsearch.biz/united.htm"; nocase; classtype:
trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001479; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Coolsearch; sid:2001479;
rev:7;)

#from Lance James and Secure Science www.securescience.net -- Thanks Lance!
#too many falses...
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Corpsespyware.net Blind Data Upload"; flow:to_server,established; uricontent:"/images/data.php?";
classtype:trojan-activity; reference:url,www.securityfocus.com/infocus/1745; reference:url,doc.emergingthreats.net/bin/view/Main/2002774; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Corpsespyware; sid:2002774; rev:3;)

#from Lance James and Secure Science www.securescience.net -- Thanks Lance!
#too many falses...
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Corpsespyware.net BlackListed Malicious Domain - google.vc"; flow:to_server,established; content:"Host|3a|";
nocase; content:"google.vc"; nocase; within:30; classtype:trojan-activity; reference:url,www.securityfocus.com/infocus/1745; reference:url,doc.emergingthreats.net/bin/view/Main/2002765;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Corpsespyware; sid:2002765; rev:5;)

#from Lance James and Secure Science www.securescience.net -- Thanks Lance!
#too many falses...
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Corpsespyware.net BlackList - pcpeek"; flow:to_server,established; content:"Host|3a|"; nocase; content:"pcpeek-
webcam-sex.com"; nocase; within:40; classtype:trojan-activity; reference:url,www.securityfocus.com/infocus/1745; reference:url,doc.emergingthreats.net/bin/view/Main/2002766;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Corpsespyware; sid:2002766; rev:5;)

#from Lance James and Secure Science www.securescience.net -- Thanks Lance!
#too many falses...
#
```

```
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Corpsespyware.net Distribution - bos.biz"; flow:to_server,established; content:"Host|3a|"; nocase;
content:"businessopportunityseeker.biz"; nocase; within:50; classtype:trojan-activity; reference:url,www.securityfocus.com/infocus/1745;
reference:url,doc.emergingthreats.net/bin/view/Main/2002767; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Corpsespyware; sid:2002767; rev:6;)

#from Lance James and Secure Science www.securescience.net -- Thanks Lance!
#too many falses...
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Corpsespyware.net Distribution - fesexy"; flow:to_server,established; content:"Host|3a|"; nocase;
content:"fesexy.net"; nocase; within:20; classtype:trojan-activity; reference:url,www.securityfocus.com/infocus/1745; reference:url,doc.emergingthreats.net/bin/view/Main/2002768;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Corpsespyware; sid:2002768; rev:5;)

#from Lance James and Secure Science www.securescience.net -- Thanks Lance!
#too many falses...
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Corpsespyware.net Distribution - studiolacase"; flow:to_server,established; content:"Host|3a|"; nocase;
content:"studiolacase.com"; nocase; within:30; classtype:trojan-activity; reference:url,www.securityfocus.com/infocus/1745; reference:url,doc.emergingthreats.net/bin/view/Main/2002769;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Corpsespyware; sid:2002769; rev:6;)

#from Lance James and Secure Science www.securescience.net -- Thanks Lance!
#too many falses...
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Corpsespyware.net - msits.exe access"; flow:to_server,established; uricontent:"/msits.exe"; nocase;
classtype:trojan-activity; reference:url,www.securityfocus.com/infocus/1745; reference:url,doc.emergingthreats.net/bin/view/Main/2002770; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Corpsespyware; sid:2002770; rev:3;)

#from Lance James and Secure Science www.securescience.net -- Thanks Lance!
#too many falses...
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Corpsespyware.net - msys.exe access"; flow:to_server,established; uricontent:"/msys.exe"; nocase;
classtype:trojan-activity; reference:url,www.securityfocus.com/infocus/1745; reference:url,doc.emergingthreats.net/bin/view/Main/2002771; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Corpsespyware; sid:2002771; rev:3;)

#Submitted by Chris Norton
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Couponage Download"; flow: to_server,established; uricontent:".dl_"; nocase; content:"couponage.com"; nocase;
classtype: policy-violation; reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=453090725; reference:url,doc.emergingthreats.net/bin/view/Main/2001453;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Couponage; sid:2001453; rev:6;)

#Submitted by Chris Norton
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Couponage Configure"; flow: to_server,established; content:".da_"; nocase; content:"couponage.com"; nocase;
classtype: policy-violation; reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=453090725; reference:url,doc.emergingthreats.net/bin/view/Main/2001454;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Couponage; sid:2001454; rev:6;)

#Submitted by Chris Norton
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Couponage Reporting"; flow: to_server,established; content:"/?keyword="; nocase; content:"couponage.com"; nocase;
classtype: policy-violation; reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=453090725; reference:url,doc.emergingthreats.net/bin/view/Main/2001455;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Couponage; sid:2001455; rev:6;)

#From Vernon Stark
#
#alert tcp any $HTTP_PORTS -> $HOME_NET any (msg:"ET MALWARE Windows executable sent when remote host claims to send an image"; flow: established,from_server; content:"Content-Type|3a|
image"; content:"MZ"; isdataat: 76,relative; content:"This program cannot be run in DOS mode"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001683;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Covert_Executable_DL; sid:2001683; rev:8;)

#From Vernon Stark
#
alert tcp any $HTTP_PORTS -> $HOME_NET any (msg:"ET MALWARE Windows executable sent when remote host claims to send image, Win32"; flow: established,from_server; content:"Content-
Type|3a| image"; content:"|0d 0a|MZ"; isdataat: 76,relative; content:"This program must be run under Win32"; classtype: trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2001684; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Covert_Executable_DL; sid:2001684; rev:9;)

#From Vernon Stark
#
alert tcp any !20 -> $HOME_NET !25 (msg:"ET MALWARE Possible Windows executable sent when remote host claims to send an image"; flow: established,from_server; content:"Content-Type|3a|
image"; content:"|0d 0a|MZ"; within: 12; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001685; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Covert_Executable_DL; sid:2001685; rev:7;)

#From Vernon Stark
#
alert tcp $EXTERNAL_NET !20 -> $HOME_NET !25 (msg:"ET MALWARE Possible Windows executable sent when remote host claims to send Javascript"; flow: established,from_server; content:"|0d
0a|Content-Type|3a| application/"; content:"javascript|0d 0a|"; within:14; content:"|0d 0a 0d 0a|MZ"; within: 40; classtype: trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2008367; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Covert_Executable_DL; sid:2008367; rev:4;)

#deapesh misra
#
alert tcp any !20 -> $HOME_NET !25 (msg:"ET MALWARE Possible Windows executable sent when remote host claims to send a Text File"; flow: established,from_server; content:"Content-
Type|3a| text/plain"; content:"|0d 0a|MZ"; within: 12; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008438;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Covert_Executable_DL; sid:2008438; rev:3;)

#deapesh misra
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET MALWARE Possible Windows executable sent when remote host claims to send html content"; flow: established,from_server;
content:"Content-Type|3a| text/html|0d 0a|"; content:"|0d 0a|MZ"; within: 100; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2009897;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Covert_Executable_DL; sid:2009897; rev:2;)

#from vienna
#
alert tcp any !20 -> $HOME_NET !25 (msg:"ET MALWARE Possible Rar'd Malware sent when remote host claims to send an Image"; flow:established,from_server; content:"Content-Type|3a|
image/"; content:"|0d 0a|Rar!"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008754; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Covert_Executable_DL; sid:2008754; rev:2;)

#by: Deapesh Misra
#
alert tcp any $HTTP_PORTS -> $HOME_NET any (msg:"ET MALWARE Possible Windows executable sent when remote host claims to send HTML/CSS Content"; flow:established,to_client;
content:"Content-Type|3a| text/css|0d 0a|"; content:"|0d 0a|MZ"; within:500; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2009909;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Covert_Executable_DL; sid:2009909; rev:2;)

#by evilghost
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Executable purporting to be .txt file with no Referrer - Likely Malware"; flow:established,to_server; content:"GET
"; nocase; depth:4; content:!"|0d 0a|Referer|3a| "; nocase; uricontent:".txt"; nocase; pcre:"/\.txt$/Ui"; flowbits:set,ET.hidden.exe; flowbits:noalert; classtype:trojan-activity;
reference:url,www.symantec.com/security_response/writeup.jsp?docid=2009-072313-3630-99; reference:url,doc.emergingthreats.net/2010500; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Covert_Executable_DL; sid:2010500; rev:3;)

#by evilghost
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Executable purporting to be .cfg file with no Referrer - Likely Malware"; flow:established,to_server; content:"GET
"; nocase; depth:4; content:!"|0d 0a|Referer|3a| "; nocase; uricontent:".cfg"; nocase; pcre:"/\.cfg$/Ui"; flowbits:set,ET.hidden.exe; flowbits:noalert; classtype:trojan-activity;
reference:url,www.symantec.com/security_response/writeup.jsp?docid=2009-072313-3630-99; reference:url,doc.emergingthreats.net/2010501; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Covert_Executable_DL; sid:2010501; rev:3;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE CrazyWinnings.com Activity"; flow: established,to_server; uricontent:"/scripts/protect.php?promo=promo"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001733; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_CrazyWinnings.com;
sid:2001733; rev:5;)

#Submitted by Matt Jonkman
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Default-homepage-network.com Access"; flow: to_server,established; content:"wsh.RegWrite"; nocase;
content:"default-homepage-network.com/start.cgi?"; nocase; classtype: trojan-activity; reference:url,default-homepage-network.com/start.cgi?new-hkcu;
reference:url,doc.emergingthreats.net/bin/view/Main/2001222; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Default-Homepage-Network; sid:2001222; rev:8;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE DelFin Project Spyware (payload)"; flow: established,to_server; uricontent:"/in/payload/payload.nfo?"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002816; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Delfin;
sid:2002816; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE DelFin Project Spyware (setup)"; flow: established,to_server; uricontent:"/in/defaults/setup.nfo?"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002817; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Delfin;
sid:2002817; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE DelFin Project Spyware (setup-alt)"; flow: established,to_server; uricontent:"/in/defaults/setup-alt.nfo?"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003472; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Delfin;
sid:2003472; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE DelFin Project Spyware (payload-alt)"; flow: established,to_server; uricontent:"/in/payload/payload-alt.nfo?";
nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003473; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Delfin;
sid:2003473; rev:3;)

#submitted by John Stewart
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE DesktopTraffic Toolbar Spyware"; flow: to_server,established; uricontent:"cgi-bin/ezl_kws.fcgi?cat"; nocase;
classtype:trojan-activity; reference:url,research.spysweeper.com/threat_library/threat_details.php?threat=desktoptraffic.net_hijack;
reference:url,doc.emergingthreats.net/bin/view/Main/2001884; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_DeskTopTraffic; sid:2001884; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Deskwizz.com Spyware Install INI Download"; flow: to_server,established; uricontent:"/GetAd/tekID"; nocase;
uricontent:".ini"; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2003445; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Deskwizz.com; sid:2003445; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Deskwizz.com Spyware Install Code Download"; flow: to_server,established; uricontent:"/ax/acdt-pid"; nocase;
uricontent:".exe"; nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2003444; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Deskwizz.com; sid:2003444; rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Direct-web.co.kr Related Spyware Checkin"; flow:established,to_server; uricontent:".php?appname="; nocase;
uricontent:"&appseq="; nocase; uricontent:"&mac="; nocase; uricontent:"&type="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007978;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Direct-web.co.kr; sid:2007978; rev:2;)

#this is for the recent rash of .co.kr fake antispyware products we're seeing.
#doctorpro.co.kr, karine.co.kr, Vaccineprogram.co.kr, Mycashbank.co.kr, etc. There will surely be more. Similar url patterns though
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Doctorpro.co.kr Related Fake Anti-Spyware Install Checkin"; flow:established,to_server;
uricontent:"/install_count.html?id="; nocase; uricontent:"&MAC="; nocase; pcre:"/MAC=0\w-\w\w-\w\w-\w\w-\w\w-\w\w-\w\w/Ui"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2006425; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Doctorpro_and_Related; sid:2006425; rev:4;)

#this is for the recent rash of .co.kr fake antispyware products we're seeing.
#doctorpro.co.kr, karine.co.kr, Vaccineprogram.co.kr, Mycashbank.co.kr, etc. There will surely be more. Similar url patterns though
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Doctorpro.co.kr Related Fake Anti-Spyware Checkin"; flow:established,to_server; uricontent:"/access_count.html?
id="; nocase; uricontent:"&MAC="; nocase; pcre:"/MAC=0\w-\w\w-\w\w-\w\w-\w\w-\w\w/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2006426;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Doctorpro_and_Related; sid:2006426; rev:4;)

#this is for the recent rash of .co.kr fake antispyware products we're seeing.
#doctorpro.co.kr, karine.co.kr, Vaccineprogram.co.kr, Mycashbank.co.kr, etc. There will surely be more. Similar url patterns though
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Doctorpro.co.kr Related Fake Anti-Spyware Mac Check"; flow:established,to_server; content:"POST "; depth:5;
uricontent:"/ctrl/nchkmac.php?mac=0"; nocase; pcre:"/mac=0\w\:\w\w\:\w\w\:\w\w\:\w\w\:\w\w/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2006427;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Doctorpro_and_Related; sid:2006427; rev:4;)

#this is for the recent rash of .co.kr fake antispyware products we're seeing.
#doctorpro.co.kr, karine.co.kr, Vaccineprogram.co.kr, Mycashbank.co.kr, etc. There will surely be more. Similar url patterns though
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Doctorpro.co.kr Related Fake Anti-Spyware Checkin (open)"; flow:established,to_server; uricontent:"/open.php?sn=";
nocase; pcre:"/sn=0\w\:\w\w\:\w\w\:\w\w\:\w\w\:\w\w/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2006428;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Doctorpro_and_Related; sid:2006428; rev:4;)

#this is for the recent rash of .co.kr fake antispyware products we're seeing.
#doctorpro.co.kr, karine.co.kr, Vaccineprogram.co.kr, Mycashbank.co.kr, etc. There will surely be more. Similar url patterns though
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Doctorpro.co.kr Related Fake Anti-Spyware Post"; flow:established,to_server; content:"POST "; depth:5;
uricontent:"/ctrl/chkblack.php?mac=0"; nocase; pcre:"/mac=0\w\:\w\w\:\w\w\:\w\w\:\w\w\:\w\w/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2006431;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Doctorpro_and_Related; sid:2006431; rev:4;)

#this is for the recent rash of .co.kr fake antispyware products we're seeing.
#doctorpro.co.kr, karine.co.kr, Vaccineprogram.co.kr, Mycashbank.co.kr, etc. There will surely be more. Similar url patterns though
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Doctorpro.co.kr Related Fake Anti-Spyware Checkin (ret)"; flow:established,to_server; uricontent:"/ret.php?";
nocase; uricontent:"mode="; nocase; uricontent:"&cname="; nocase; uricontent:"&cn="; nocase; pcre:"/cn=0\w\:\w\w\:\w\w\:\w\w\:\w\w\:\w\w/Ui"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2006432; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Doctorpro_and_Related; sid:2006432; rev:4;)

#this is for the recent rash of .co.kr fake antispyware products we're seeing.
#doctorpro.co.kr, karine.co.kr, Vaccineprogram.co.kr, Mycashbank.co.kr, etc. There will surely be more. Similar url patterns though
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Doctorpro.co.kr Related Fake Anti-Spyware Post (api_result)"; flow:established,to_server; content:"POST "; depth:5;
uricontent:"/ctrl/api_result.php?"; nocase; uricontent:"mode="; nocase; uricontent:"&PartID="; nocase; uricontent:"&mac="; nocase; pcre:"/mac=0\w\:\w\w\:\w\w\:\w\w\:\w\w\:\w\w/Ui";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2006433; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Doctorpro_and_Related; sid:2006433; rev:4;)

#more from the same folks
#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Viruscheck.co.kr Related Fake Anti-Spyware Post (chkvs)"; flow:established,to_server; content:"POST "; depth:5;
uricontent:"/chkvs.php?mac=0"; nocase; pcre:"/mac=0\w\:\w\w\:\w\w\:\w\w\:\w\w\:\w\w/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007642;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Doctorpro_and_Related; sid:2007642; rev:4;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Dollarrevenue.com Spyware Code Download"; flow:established,to_server; uricontent:"/bundle/drsmartload.exe"; nocase;
classtype:trojan-activity; reference:url,dollarrevenue.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002967; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Dollarrevenue.net; sid:2002967; rev:3;)

#by Scot Melnick
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE TROJAN_VB Microjoin"; flow:established,to_server; uricontent:"/bundle/loader.exe"; nocase; classtype:trojan-
activity; reference:url,de.trendmicro-europe.com/consumer/vinfo/encyclopedia.php?VName=TROJ_VB.AWW; reference:url,doc.emergingthreats.net/bin/view/Main/2003084;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Dropper.Microjoin; sid:2003084; rev:3;)

#by Matt Jonkman, from Spyware Listening Post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Dropspam.com Spyware Reporting"; flow:established,to_server; uricontent:"/reportaddon.cgi?"; nocase;
uricontent:"report.cgi?"; nocase; uricontent:"user="; nocase; uricontent:"software="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003440;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Dropspam.com; sid:2003440; rev:3;)

#matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE E2give Related Downloading IeBHOs.dll"; flow: to_server,established; uricontent:"/downloads/IeBHOs.dll"; nocase;
classtype:trojan-activity; reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=E2Give&threatid=4728; reference:url,doc.emergingthreats.net/bin/view/Main/2001415;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_E2give.com; sid:2001415; rev:7;)

#matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE E2give Related Reporting Install"; flow: to_server,established; uricontent:"/count/count.php?&mm"; nocase;
classtype:trojan-activity; reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=E2Give&threatid=4728; reference:url,doc.emergingthreats.net/bin/view/Main/2001416;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_E2give.com; sid:2001416; rev:7;)

#matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE E2give Related Receiving Config"; flow: to_server,established; uricontent:"/config/?"; nocase; uricontent: "v=5";
nocase; uricontent: "n=mm2"; nocase; uricontent: "i="; nocase; classtype:trojan-activity; reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=E2Give&threatid=4728;
reference:url,doc.emergingthreats.net/bin/view/Main/2001417; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_E2give.com; sid:2001417; rev:8;)

#matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE E2give Related Downloading Code"; flow: to_server,established; uricontent:"/soft/unstall.exe"; nocase;
classtype:trojan-activity; reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=E2Give&threatid=4728; reference:url,doc.emergingthreats.net/bin/view/Main/2001418;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_E2give.com; sid:2001418; rev:7;)

#matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE E2give Related Reporting"; flow: to_server,established; uricontent:"/count/count.php?&mm2cpr"; nocase;
classtype:trojan-activity; reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=E2Give&threatid=4728; reference:url,doc.emergingthreats.net/bin/view/Main/2001423;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_E2give.com; sid:2001423; rev:7;)

#from spyware listening post hits
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE E2give Spyware Reporting (check url)"; flow: to_server,established; uricontent:"/go/check?build="; nocase;
uricontent:"&source="; nocase; uricontent:"&merchants="; nocase; classtype: trojan-activity; reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=E2Give&threatid=4728;
reference:url,doc.emergingthreats.net/bin/view/Main/2003504; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_E2give.com; sid:2003504; rev:3;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE ESyndicate Spyware Install (esyndicateinst.exe)"; flow: to_server,established;
uricontent:"/files/eSyndicateInst.exe"; nocase; classtype: trojan-activity; reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=453094058;
reference:url,doc.emergingthreats.net/bin/view/Main/2002009; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_ESyndicate; sid:2002009; rev:6;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE ESyndicate Spyware Install (sepinst.exe)"; flow: to_server,established; uricontent:"/files/SEPInst.exe"; nocase;
classtype: trojan-activity; reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=453094058; reference:url,doc.emergingthreats.net/bin/view/Main/2002010;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_ESyndicate; sid:2002010; rev:6;)

#By Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE EZSearch Spyware Reporting Search Strings"; flow:established,to_server; uricontent:"/partner/rt.php?q="; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002317; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_EZSearch;
sid:2002317; rev:3;)

#By Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE EZSearch Spyware Reporting Search Category"; flow:established,to_server; uricontent:"/partner/rt.php?cat="; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002318; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_EZSearch;
sid:2002318; rev:3;)

#By Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE EZSearch Spyware Reporting 2"; flow:established,to_server; uricontent:"/partner/bom.php?e="; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002319; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_EZSearch;
sid:2002319; rev:3;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Ebates Install"; flow: to_server,established; uricontent:"/ebates.exe"; classtype: policy-violation;
reference:url,www.pestpatrol.com/PestInfo/e/ebates_moneymaker.asp; reference:url,doc.emergingthreats.net/bin/view/Main/2001038; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Ebates_Moe_Money_Maker; sid:2001038; rev:7;)

#from spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Effectivebrands.com Spyware Checkin"; flow:established,to_server; uricontent:"/iis2ebs.asp"; nocase;
content:"effectivebrands.com"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003304; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Effectivebrands.com; sid:2003304; rev:3;)

#from spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Effectivebrands.com Spyware Checkin 2"; flow:established,to_server; uricontent:"/iis2ucms.asp"; nocase;
content:"effectivebrands.com"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003360; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Effectivebrands.com; sid:2003360; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Elitemediagroup.net Spyware Config Download"; flow:established,to_server; uricontent:"/bundle.php?aff="; nocase;
classtype:trojan-activity; reference:url,elitemediagroup.net; reference:url,doc.emergingthreats.net/bin/view/Main/2002966; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Elitemediagroup.net; sid:2002966; rev:3;)

#By Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Epilot.com Spyware Reporting"; flow:established,to_server; uricontent:"/getresults.aspx"; nocase; uricontent:"?
aff="; nocase; uricontent:"&ip="; nocase; uricontent:"&keyword="; nocase; uricontent:"&source="; nocase; classtype:trojan-activity;
reference:url,www.intermute.com/spysubtract/researchcenter/ClientMan.html; reference:url,doc.emergingthreats.net/bin/view/Main/2003414; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Epilot.com; sid:2003414; rev:3;)

#By Matt Jonkman, From spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Epilot.com Spyware Reporting Clicks"; flow:established,to_server; uricontent:"/click.aspx?"; nocase; uricontent:"?
xp="; nocase; content:"Host\: "; nocase; content:"epilot.com"; nocase; distance:0; classtype:trojan-activity; reference:url,www.intermute.com/spysubtract/researchcenter/ClientMan.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2003416; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Epilot.com; sid:2003416; rev:3;)

#matt Jonkman from Spyware LP Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Evidencenuker.com Fake AV Updating"; flow:established,to_server; uricontent:"/products/evidencenuker/update.php?
version="; nocase; classtype:trojan-activity; reference:url,www.evidencenuker.com; reference:url,doc.emergingthreats.net/bin/view/Main/2003568;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_EvidenceNuker.com; sid:2003568; rev:3;)
```

```
#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE F1Organizer Install Attempt"; flow: to_server,established; uricontent:"/f1/objects/"; nocase; classtype: trojan-
activity; reference:url,doc.emergingthreats.net/bin/view/Main/2000585; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_F1Organizer.com; sid:2000585;
rev:7;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE F1Organizer Reporting"; flow: to_server,established; uricontent:"/f1/audit/"; nocase; classtype: trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2000582; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_F1Organizer.com; sid:2000582; rev:7;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE F1Organizer Config Download"; flow: to_server,established; uricontent:"/F1/Cmd4F1"; nocase; classtype: trojan-
activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001221; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_F1Organizer.com; sid:2001221;
rev:6;)

#Submitted by Matt Jonkman
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Featured-Results.com Agent Reporting Data"; flow: to_server,established; uricontent:"action=any"; nocase;
uricontent:"country="; nocase; pcre:"/(POST |POST (http|https)\:\/\/[-0-9a-z.]*)\/.*perl\/fr\.pl/i"; classtype: trojan-activity; reference:url,www.featured-results.com;
reference:url,doc.emergingthreats.net/bin/view/Main/2001293; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Featured-results; sid:2001293; rev:10;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Findwhat.com Spyware (clickthrough)"; flow: to_server,established; uricontent:"/bin/findwhat.dll?clickthrough&";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003579; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Findwhat.com; sid:2003579; rev:3;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Findwhat.com Spyware (sendtracker)"; flow: to_server,established; uricontent:"/bin/findwhat.dll?sendtracker&";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003580; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Findwhat.com; sid:2003580; rev:3;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Findwhat.com Spyware (sendmedia)"; flow: to_server,established; uricontent:"/bin/findwhat.dll?sendmedia&"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003581; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Findwhat.com;
sid:2003581; rev:3;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE FlashPoint Agent Retrieving New Code"; flow: to_server,established; uricontent:"/ftxmon.php?"; classtype: trojan-
activity; reference:url,www.flashpoint.bm; reference:url,doc.emergingthreats.net/bin/view/Main/2000905; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_FlashPoint; sid:2000905; rev:7;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE FlashTrack Agent Retrieving New App Code"; flow: to_server,established; uricontent:"/apps/r.exe"; classtype:
trojan-activity; reference:url,www.flashpoint.bm; reference:url,doc.emergingthreats.net/bin/view/Main/2000936; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_FlashPoint; sid:2000936; rev:7;)

#matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Flingstone Spyware Install (cxtpls)"; flow: established,to_server; uricontent:"/softwares/cxtpls_loader_ff.exe";
nocase; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.winfavorites.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001710;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Flingstone; sid:2001710; rev:8;)

#matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Flingstone Spyware Install (sportsinteraction)"; flow: established,to_server;
uricontent:"/softwares/SportsInteraction.exe"; nocase; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.winfavorites.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001705; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Flingstone; sid:2001705; rev:8;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Freeze.com Spyware/Adware (Install)"; flow: to_server,established; uricontent:"/checkhttp.htm"; nocase;
content:"User-Agent|3a| Wise"; nocase; content:"freeze.com"; nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002840;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Freeze.com; sid:2002840; rev:4;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Freeze.com Spyware/Adware (Install Registration)"; flow: to_server,established; uricontent:"/ping/?shortname=";
nocase; content:"User-Agent|3a| Wise"; nocase; content:"freeze.com"; nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002841;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Freeze.com; sid:2002841; rev:4;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Freeze.com Spyware/Adware (Pulling Ads)"; flow: to_server,established; uricontent:"/ToastMessage/"; nocase;
uricontent:"/Toast.asp?ysaid="; nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2003362; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Freeze.com; sid:2003362; rev:3;)

#by: Jeremy Conway at sudosecure.net
#ref: f6a78be315d98ba8df4e72296ac8ec0c
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE W3i Related Adware/Spyware"; flow:established,to_server; content:"GET "; nocase; depth:4; uricontent:"shortname=";
nocase; uricontent:"os="; nocase; uricontent:"v="; nocase; uricontent:"browsers="; nocase; uricontent:"readable="; nocase; classtype:trojan-activity;
reference:url,www.tallemu.com/oasis2/vendor/w3i__llc/623302; reference:url,doc.emergingthreats.net/2009705; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Freeze.com; sid:2009705; rev:3;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Fun Web Products Install"; flow: to_server,established; uricontent:"/install_ie.jsp?product="; classtype: policy-
violation; reference:url,www.funwebproducts.com; reference:url,doc.emergingthreats.net/bin/view/Main/2000599; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Fun_Web_Products; sid:2000599; rev:6;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Fun Web Products SmileyCentral"; flow: to_server,established; uricontent:"/images/smileycentral/"; nocase;
content:"FunWebProducts"; nocase; classtype: policy-violation; reference:url,www.funwebproducts.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001013;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Fun_Web_Products; sid:2001013; rev:7;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Fun Web Products Agent Traffic"; flow: to_server,established; content:"FunWebProducts|3b|"; nocase; threshold: type
limit, track by_src, count 2, seconds 360; classtype: policy-violation; reference:url,www.funwebproducts.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001034;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Fun_Web_Products; sid:2001034; rev:17;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Fun Web Products MyWay Agent Traffic"; flow: to_server,established; content:"FunWebProducts-MyWay|3b|"; nocase;
threshold: type limit, track by_src, count 10, seconds 60; classtype: policy-violation; reference:url,www.funwebproducts.com;
reference:url,doc.emergingthreats.net/bin/view/Main/2001043; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Fun_Web_Products; sid:2001043; rev:11;)

#From Listening Post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Fun Web Products Smileychooser Spyware"; flow: to_server,established; uricontent:"/SmileyChooser.html?"; nocase;
uricontent:"v="; nocase; classtype: policy-violation; reference:url,www.funwebproducts.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002305;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Fun_Web_Products; sid:2002305; rev:6;)
```

```
#From Listening Post data
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Fun Web Products Smileychooser Spyware"; flow: to_server,established; uricontent:"/SmileyChooser.html?"; nocase;
uricontent:"v="; nocase; classtype:policy-violation; reference:url,www.funwebproducts.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002310;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Fun_Web_Products; sid:2002310; rev:6;)

#From Listening Post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Fun Web Products Cursorchooser Spyware"; flow: to_server,established; uricontent:"/CursorChooser.html?"; nocase;
classtype: policy-violation; reference:url,www.funwebproducts.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002306; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Fun_Web_Products; sid:2002306; rev:4;)

#From Listening Post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Fun Web Products Stampchooser Spyware"; flow: to_server,established; uricontent:"/StampChooser.html?"; nocase;
uricontent: "v="; nocase; classtype: policy-violation; reference:url,www.funwebproducts.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002307;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Fun_Web_Products; sid:2002307; rev:5;)

#by Shirkdog
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Fun Web Products StationaryChooser Spyware"; flow: to_server,established; uricontent:"/StationeryChooser.html?";
nocase; uricontent: "v="; nocase; classtype: policy-violation; reference:url,www.funwebproducts.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002858;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Fun_Web_Products; sid:2002858; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Fun Web Products SmileyCentral IEsp2 Install"; flow: to_server,established;
uricontent:"/download/install_ie_sp2.jhtml?"; nocase; uricontent:"product="; nocase; uricontent:"utmCall="; nocase; uricontent:"bOrganic="; nocase; classtype:trojan-activity;
reference:url,www.myfuncards.com; reference:url,doc.emergingthreats.net/bin/view/Main/2003151; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Fun_Web_Products; sid:2003151; rev:3;)

#Matt Jonkman from Spyware LP Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Gamehouse.com Activity"; flow: to_server,established; uricontent:"/game-quit-count.jsp?ghgamecode="; classtype:
trojan-activity; reference:url,www.gamehouse.com; reference:url,doc.emergingthreats.net/bin/view/Main/2003348; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Gamehouse.com; sid:2003348; rev:3;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Gator Cookie"; flow: to_server,established; content:"webpdpcookie"; content:".gator.com"; nocase; classtype:
policy-violation; reference:url,www3.ca.com/securityadvisor/pest/content.aspx?q=67999; reference:url,doc.emergingthreats.net/bin/view/Main/2000025;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Gator_Agent; sid:2000025; rev:9;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Gator Checkin"; flow: to_server,established; uricontent:"/gbsf/"; nocase; classtype: policy-violation;
reference:url,www3.ca.com/securityadvisor/pest/content.aspx?q=67999; reference:url,doc.emergingthreats.net/bin/view/Main/2000595; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Gator_Agent; sid:2000595; rev:8;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Gator New Code Download"; flow: to_server,established; uricontent:"/gatorcme/"; nocase; classtype: policy-
violation; reference:url,www3.ca.com/securityadvisor/pest/content.aspx?q=67999; reference:url,doc.emergingthreats.net/bin/view/Main/2000597; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Gator_Agent; sid:2000597; rev:7;)

#Matt Jonkman (depth added by bobkberg)
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Gator/Claria Data Submission"; flow: to_server,established; content:"POST "; depth:5; uricontent:"gs_trickler";
nocase; classtype: policy-violation; reference:url,www3.ca.com/securityadvisor/pest/content.aspx?q=67999; reference:url,doc.emergingthreats.net/bin/view/Main/2000596;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Gator_Agent; sid:2000596; rev:12;)

#Matt Jonkman (depth added by bobkberg)
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Gator/Clarian Agent"; flow: to_server,established; uricontent:"/gbsf/"; nocase; uricontent:"gtrg2ze"; nocase;
classtype:policy-violation; reference:url,www3.ca.com/securityadvisor/pest/content.aspx?q=67999; reference:url,doc.emergingthreats.net/bin/view/Main/2001306;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Gator_Agent; sid:2001306; rev:9;)

#Matt Jonkman, from spyware LP Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Gator/Clarian Spyware Posting Data"; flow: to_server,established; uricontent:"/gs_med"; nocase; classtype:trojan-
activity; reference:url,www3.ca.com/securityadvisor/pest/content.aspx?q=67999; reference:url,doc.emergingthreats.net/bin/view/Main/2003575; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Gator_Agent; sid:2003575; rev:4;)

#These are for common names of malcode files as seen in common places.
#Matt Jonkman
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Likely Trojan/Spyware Installer Requested (1)"; flow: established,to_server; uricontent:".scr"; nocase;
pcre:"/(cartao|mensagem|voxcards|humortadela|ouca|cartaovirtual|uol3171|embratel|yahoo|viewforhumor|humormenssagem|terra)\.scr/Ui"; classtype: trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2001850; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_General_Requests; sid:2001850; rev:9;)

#These are for common names of malcode files as seen in common places.
#Matt Jonkman
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Likely Trojan/Spyware Installer Requested (2)"; flow: established,to_server; uricontent:".exe"; nocase;
pcre:"/(discador|ocartao|msgav|extrato|correcao|extrato_tim|visualizar|cartas&cartoes|embratel|cartao|MSN_INSTALL|VirtualCards|atualizacaonorton|serasar|CobrancaEmbratel|ExtratoTim|Flas
hFotos|Vacina-Norton|CartaoIloves|Cobranca|fotos_ineditas|boletocobranca|saudades|wwwuolcartoescombr|cartaoanimado)\.exe/Ui"; classtype: trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2002093; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_General_Requests; sid:2002093; rev:6;)

#Submitted by Joseph Gama
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET MALWARE IE homepage hijacking"; flow: from_server,established; content:"wsh.RegWrite"; nocase;
content:"HKLM\\\\Software\\\\Microsoft\\\\Internet Explorer\\\\Main\\\\Start Page"; nocase; classtype: misc-attack;
reference:url,www.geek.com/news/geeknews/2004Jun/gee20040610025522.htm; reference:url,doc.emergingthreats.net/bin/view/Main/2000514; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_General_Spyware_Install; sid:2000514; rev:7;)

#Submitted by Joseph Gama
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET MALWARE shell browser vulnerability W9x/XP"; flow: from_server,established; content:"shell|3a|windows"; nocase; classtype:
misc-attack; reference:url,www.packetfocus.com/shell_exploit.htm; reference:url,doc.emergingthreats.net/bin/view/Main/2000519; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_General_Spyware_Install; sid:2000519; rev:9;)

#Submitted by Joseph Gama
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET MALWARE shell browser vulnerability NT/2K"; flow: from_server,established; content:"shell|3a|winnt"; nocase; classtype:
misc-attack; reference:url,www.packetfocus.com/shell_exploit.htm; reference:url,doc.emergingthreats.net/bin/view/Main/2000520; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_General_Spyware_Install; sid:2000520; rev:9;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE GlobalPhon.com Dialer"; flow: to_server,established; content:"Host|3a| www.globalphon.com"; classtype: trojan-
activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001656; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_GlobalPhon; sid:2001656; rev:5;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE GlobalPhon.com Dialer Download"; flow: to_server,established; uricontent:"/dialer/internazionale_ver"; nocase;
uricontent:".CAB"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001657; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_GlobalPhon; sid:2001657; rev:4;)
```

```
#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE GlobalPhon.com Dialer (no_pop)"; flow: to_server,established; uricontent:"/no_pop.asp?"; nocase; uricontent: "id=";
nocase; content:"globalphon.com"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001659; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_GlobalPhon; sid:2001659; rev:6;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE GlobalPhon.com Dialer (add_ocx)"; flow: to_server,established; uricontent:"/add_ocx.asp?"; nocase; uricontent:
"id="; nocase; content:"globalphon.com"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001660; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_GlobalPhon; sid:2001660; rev:6;)

#by Jeremy at sudosecure
#ref: 9ab0b5608af7c2c7fb3b631f27ee79c6
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Gooochi Related Spyware Ad pull"; flow:established,to_server; content:"GET "; depth:4; uricontent:"?z="; nocase;
uricontent:"|26|ch="; nocase; uricontent:"|26|dim="; nocase; uricontent:"|26|abr="; nocase; content:!"Referer|3a| "; nocase; classtype:trojan-activity;
reference:url,www.threatexpert.com/reports.aspx?find=ads.gooochi.biz; reference:url,doc.emergingthreats.net/bin/view/Main/2008375; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Gooochi; sid:2008375; rev:4;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE GrandstreetInteractive.com Install"; flow: to_server,established; uricontent:"/tdtb.exe"; nocase; classtype:
trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002012; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_GrandStreetInteractive.com;
sid:2002012; rev:4;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE GrandstreetInteractive.com Update"; flow: to_server,established; uricontent:"/wupdsnff.exe"; nocase; classtype:
trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002013; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_GrandStreetInteractive.com;
sid:2002013; rev:4;)

#by Matt jonkman, guard-center.com crapware (if you're gonna pretend to scan a disk, you ought to at least access the disk a little)
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Guard-Center.com Fake AntiVirus Post-Install Checkin"; flow:established,to_server; uricontent:".php?";
uricontent:"&advid="; uricontent:"&u="; uricontent:"&p="; content:"HTTP/1."; content:!"|0d 0a|User-Agent|3a|"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2007744; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Guard-Center.com; sid:2007744; rev:5;)

#by matt jonkman
#many malware packages use hex to obscure an IP
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Hex Encoded IP HTTP Request - Likely Malware"; flow:established,to_server; content:"|0d 0a|Host|3a| 0x";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007951; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Hex_Domain_Request;
sid:2007951; rev:3;)

#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE host-domain-lookup.com spyware related Checkin"; flow:established,to_server; uricontent:"?udata=";
uricontent:"mission_supgrade|3a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007749; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Host-domain-lookup.com; sid:2007749; rev:4;)

#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE host-domain-lookup.com spyware related Start Report"; flow:established,to_server; uricontent:"?udata=";
uricontent:"program_started|3a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007750; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Host-domain-lookup.com; sid:2007750; rev:4;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Hotbar Install (1)"; flow: to_server,established; uricontent:"/install/startInstallprocess.asp?"; nocase;
uricontent: "Defau"; classtype: trojan-activity; reference:url,www.hotbar.com; reference:url,doc.emergingthreats.net/bin/view/Main/2000920; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Hotbar; sid:2000920; rev:9;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Hotbar Install (2)"; flow: to_server,established; uricontent:"/install/process/upsale/hotbar"; classtype: trojan-
activity; reference:url,www.hotbar.com; reference:url,doc.emergingthreats.net/bin/view/Main/2000921; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Hotbar; sid:2000921; rev:8;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Hotbar Install (3)"; flow: to_server,established; uricontent:"/installs/hotbar/programs/"; classtype: trojan-
activity; reference:url,www.hotbar.com; reference:url,doc.emergingthreats.net/bin/view/Main/2000922; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Hotbar; sid:2000922; rev:8;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Hotbar Agent Reporting Information"; flow: to_server,established; content:"POST "; depth:5; nocase;
uricontent:"/reports/hotbar/"; classtype: trojan-activity; reference:url,www.hotbar.com; reference:url,doc.emergingthreats.net/bin/view/Main/2000923;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Hotbar; sid:2000923; rev:8;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Hotbar Agent Upgrading"; flow: to_server,established; uricontent:"/updates/hotbar/"; nocase; classtype: trojan-
activity; reference:url,www.hotbar.com; reference:url,doc.emergingthreats.net/bin/view/Main/2000924; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Hotbar; sid:2000924; rev:8;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Hotbar Agent Activity"; flow: to_server,established; uricontent:"/dynamic/hotbar/"; nocase; threshold: type limit,
count 1, track by_src, seconds 360; classtype: trojan-activity; reference:url,www.hotbar.com; reference:url,doc.emergingthreats.net/bin/view/Main/2000929;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Hotbar; sid:2000929; rev:8;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Hotbar Agent Partner Checkin"; flow: to_server,established; uricontent:"/partners/"; nocase;
uricontent:"partners.xip"; nocase; classtype: trojan-activity; reference:url,www.hotbar.com; reference:url,doc.emergingthreats.net/bin/view/Main/2000925;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Hotbar; sid:2000925; rev:7;)

#from Shirkdog
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Hotbar Agent Subscription POST"; flow: to_server,established; uricontent:"/hotbar/"; nocase;
uricontent:"Subscription.dll?"; nocase; classtype: trojan-activity; reference:url,www.hotbar.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002820;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Hotbar; sid:2002820; rev:3;)

#Matt Jonkman from spyware lp data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Hotbar Agent Adopt/Zango"; flow: to_server,established; uricontent:"/adopt.jsp?"; nocase; uricontent:"l="; nocase;
uricontent:"&sz="; nocase; uricontent:"cid="; nocase; classtype: trojan-activity; reference:url,www.hotbar.com; reference:url,doc.emergingthreats.net/bin/view/Main/2003364;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Hotbar; sid:2003364; rev:3;)

#Matt Jonkman from spyware lp data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Hotbar Keywords Download"; flow: to_server,established; uricontent:"/keywords/kyfb."; nocase;
uricontent:"partner_id="; nocase; classtype: trojan-activity; reference:url,www.hotbar.com; reference:url,doc.emergingthreats.net/bin/view/Main/2003388;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Hotbar; sid:2003388; rev:3;)
```

```
#matt jonkman, new version of hotbar apparently
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Hotbar.com Related Spyware Install Report"; flow:established,to_server; uricontent:"/ciconfig.aspx?did=";
uricontent:"&brandid="; uricontent:"&os="; uricontent:"&pkg_ver="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008917;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Hotbar; sid:2008917; rev:2;)

#matt jonkman, new version of hotbar apparently
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Hotbar.com Related Spyware Activity Report"; flow:established,to_server; uricontent:"/trackedevent.aspx?eid=";
uricontent:"&brand="; uricontent:"&os="; uricontent:"&mt="; uricontent:"&pkg_ver="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008918;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Hotbar; sid:2008918; rev:2;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE ICQ-Update.biz Reporting Install"; flow: to_server,established; uricontent:"log.php?"; nocase; uricontent: "IP=";
nocase; uricontent:"Port1="; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001490; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_ICQ-Update.biz; sid:2001490; rev:8;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE IEHelp.net Spyware Installer"; flow:established,to_server; uricontent:"/counter/help.chm"; nocase;
classtype:trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/trojan.domcom.html; reference:url,doc.emergingthreats.net/bin/view/Main/2002090;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_IEHelp.net; sid:2002090; rev:5;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE IEHelp.net Spyware checkin"; flow:established,to_server; uricontent:"/l/gpr.php?"; nocase; uricontent: "ID1=";
nocase; classtype:trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/trojan.domcom.html; reference:url,doc.emergingthreats.net/bin/view/Main/2002096;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_IEHelp.net; sid:2002096; rev:6;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE ISearchTech.com XXXPornToolbar Reporting"; flow: to_server,established;
uricontent:"/ist/scripts/log_downloads.php"; nocase; classtype: trojan-activity; reference:url,www.isearchtech.com; reference:url,doc.emergingthreats.net/bin/view/Main/2000927;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_ISearchTech.com; sid:2000927; rev:7;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE ISearchTech.com XXXPornToolbar Activity (1)"; flow: to_server,established; uricontent:"/ist/bars/"; nocase;
classtype: trojan-activity; reference:url,www.isearchtech.com; reference:url,doc.emergingthreats.net/bin/view/Main/2000928; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_ISearchTech.com; sid:2000928; rev:8;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE ISearchTech.com XXXPornToolbar Activity (2)"; flow: to_server,established; uricontent:"/ist/softwares/"; nocase;
classtype: trojan-activity; reference:url,www.isearchtech.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001395; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_ISearchTech.com; sid:2001395; rev:8;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE ISearchTech.com XXXPornToolbar Data Submission"; flow: to_server,established;
uricontent:"/ist/scripts/istsvc_ads_data.php?"; nocase; uricontent: "version="; nocase; classtype: trojan-activity; reference:url,www.isearchtech.com;
reference:url,doc.emergingthreats.net/bin/view/Main/2001697; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_ISearchTech.com; sid:2001697; rev:6;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Incredisearch.com Spyware Ping"; flow: established,to_server; uricontent:"/ping.asp"; nocase;
content:"incredisearch.com"; depth:300; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001793; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Incredisearch.com; sid:2001793; rev:6;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Incredisearch.com Spyware Activity"; flow: established,to_server; content:"Host|3a| www.incredisearch.com";
depth:300; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001794; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Incredisearch.com; sid:2001794; rev:7;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Instafinder.com spyware"; flow: established,to_server; uricontent:"/404/update/instafi"; nocase; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003376; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Instafinder.com; sid:2003376;
rev:3;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Internet Fuel.com Install"; flow: to_server,established; uricontent:"/cgi-bin/omnidirect.cgi?&debug_log="; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002015; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Internet_Fuel;
sid:2002015; rev:4;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Internet Optomizer Reporting Data"; flow: to_server,established; uricontent:"/io/downloads/"; nocase;
content:"/ws18/optimize"; nocase; classtype: policy-violation; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.netoptimizer.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001308; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Internet_Optimizer; sid:2001308; rev:7;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Internet Optimizer Spyware Install"; flow: to_server,established; uricontent:"/internet-optimizer/"; nocase;
uricontent:"/optimize"; nocase; classtype: policy-violation; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.netoptimizer.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001396; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Internet_Optimizer; sid:2001396; rev:6;)

#by: Jeremy Conway at sudosecure.net
#ref: b5880918affcbb25120b431a45b99429
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET MALWARE Adware Istbar Search Hijacker and Downloader"; flow:established,to_client; content:" 200 OK|0d 0a|"; nocase;
depth:64; content:"|0d 0a|Content-Type|3a| qvod_update|0d 0a|"; nocase; content:"|0d 0a 0d 0a 5b|AGENTLIST|5d 0d 0a|ip0="; nocase; content:"|0d 0a|port0="; nocase; within:25;
content:"|0d 0a 0d 0a|ip1="; nocase; content:"|0d 0a|port1="; nocase; within:25; classtype:trojan-activity; reference:url,www.pctools.com/mrc/infections/id/Trojan.ISTbar/;
reference:url,www.threatexpert.com/reports.aspx?find=Trojan.ISTbar; reference:url,doc.emergingthreats.net/2009597; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Istbar; sid:2009597; rev:2;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE jmnad1.com Spyware Install (1)"; flow: to_server,established; uricontent:"/install.qg?"; nocase; uricontent: "ID=";
nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002019; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Jmnad1.com; sid:2002019; rev:9;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE jmnad1.com Spyware Install (2)"; flow: to_server,established; uricontent:"/download/mw_4s_stub.exe"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002016; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Jmnad1.com;
sid:2002016; rev:8;)

#Submitted by Matt Jonkman
#
#alert udp $HOME_NET 3531 -> $EXTERNAL_NET 3531 (msg:"ET MALWARE JoltID Agent Probing or Announcing UDP"; classtype: trojan-activity; reference:url,www.joltid.com;
reference:url,forum.treweeke.com/lofiversion/index.php/t597.html; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.p2pnetworking.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2000900; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_JoltID; sid:2000900; rev:8;)

#Submitted by Matt Jonkman
#
```

```
#alert tcp $HOME_NET any -> $EXTERNAL_NET 3531 (msg:"ET MALWARE JoltID Agent Communicating TCP"; flow: to_server,established; classtype: trojan-activity; reference:url,www.joltid.com;
reference:url,forum.treweeke.com/lofiversion/index.php/t597.html; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.p2pnetworking.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2000901; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_JoltID; sid:2000901; rev:9;)

#Submitted by Matt Jonkman
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 3531 (msg:"ET MALWARE JoltID Agent Keep-Alive"; flow: to_server,established; dsize: 1; content:"|4b|"; classtype: trojan-activity;
reference:url,www.joltid.com; reference:url,forum.treweeke.com/lofiversion/index.php/t597.html; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.p2pnetworking.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001015; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_JoltID; sid:2001015; rev:9;)

#Submitted by Matt Jonkman
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE JoltID Agent P2P via Proxy Server"; flow: to_server,established; content:"POST http|3a|//"; nocase;
content:"|3a|3531/.pkt"; nocase; within: 20; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.p2pnetworking.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001679; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_JoltID; sid:2001679; rev:13;)

#Submitted by Matt Jonkman
#
#alert tcp $HOME_NET any <> $EXTERNAL_NET 3531 (msg:"ET MALWARE JoltID Agent Requesting File"; flow: established,to_server; content:"GIVE "; content:"User-Agent|3a|"; nocase;
content:"PeerEnabler"; within:120; classtype: trojan-activity; reference:url,www.joltid.com; reference:url,forum.treweeke.com/lofiversion/index.php/t597.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001654; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_JoltID; sid:2001654; rev:11;)

#by Jamie Blasco
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Possible Malicious Applet Access (justexploit kit)"; flow:to_server,established; uricontent:"/sdfg.jar"; classtype:
trojan-activity; reference:url,www.malwaredomainlist.com/forums/index.php?topic=3570.0; reference:url,doc.emergingthreats.net/2010438; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Justexploit; sid:2010438; rev:3;)

#Submitted by Jason Haar
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Keenvalue Update Engine"; flow: to_server,established; content:"|0d0a|Host|3a|secure.keenvalue.com";
content:"|0d0a|Extension|3a|Remote-Passphrase"; within: 300; classtype: trojan-activity; reference:url,www.safer-networking.org/index.php?page=updatehistory&detail=2003-11-24;
reference:url,doc.emergingthreats.net/bin/view/Main/2000932; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Keenvalue; sid:2000932; rev:6;)

#Matt Jonkman
#all sorts of junk at www.thespyguard.com, fake antispyware trojan
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Thespyguard.com Spyware Install"; flow:established,to_server; uricontent:"/soft/installers/spyguardf.php"; nocase;
classtype:trojan-activity; reference:url,www.thespyguard.com; reference:url,www.kliksoftware.com; reference:url,doc.emergingthreats.net/bin/view/Main/2003201;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Kliksoftware; sid:2003201; rev:3;)

#Matt Jonkman
#all sorts of junk at www.thespyguard.com, fake antispyware trojan
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Thespyguard.com Spyware Update Check"; flow:established,to_server; uricontent:"/soft/update/check_update.php";
nocase; content:"Host|3a| www.kliksoftware.com"; nocase; classtype:trojan-activity; reference:url,www.kliksoftware.com; reference:url,www.thespyguard.com;
reference:url,doc.emergingthreats.net/bin/view/Main/2003202; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Kliksoftware; sid:2003202; rev:4;)

#Matt Jonkman
#all sorts of junk at www.thespyguard.com, fake antispyware trojan
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Hitvirus Fake AV Install"; flow:established,to_server; uricontent:"/soft/installers/hitvirusf.php"; nocase;
content:"get.hitvirus.com"; nocase; classtype:trojan-activity; reference:url,www.kliksoftware.com; reference:url,doc.emergingthreats.net/bin/view/Main/2003203;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Kliksoftware; sid:2003203; rev:3;)

#Matt Jonkman
#all sorts of junk at www.thespyguard.com, fake antispyware trojan
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Thespyguard.com Spyware Updating"; flow:established,to_server; uricontent:"/soft/update/get.php"; nocase;
uricontent:"pid="; nocase; uricontent:"mail="; nocase; content:"Host|3a| www.kliksoftware.com"; nocase; classtype:trojan-activity; reference:url,www.kliksoftware.com;
reference:url,www.thespyguard.com; reference:url,doc.emergingthreats.net/bin/view/Main/2003204; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Kliksoftware; sid:2003204; rev:4;)

#from spyware listeningpost data, by matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE KMIP.net Spyware"; flow:established,to_server; uricontent:"/iesocks?peer_id="; nocase; uricontent:"ver="; nocase;
classtype:trojan-activity; reference:url,www.kmip.net; reference:url,doc.emergingthreats.net/bin/view/Main/2003298; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Kmip.net; sid:2003298; rev:3;)

#from spyware listeningpost data, by matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE KMIP.net Spyware 2"; flow:established,to_server; uricontent:"/sp?c=N&i="; nocase; uricontent:"&v="; nocase;
classtype:trojan-activity; reference:url,www.kmip.net; reference:url,doc.emergingthreats.net/bin/view/Main/2003526; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Kmip.net; sid:2003526; rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Kwsearchguide.com Related Spyware Checkin"; flow:established,to_server; uricontent:"/statics.php?maddr="; nocase;
uricontent:"&ipaddr="; nocase; uricontent:"&ovt="; nocase; uricontent:"&verno="; nocase; uricontent:"&action="; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2008067; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Kwsearchguide.com; sid:2008067; rev:2;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Kwsearchguide.com Related Spyware Keepalive"; flow:established,to_server; uricontent:"/alive.php?ovt=new_link";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008069; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Kwsearchguide.com; sid:2008069; rev:2;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE LocalNRD Spyware Checkin"; flow: to_server,established; uricontent:"/a/Drk.syn?"; nocase; uricontent: "adcontext";
nocase; classtype: trojan-activity; reference:url,www.localnrd.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001340; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Localnrd; sid:2001340; rev:9;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Look2me Spyware Activity (1)"; flow: to_server,established; content:"Referer|3a| Look2Me"; nocase; classtype:
trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.look2me.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001499;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Look2me; sid:2001499; rev:8;)

#by Pedro Marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Adware.Look2Me Activity"; flow:established,to_server; uricontent:"?B="; uricontent:"&V="; uricontent:"&M=";
uricontent:"&R="; uricontent:"&ID={"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008474; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Look2me; sid:2008474; rev:2;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE MSUpdater.net Spyware Checkin"; flow:established,to_server; uricontent:"/popsetarray.php?&country="; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002094; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_MSUpdater.net;
sid:2002094; rev:4;)

#by Matt Jonkman, from sunbelt blog
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Malwarealarm.com Fake AV/AntiSpyware Updating"; flow:established,to_server; uricontent:"/update.php?v="; nocase;
uricontent:"&d="; nocase; uricontent:"&vs="; nocase; content:"Host|3a| www.MalwareAlarm.com"; nocase; classtype:trojan-activity; reference:url,sunbeltblog.blogspot.com/2007/04/another-
fake-security-scam-site_9466.html; reference:url,doc.emergingthreats.net/bin/view/Main/2003611; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Malwarealarm.com; sid:2003611; rev:5;)
```

```
#by Matt Jonkman, from sunbelt blog
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Malwarealarm.com Fake AV/AntiSpyware Download"; flow:established,to_server; uricontent:"GET /madownload.php?
&advid="; nocase; uricontent:"&u="; nocase; uricontent:"&p="; nocase; content:"Host\: download.MalwareAlarm.com"; nocase; classtype:trojan-activity;
reference:url,sunbeltblog.blogspot.com/2007/04/another-fake-security-scam-site_9466.html; reference:url,doc.emergingthreats.net/bin/view/Main/2003612;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Malwarealarm.com; sid:2003612; rev:4;)

#submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE MarketScore.com Spyware Configuration Access"; flow: to_server,established; uricontent:"/oss/remoteconfig.asp";
classtype: policy-violation; reference:url,www.marketscore.com; reference:url,www.spysweeper.com/remove-marketscore.html; reference:url,doc.emergingthreats.net/bin/view/Main/2000902;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_MarketScore; sid:2000902; rev:7;)

#submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE MarketScore.com Spyware Access"; flow: to_server,established; uricontent:"proxyhttp|0b|marketscore|03|com";
classtype: policy-violation; reference:url,www.marketscore.com; reference:url,www.spysweeper.com/remove-marketscore.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001359;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_MarketScore; sid:2001359; rev:7;)

#submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 443 (msg:"ET MALWARE MarketScore.com Spyware SSL Access"; flow: to_server,established; content:"www.marketscore.com"; content:"InstantSSL1";
nocase; classtype: policy-violation; reference:url,www.marketscore.com; reference:url,www.spysweeper.com/remove-marketscore.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001563; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_MarketScore; sid:2001563; rev:6;)

#submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE MarketScore.com Spyware Proxied Traffic"; flow: to_server,established; content:"X-OSSProxy|3a| OSSProxy";
classtype: policy-violation; reference:url,www.marketscore.com; reference:url,www.spysweeper.com/remove-marketscore.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001564;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_MarketScore; sid:2001564; rev:7;)

#submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE MarketScore Spyware Uploading Data"; flow: to_server,established; uricontent:"/scripts/contentidpost.dll"; nocase;
content:"OSS-Proxy"; nocase; classtype: policy-violation; reference:url,www.marketscore.com; reference:url,www.spysweeper.com/remove-marketscore.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2003253; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_MarketScore; sid:2003253; rev:3;)

#Info from sgtocanada
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE MarketScore.com Spyware Proxied Traffic (mitmproxy agent)"; flow: to_server,established; content:"Proxy-agent|3a|
ManInTheMiddle-Proxy"; nocase; classtype: policy-violation; reference:url,www.marketscore.com; reference:url,www.spysweeper.com/remove-marketscore.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001586; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_MarketScore; sid:2001586; rev:7;)

#Info from sgtocanada
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE MarketScore.com Spyware Upgrading"; flow: to_server,established; uricontent:"/oss/upgrchk_2a.asp"; nocase;
classtype: policy-violation; reference:url,www.marketscore.com; reference:url,www.spysweeper.com/remove-marketscore.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001587;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_MarketScore; sid:2001587; rev:5;)

#Info from sgtocanada
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE MarketScore.com Spyware Activity (1)"; flow: to_server,established; uricontent:"/oss/dittorules.asp"; nocase;
classtype: policy-violation; reference:url,www.marketscore.com; reference:url,www.spysweeper.com/remove-marketscore.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001588;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_MarketScore; sid:2001588; rev:6;)

#Info from sgtocanada
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE MarketScore.com Spyware Activity (2)"; flow: to_server,established; uricontent:"/oss/routerrules2.asp"; nocase;
classtype: policy-violation; reference:url,www.marketscore.com; reference:url,www.spysweeper.com/remove-marketscore.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001589;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_MarketScore; sid:2001589; rev:6;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET [$HTTP_PORTS,8080] (msg:"ET MALWARE Matcash Trojan Related Spyware Code Download"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
Windows 5.1 (2600)|3b| DMCP"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008759; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Matcash.com; sid:2008759; rev:5;)

#Matt Jonkman from spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Trinityacquisitions.com and Maximumexperience.com Spyware Activity"; flow:to_server,established;
uricontent:"/upd/check?version="; nocase; uricontent:"&localeId="; nocase; uricontent:"&affid="; nocase; uricontent:"&updatevalue="; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2003344; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_MaxExp_TrinityAcquisitions.com; sid:2003344;
rev:3;)

#Mark Tombaugh
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Media Pass ActiveX Install"; flow: to_server,established; uricontent:"/MediaPassK.exe"; nocase; classtype: policy-
violation; reference:url,www.benedelman.org/news/010205-1.html; reference:url,static.windupdates.com/Release/v19/Info.txt; reference:url,doc.emergingthreats.net/bin/view/Main/2001783;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_MediaPass; sid:2001783; rev:8;)

#Submitted by Chris Norton
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE MediaTickets Download"; flow: to_server,established; uricontent:"MediaTicketsInstaller.cab"; content:"Host|3a|
www.mt-download.com"; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.winad.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001448; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_MediaTickets; sid:2001448; rev:10;)

#Submitted by Chris Norton
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE MediaTickets Spyware Install"; flow: to_server,established; uricontent:"/mtrslib2.js"; nocase; classtype: trojan-
activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.winad.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001481;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_MediaTickets; sid:2001481; rev:6;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Medialoads.com Spyware Config"; flow: to_server,established; uricontent:"/dw/cgi/download.cgi?"; nocase;
uricontent:"sn="; nocase; uricontent:"pid="; nocase; content:"Host|3a|config.medialoads.com"; nocase; classtype: trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2001503; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Medialoads.com; sid:2001503; rev:8;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Medialoads.com Spyware Reporting (download.cgi)"; flow: to_server,established; uricontent:"/dw/cgi/download.cgi?";
nocase; uricontent:"sn="; nocase; content:"Host|3a|config.medialoads.com"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001508;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Medialoads.com; sid:2001508; rev:9;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Medialoads.com Spyware Reporting (register.cgi)"; flow: to_server,established; uricontent:"/dw/cgi/register.cgi?";
nocase; uricontent:"v="; nocase; content:"Host|3a|config.medialoads.com"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001509;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Medialoads.com; sid:2001509; rev:9;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Medialoads.com Spyware Identifying Country of Origin"; flow: to_server,established;
uricontent:"/dw/cgi/country.cgi"; nocase; content:"User-Agent|3a|"; nocase; content:"NSISDL"; within:120; nocase; classtype: trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2001507; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Medialoads.com; sid:2001507; rev:10;)

#Submitted by Matt Jonkman
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Metarewards Spyware Activity"; flow: to_server,established; content:"Host|3a| www.metareward.com"; nocase;
classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2001666; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Metarward.com;
sid:2001666; rev:5;)

#From listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Metarewards Disclaimer Access"; flow: to_server,established; uricontent:"/www.metareward.com/mailimg/disclaimer/";
nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002309; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Metarward.com; sid:2002309; rev:4;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Microgaming.com Spyware Installation (dlhelper)"; flow: established,to_server; uricontent:"/dlhelper.cab"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001641; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Microgaming.com;
sid:2001641; rev:6;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Microgaming.com Spyware Installation (2)"; flow: established,to_server; uricontent:"/DownloadHNew.asp?"; nocase;
uricontent:"btag="; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001643; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Microgaming.com; sid:2001643; rev:7;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Microgaming.com Spyware Reporting Installation"; flow: established,to_server;
uricontent:"/dlhelper/downloadlogger2.asp?"; nocase; uricontent:"time="; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001644;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Microgaming.com; sid:2001644; rev:6;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Microgaming.com Spyware Casino App Install"; flow: established,to_server; uricontent:"/viper/thunderluck/00";
nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001645; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Microgaming.com; sid:2001645; rev:5;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Mindset Interactive Install (1)"; flow: to_server,established; uricontent:"/mindset5/data"; nocase; classtype:
trojan-activity; reference:url,www.mindsetinteractive.com; reference:url,doc.emergingthreats.net/bin/view/Main/2000583; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Mindsetinteractive; sid:2000583; rev:7;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Mindset Interactive Install (2)"; flow: to_server,established; uricontent:"/mindset/data"; nocase; classtype:
trojan-activity; reference:url,www.mindsetinteractive.com; reference:url,doc.emergingthreats.net/bin/view/Main/2000584; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Mindsetinteractive; sid:2000584; rev:7;)

#Submitted by Matt Jonkman
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Mindset Interactive Ad Retrieval"; flow: to_server,established; uricontent:"/mindset5"; nocase; classtype:
trojan-activity; reference:url,www.mindsetinteractive.com; reference:url,doc.emergingthreats.net/bin/view/Main/2000594; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Mindsetinteractive; sid:2000594; rev:7;)

#by Matt Jonkman, from spyware LP Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Mirarsearch.com Spyware Posting Data"; flow:established,to_server; uricontent:"/v70match.cgi?"; nocase;
uricontent:"key1="; nocase; uricontent:"&key2="; nocase; uricontent:"&match="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003577;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Mirarsearch.com; sid:2003577; rev:3;)

#by Pedro Marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Adware-Mirar Reporting (BAR)"; flow:to_server,established; uricontent:"download.cgi?BUILDNAME="; nocase;
uricontent:"&AFFILIATE="; uricontent:"&ID="; uricontent:"&ERROR=0"; content:"|0d 0a|User-Agent|3a| BAR"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2009234;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Mirarsearch.com; sid:2009234; rev:3;)

#Matt Jonkman 2/22/05
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE My-Stats.com Spyware Checkin"; flow: established,to_server; uricontent:"/ad-partner/SelectConfirm.php?"; nocase;
uricontent:"dummy="; nocase; classtype: misc-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001747; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_My-Stats.com; sid:2001747; rev:7;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE MyGlobalSearch Spyware bar update"; flow:established,to_server; uricontent:"/images/mysearchbar/highlight"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003351; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_MyGlobalSearch;
sid:2003351; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE MyGlobalSearch Spyware bar update 2"; flow:established,to_server; uricontent:"/images/mysearchbar/customize";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003352; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_MyGlobalSearch; sid:2003352; rev:3;)

#by Akash Mahajan
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Sears.com/Kmart.com My SHC Community spyware download"; flow:to_server,established; content:"GET "; depth:4;
uricontent:"/CSetup_xp.cab"; classtype:trojan-activity; reference:url,community.ca.com/blogs/securityadvisor/archive/2007/12/20/sears-com-join-the-community-get-spyware.aspx;
reference:url,www.benedelman.org/news/010108-1.html; reference:url,doc.emergingthreats.net/bin/view/Main/2007996; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_MySHC; sid:2007996; rev:2;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE MySearchNow.com Spyware"; flow: to_server,established; uricontent:"exe/dns.html"; nocase; content:"User-Agent|3a|
TPSystem"; nocase; classtype:trojan-activity; reference:url,www.mysearchnow.com; reference:url,doc.emergingthreats.net/bin/view/Main/2003221; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_MySearchnow.com; sid:2003221; rev:4;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE MySideSearch.com Spyware Install"; flow:established,to_server; uricontent:".php?aff=mysidesearch&act=install";
content:"|0d 0a|User-Agent|3a| NSISDL/1.2 (Mozilla)|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008915;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_MySideSearch.com; sid:2008915; rev:3;)

#by: Jeremy Conway at sudosecure.net
#ref: 82bd65bc1c0b2b6d2bc599d1295a3579
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE MySideSearch Browser Optimizer"; flow:established,to_server; content:"GET "; depth:4; content:"|0d 0a|User-
Agent|3a| NSISDL/1.2 (Mozilla)|0d 0a|"; nocase; uricontent:".php?aff="; nocase; uricontent:"&act="; nocase; classtype:trojan-activity;
reference:url,www.spywareremove.com/removeMySideSearch.html; reference:url,www.threatexpert.com/threats/adware-win32-mysidesearch.html;
reference:url,www.pctools.com/mrc/infections/id/Adware.MySideSearch/; reference:url,doc.emergingthreats.net/2009524; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_MySideSearch.com; sid:2009524; rev:4;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE My Search Bar Install"; flow: to_server,established; uricontent:"/mysetp.exe"; nocase; classtype:trojan-activity;
reference:url,www.2-spyware.com/parasite-my-search-bar.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001040; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_My_Search_Bar; sid:2001040; rev:8;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE My Search Spyware Config Download"; flow: to_server,established; uricontent:"/ms"; nocase; uricontent:"cfg.jsp?";
```

```
uricontent:"v="; nocase; pcre:"/\/ms\d\d\dcfg\.jsp/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002839;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_My_Search_Bar; sid:2002839; rev:5;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE MyWebSearch Toolbar Receiving Configuration"; flow: to_server,established; uricontent:"/speedbar/mySpeedbarCfg";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2000600; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_My_Web_Toolbar; sid:2000600; rev:11;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE MyWebSearch Toolbar Traffic (bar config download)"; flow: to_server,established; uricontent:"/barcfg.jsp?"; nocase;
content:"MyWebSearchWB"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002836; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_My_Web_Toolbar; sid:2002836; rev:6;)

#New, from spyware listening post hits
#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE MyWebSearch Toolbar Receiving Config 2"; flow: to_server,established; uricontent:"/mySpeedbarCfg2.jsp"; nocase;
content:"MyWebSearch"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003222; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_My_Web_Toolbar; sid:2003222; rev:5;)

#New, from spyware listening post hits
#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE MyWebSearch Toolbar Posting Activity Report"; flow:to_server,established; uricontent:"/jsp/cfg_redir2.jsp?id=";
nocase; uricontent:"url=http"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003617; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_My_Web_Toolbar; sid:2003617; rev:5;)

#New, from spyware listening post hits
#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE MyWay Spyware Posting Activity Report - Dell Related"; flow:to_server,established;
uricontent:"/script/bzDellHpData.js?"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003621; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_My_Web_Toolbar; sid:2003621; rev:5;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE New.net Spyware updating"; flow:established,to_server; uricontent:"/download/NewDotNet/"; nocase;
uricontent:"/upgrade.cab?"; nocase; uricontent:"upg="; nocase; uricontent:"ec="; nocase; classtype:trojan-activity; reference:url,www.new.net;
reference:url,doc.emergingthreats.net/bin/view/Main/2003240; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_New.net; sid:2003240; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE New.net Spyware Checkin"; flow:established,to_server; uricontent:"/?version="; nocase; uricontent:"discard_tag=";
nocase; uricontent:"source="; nocase; uricontent:"ptr="; nocase; uricontent:"br=NewDotNet"; nocase; uricontent:"ec="; nocase; classtype:trojan-activity; reference:url,www.new.net;
reference:url,doc.emergingthreats.net/bin/view/Main/2003241; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_New.net; sid:2003241; rev:4;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Oenji.com Install"; flow: to_server,established; uricontent:"/Bundled/OemjiInstall"; nocase; classtype: trojan-
activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001538; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Oemji.com; sid:2001538; rev:6;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Spyspotter.com Access, Likely Spyware"; flow: to_server,established; content:"Host|3a|"; nocase; depth: 400;
content:".oemji.com"; within: 25; distance: 1; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001539; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Oemji.com; sid:2001539; rev:9;)

#by Reg Quinton
#
alert tcp $HOME_NET [0:20,22:24,26:464,466:586,588:901,903:65535] -> any any (msg:"ET MALWARE Suspicious FTP 220 Banner on Local Port (-)"; flow:from_server,established; content:"220-";
depth:4; classtype:non-standard-protocol; reference:url,doc.emergingthreats.net/bin/view/Main/2003055; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Off_Port_FTP; sid:2003055; rev:10;)

#by Reg Quinton
#
alert tcp $HOME_NET [0:20,22:24,26:138,140:444,446:464,466:586,588:901,903:1432,1434:65535] -> any any (msg:"ET MALWARE Suspicious FTP 220 Banner on Local Port (spaced)";
flow:from_server,established; content:"220 "; depth:4; classtype:non-standard-protocol; reference:url,doc.emergingthreats.net/2011124; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Off_Port_FTP; sid:2011124; rev:11;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE OfferOptimizer.com Spyware"; flow: to_server,established; uricontent:"/ctx/keyword_context.php?"; nocase;
uricontent:"urlContext=http"; nocase; classtype: policy-violation; reference:url,www.offeroptimizer.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001341;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Offer_Optimizer; sid:2001341; rev:9;)

#by Will Metcalf
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE OneStepSearch Host Activity"; flow: to_server,established; content:"GET "; depth:4; content:"|0d0a|host|3a|
upgrade.onestepsearch.net"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007855; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Onestepsearch; sid:2007855; rev:3;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE OutBlaze.com Spyware Activity"; flow: to_server,established; uricontent:"/scripts/adpopper/webservice.main";
nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002044; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Outblaze.com; sid:2002044; rev:4;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Outerinfo.com Spyware Install"; flow: to_server,established; uricontent:"/ctxad-"; nocase; pcre:"/ctxad-
\d+\.sig/Ui"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001495; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Outerinfo.com; sid:2001495; rev:8;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Outerinfo.com Spyware Advertising Campaign Download"; flow: to_server,established; uricontent:"/campaigns"; nocase;
content:"outerinfo.com"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001496; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Outerinfo.com; sid:2001496; rev:5;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Outerinfo.com Spyware Activity"; flow: to_server,established; content:"Host|3a| campaigns.outerinfo.com"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001497; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Outerinfo.com;
sid:2001497; rev:6;)

#Matt jonkman, from spywarelp data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Outerinfo.com Spyware Checkin"; flow: to_server,established; uricontent:"/notify.php?"; nocase; uricontent:"pid=";
nocase; uricontent:"&module="; nocase; uricontent:"&v="; nocase; uricontent:"&result="; nocase; uricontent:"&message="; nocase; content:"outerinfo.com"; nocase; classtype: trojan-
activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003426; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Outerinfo.com; sid:2003426; rev:3;)

#Submitted by Chris Norton
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Overpro Spyware Bundle Install"; flow: to_server,established; content:"Host|3a| download.overpro.com"; nocase;
pcre:"/(GET |GET (http|https)\:\/\/[-0-9a-z.]*)\/WildApp\.cab/i"; classtype: trojan-activity; reference:url,www.wildarcade.com;
reference:url,doc.emergingthreats.net/bin/view/Main/2001444; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Overpro; sid:2001444; rev:11;)
```

```
#By Matt Jonkman
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Overpro Spyware Games"; flow: to_server,established; uricontent:"/blocks/blasterblocks"; nocase; classtype:
trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.overpro.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001459;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Overpro; sid:2001459; rev:9;)

#By Matt Jonkman
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Overpro Spyware Install Report"; flow: to_server,established; uricontent:"/processInstall.aspx"; nocase;
classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.overpro.html; reference:url,doc.emergingthreats.net/bin/view/Main/2002017;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Overpro; sid:2002017; rev:7;)

#by jeremy at sudosecure
#ref: 48ba8bfecf840fc9a5f8ff2e225452a7
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE EMO/PCPrivacyCleaner Rougue Secuirty App GET Checkin"; flow:established,to_server; content:"GET "; depth:4;
uricontent:"action="; nocase; uricontent:"addt="; nocase; uricontent:"pc|5F|id="; nocase; uricontent:"abbr="; nocase; classtype:trojan-activity;
reference:url,www.spywaresignatures.com/details/pcprivacycleaner.pdf; reference:url,doc.emergingthreats.net/bin/view/Main/2008456; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_PCPrivacycleaner; sid:2008456; rev:3;)

#Matt Jonkman from Spyware Listening Post Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Pacimedia Spyware 1"; flow:to_server,established; uricontent:"/mcp/mcp.cgi"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2002083; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Pacimedia; sid:2002083; rev:4;)

#Matt Jonkman from Spyware Listening Post Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Pacimedia Spyware 2"; flow: to_server,established; uricontent:"/xml/check.php?"; nocase; uricontent:"u="; nocase;
classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002194; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Pacimedia;
sid:2002194; rev:6;)

#lovely fake av package at pcdoc.co.kr
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS PCDoc.co.kr Fake AV User-Agent (PCDoc11)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| PCDoc";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007786; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Pcdoc.co.kr;
sid:2007786; rev:4;)

#lovely fake av package at pcdoc.co.kr
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET USER_AGENTS PCDoc.co.kr Fake AV User-Agent (mypcdoctor)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
mypcdoc"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007804; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Pcdoc.co.kr; sid:2007804; rev:3;)

#Submitted by Chris Norton
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE PeopleOnPage Install"; flow: to_server,established; uricontent:"/install/pop"; nocase; classtype: policy-violation;
reference:url,www.peopleonpage.com; reference:url,www.safer-networking.org/en/threats/602.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001445;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_PeopleonPage; sid:2001445; rev:10;)

#Submitted by Chris Norton
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE PeopleOnPage Ping"; flow: to_server,established; content:"Host|3a| srv.peopleonpage.com"; nocase; pcre:"/(POST
|POST (http|https)\:\/\/[-0-9a-z.]*)\/s\/l\/firstping/i"; classtype: policy-violation; reference:url,www.peopleonpage.com; reference:url,www.safer-networking.org/en/threats/602.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001446; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_PeopleonPage; sid:2001446; rev:9;)

#by: Jeremy Conway at sudosecure.net
#ref: a9036ae5d9bb8e3c53d5e0126d448d1d
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Adware PlusDream - GET Config Download/Update"; flow:established,to_server; content:"GET "; depth:4;
uricontent:".php?kind="; nocase; uricontent:"&pid="; nocase; uricontent:"&ver="; nocase; uricontent:"&addresses="; nocase; uricontent:"&hdmacid="; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2009712; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_PlusDream; sid:2009712; rev:2;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Popuptraffic.com Bot Reporting"; flow: to_server,established; uricontent:"/scripts/click.php?"; nocase;
uricontent:"hid="; classtype: policy-violation; reference:url,popuptraffic.com; reference:url,doc.emergingthreats.net/bin/view/Main/2000577; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Popuptraffic.com_Reporting; sid:2000577; rev:8;)

#By Matt Jonkman from spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Privacyprotector.com Fake Anti-Spyware Install"; flow: to_server,established;
uricontent:"/privacyprotectorfreesetup.exe"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003547; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Privacyprotector.com; sid:2003547; rev:3;)

#By Matt Jonkman from spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Privacyprotector.com Fake Anti-Spyware Checkin"; flow: to_server,established; uricontent:"/?action="; nocase;
uricontent:"&type="; nocase; uricontent:"&pc_id="; nocase; uricontent:"&abbr="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003548;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Privacyprotector.com; sid:2003548; rev:3;)

#storageguardsoft.com also related, same installer, similar hosts
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE AVSystemcare.com.com Fake Anti-Virus Product"; flow:established,to_server; uricontent:"?proto="; nocase;
uricontent:"&rc="; nocase; uricontent:"&v="; nocase; uricontent:"&abbr="; nocase; uricontent:"&platform="; nocase; uricontent:"&os_version="; nocase; uricontent:"&ac="; nocase;
uricontent:"&appid="; nocase; uricontent:"&em="; nocase; uricontent:"&pcid="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007664;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Privacyprotector.com; sid:2007664; rev:3;)

#Submitted by John Stewart, 2/23/2005
#
alert tcp $HOME_NET any -> any $HTTP_PORTS (msg:"ET MALWARE Pynix.dll BHO Activity"; flow: established,to_server; uricontent:"ABETTERINTERNET.EXE"; nocase; uricontent:"bho=PYNIX.DLL";
nocase; classtype: trojan-activity; reference:url,www.pynix.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001748; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Pynix; sid:2001748; rev:5;)

#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Rabio Spyware/Adware Initial Registration"; flow:established,to_server; dsize:<200; content:"POST "; depth:5;
content:"|0d 0a 0d 0a|REGISTER|7c|"; pcre:"/REGISTER\x7c\d+\x7c\d+\x7c\d+\x7c\d+/"; classtype:trojan-activity; reference:url,www.spywareguide.com/product_show.php?id=3770;
reference:url,www.rabio.com; reference:url,doc.emergingthreats.net/bin/view/Main/2007820; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Rabio;
sid:2007820; rev:2;)

#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Rabio.com Related Adware/Spyware User-Agent (HTTP_CONNECT_2)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| HTTP_Connect_"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007821; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Rabio; sid:2007821; rev:3;)

#Updated by Jonathan Miner
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE rcprograms"; flow: to_server,established; content:"update.rcprograms.com"; nocase; classtype: trojan-activity;
reference:url,sarc.com/avcenter/venc/data/adware.rcprograms.html; reference:url,doc.emergingthreats.net/bin/view/Main/2000024; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Rcprograms; sid:2000024; rev:7;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Rdxrp.com Traffic"; flow: to_server,established; uricontent:"/rdxr020304.dat"; nocase; classtype: trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2001311; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Rdxrp.com; sid:2001311; rev:5;)
```

```
#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Rdxrp.com Traffic (Generic)"; flow: to_server,established; uricontent:"/rdxr"; nocase; uricontent:".dat"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001312; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Rdxrp.com;
sid:2001312; rev:5;)

#they run a lot of casino online games
#matt jonkman, re f5e2b1706a3e0e6d34e70677a6e952a6
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 20000 (msg:"ET MALWARE Realtimegaming.com Online Casino Spyware Gaming Checkin"; flow:established,to_server; dsize:<30; content:"|43 01 00|";
depth:4; content:"Casino"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008402; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Realtimegaming.com; sid:2008402; rev:3;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Regnow.com Access"; flow: to_server,established; uricontent:"/softsell/visitor.cgi?"; nocase;
uricontent:"affiliate="; nocase; classtype: trojan-activity; reference:url,www.regnow.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001223;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Regnow.com; sid:2001223; rev:7;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Regnow.com Gamehouse.com Access"; flow: to_server,established; uricontent:"/affiliates/template.jsp?"; nocase;
uricontent:"AID="; nocase; classtype: trojan-activity; reference:url,www.gamehouse.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001224;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Regnow.com; sid:2001224; rev:7;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Salongas Infection"; flow: to_server,established; uricontent:"/sp.htm?id="; classtype: trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2000601; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Salongas; sid:2000601; rev:5;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Search Relevancy Spyware"; flow: established,to_server; uricontent:"/SearchRelevancy/SearchRelevancy.dll"; nocase;
classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/spyware.relevancy.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001696;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_SearchRelevancy; sid:2001696; rev:8;)

#By Matt Jonkman from Listening Post Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Searchfeed.com Spyware 1"; flow: to_server,established; uricontent:"/rd/Clk.jsp"; classtype: trojan-activity;
reference:url,www.searchfeed.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002296; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Searchfeed.com; sid:2002296; rev:6;)

#By Matt Jonkman from Listening Post Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Searchfeed.com Spyware 2"; flow: to_server,established; uricontent:"/rd/feed/TextFeed.jsp"; classtype: trojan-
activity; reference:url,www.searchfeed.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002297; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Searchfeed.com; sid:2002297; rev:4;)

#By Matt Jonkman from Listening Post Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Searchfeed.com Spyware 3"; flow: to_server,established; uricontent:"/rd/feed/XMLFeed.jsp"; classtype: trojan-
activity; reference:url,www.searchfeed.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002298; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Searchfeed.com; sid:2002298; rev:4;)

#By Matt Jonkman from Listening Post Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Searchfeed.com Spyware 4"; flow: to_server,established; uricontent:"/rd/feed/JavaScriptFeed.jsp"; classtype:
trojan-activity; reference:url,www.searchfeed.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002299; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Searchfeed.com; sid:2002299; rev:4;)

#By Matt Jonkman from Listening Post Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Searchfeed.com Spyware 5"; flow: to_server,established; uricontent:"/rd/feed/JavaScriptFeedSE.jsp"; classtype:
trojan-activity; reference:url,www.searchfeed.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002300; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Searchfeed.com; sid:2002300; rev:4;)

#By Matt Jonkman from Listening Post Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Searchfeed.com Spyware 6"; flow: to_server,established; uricontent:"/rd/SearchResults.jsp"; classtype: trojan-
activity; reference:url,www.searchfeed.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002301; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Searchfeed.com; sid:2002301; rev:4;)

#By Matt Jonkman from Listening Post Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Searchfeed.com Spyware 7"; flow: to_server,established; uricontent:"/rd/jsp/BidRank/index.jsp"; classtype: trojan-
activity; reference:url,www.searchfeed.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002302; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Searchfeed.com; sid:2002302; rev:4;)

#By Matt Jonkman from Listening Post Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Searchfeed.com Spyware 8"; flow: to_server,established; uricontent:"/SFToolBar.html"; classtype: trojan-activity;
reference:url,www.searchfeed.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002303; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Searchfeed.com; sid:2002303; rev:4;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Searchmeup Spyware Install (toolbar)"; flow: to_server,established; uricontent:"/dkprogs/toolbar.txt"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001473; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Searchmeup;
sid:2001473; rev:7;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Searchmeup Spyware Install (prog)"; flow: to_server,established; uricontent:"/dkprogs/dktibs.php"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001474; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Searchmeup;
sid:2001474; rev:7;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Searchmeup Spyware Receiving Commands"; flow: to_server,established; uricontent:"/xpsystem/commands.ini"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001475; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Searchmeup;
sid:2001475; rev:6;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Searchmeup Spyware Install (systime)"; flow: to_server,established; uricontent:"/dkprogs/systime.txt"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001480; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Searchmeup;
sid:2001480; rev:7;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Searchmeup Spyware Install (mstask)"; flow: to_server,established; uricontent:"/dkprogs/mstasks3.txt"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001483; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Searchmeup;
sid:2001483; rev:7;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Searchmeup Spyware Install (d.exe)"; flow: to_server,established; uricontent:"/x30/d.exe"; nocase; classtype:
trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001484; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Searchmeup; sid:2001484;
rev:7;)
```

```
#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Searchmiracle.com Spyware Install (v3cab)"; flow: to_server,established; uricontent:"/cab/v3cab.cab"; classtype:
trojan-activity; reference:url,www.searchmiracle.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001540; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Searchmiracle.com; sid:2001540; rev:9;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Searchmiracle.com Access, Likely Spyware"; flow: to_server,established; content:"Host|3a|"; nocase; depth: 400;
content:".searchmiracle.com"; nocase; within: 35; distance: 1; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/trojan.elitebar.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001532; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Searchmiracle.com; sid:2001532; rev:11;)

#By Matt Jonkman
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET MALWARE Searchmiracle.com Spyware Installer silent.exe Download"; flow: from_server,established; content:"|20 28 43 29 20
32 30 30 31 2c 20 32 30 30 33 20 52 61 64 69 6d 20 50 69 63 68 61|"; classtype: trojan-activity; reference:url,www.searchmiracle.com/silent.exe;
reference:url,doc.emergingthreats.net/bin/view/Main/2001533; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Searchmiracle.com; sid:2001533; rev:9;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Searchmiracle.com Spyware Install (silent_install)"; flow: to_server,established; uricontent:"/silent_install.exe";
nocase; classtype: trojan-activity; reference:url,www.searchmiracle.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001534; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Searchmiracle.com; sid:2001534; rev:11;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Searchmiracle.com Spyware Install (protector.exe)"; flow: to_server,established; uricontent:"/protector.exe";
content:"Host|3a| install.searchmiracle.com"; nocase; classtype: trojan-activity; reference:url,www.searchmiracle.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001535;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Searchmiracle.com; sid:2001535; rev:11;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Searchmiracle.com Spyware Install (install)"; flow: to_server,established; uricontent:"/sideb.exe";
content:"Host|3a| install.searchmiracle.com"; nocase; classtype: trojan-activity; reference:url,www.searchmiracle.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001744;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Searchmiracle.com; sid:2001744; rev:11;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Searchmiracle.com Spyware Install - silent.exe"; flow: to_server,established; uricontent:"/silent.exe"; nocase;
classtype: trojan-activity; reference:url,www.searchmiracle.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002091; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Searchmiracle.com; sid:2002091; rev:5;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Search Scout Related Spyware (content)"; flow: established,to_server; content:"Host|3a| content.searchscout.com";
nocase; classtype: policy-violation; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.searchscout.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001650;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Searchscout; sid:2001650; rev:7;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Search Scout Related Spyware (results)"; flow: established,to_server; content:"Host|3a| results.searchscout.com";
nocase; classtype: policy-violation; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.searchscout.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001653;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Searchscout; sid:2001653; rev:7;)

#by Matt Jonkman, from spyware LP Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Security-updater.com Spyware Posting Data"; flow:established,to_server; uricontent:"/SA/receive_data.php3?tcpc=";
content:"security-updater.com"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003576; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Security-updater.com; sid:2003576; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Seekmo.com Spyware Data Upload"; flow:established,to_server; uricontent:".aspx?"; uricontent:"eid=";
uricontent:"&pkg_ver="; uricontent:"&ver="; uricontent:"&brand="; uricontent:"&mt="; uricontent:"&partid="; uricontent:"&altdid="; uricontent:"&os="; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2008356; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Seekmo.com; sid:2008356; rev:2;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Servicepack.kr Fake Patch Software Checkin"; flow:established,to_server; uricontent:".php?kind="; nocase;
uricontent:"&ver="; nocase; uricontent:"&ver2="; nocase; uricontent:"&ver3="; nocase; uricontent:"&pid="; nocase; uricontent:"&supportid="; nocase; uricontent:"&uniq="; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008016; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Servicepack.kr;
sid:2008016; rev:2;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Sexmaniack Install Tracking"; flow: to_server,established; uricontent:"/counted.php?ref="; nocase;
content:"Host|3a| counter.sexmaniack.com"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001460; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Sexmaniak; sid:2001460; rev:8;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Shop At Home Select.com Install Attempt"; flow: to_server,established; uricontent:"/mindset/bunsetup.cab"; nocase;
classtype: policy-violation; reference:url,www.spywareguide.com/product_show.php?id=700; reference:url,www.shopathomeselect.com;
reference:url,doc.emergingthreats.net/bin/view/Main/2000580; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_ShopAtHomeSelect; sid:2000580; rev:7;)

#Submitted by Matt Jonkman
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET MALWARE Shop At Home Select.com Install Download"; flow: from_server,established; content:"|ab 3b d4 97 d4 a7 b4 1d da 6e
6d 0f f4 aa 4f|"; content:"|46 b3 3b 8b 38 cc 2c 2a a4 c3 07 67 67 df 65 41|"; classtype: policy-violation; reference:url,www.spywareguide.com/product_show.php?id=700;
reference:url,www.shopathomeselect.com; reference:url,doc.emergingthreats.net/bin/view/Main/2000581; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_ShopAtHomeSelect; sid:2000581; rev:8;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Shop at Home Select Spyware Heartbeat"; flow: established,to_server; uricontent:"/s.dll?
MfcISAPICommand=heartbeat&param="; nocase; classtype: policy-violation; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.sahagent.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001708; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_ShopAtHomeSelect; sid:2001708; rev:8;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Shop at Home Select Spyware Install"; flow: established,to_server; uricontent:"/arcadecash/setup"; nocase;
classtype: policy-violation; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.sahagent.html; reference:url,doc.emergingthreats.net/bin/view/Main/2002037;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_ShopAtHomeSelect; sid:2002037; rev:5;)

#matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Shopnav Spyware Install"; flow: to_server,established; uricontent:"/toolbarv3.cgi?UID="; nocase;
uricontent:"&version="; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/spyware.shopnav.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2002000; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_ShopNav; sid:2002000; rev:5;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Shopcenter.co.kr Spyware Install Report"; flow:established,to_server; uricontent:"/RewardInstall.php?mac=0";
uricontent:"&hdd="; uricontent:"&ver="; uricontent:"&ie="; uricontent:"&win="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008370;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Shopcenter.co.kr; sid:2008370; rev:2;)

#Submitted by Matt Jonkman
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE SideStep Bar Install"; flow: to_server,established; uricontent:"/servlet/sbinstservlet"; nocase; classtype: policy-
violation; reference:url,www.sidestep.com; reference:url,www.spyany.com/program/article_spw_rm_SideStep.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001016;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_SideStep_Bar; sid:2001016; rev:8;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE SideStep Bar Reporting Data"; flow: to_server,established; uricontent:"/servlet/sblogservlet"; nocase; classtype:
policy-violation; reference:url,www.sidestep.com; reference:url,www.spyany.com/program/article_spw_rm_SideStep.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001017;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_SideStep_Bar; sid:2001017; rev:8;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE SideStep Bar Reporting Data (sbstart)"; flow: to_server,established; uricontent:"/servlet/SbStartservlet"; nocase;
classtype: policy-violation; reference:url,www.sidestep.com; reference:url,www.spyany.com/program/article_spw_rm_SideStep.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2002821; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_SideStep_Bar; sid:2002821; rev:5;)

#by RPG
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Simbar Spyware User-Agent Detected"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| ";
content:"SIMBAR="; within:150; pcre:"/User-Agent\:[^\n]+\;\sSIMBAR=/"; threshold:type limit, count 1, seconds 60, track by_src; classtype:trojan-activity;
reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=AdWare.Win32.Simbar.a&threatid=427805; reference:url,vil.nai.com/vil/content/v_131206.htm;
reference:url,doc.emergingthreats.net/bin/view/Main/2009005; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Simbar; sid:2009005; rev:5;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Smartpops.com Spyware Install rh.exe"; flow: to_server,established; uricontent:"/install/RH/rh.exe"; nocase;
classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.smartpops.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001505;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Smartpops.com; sid:2001505; rev:8;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Smartpops.com Spyware Install"; flow: to_server,established; uricontent:"/install/SE/sed.exe"; nocase; classtype:
trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.smartpops.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001516;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Smartpops.com; sid:2001516; rev:7;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Smartpops.com Spyware Update"; flow: to_server,established; uricontent:"/data/spv15.dat?v="; nocase; classtype:
trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.smartpops.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001513;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Smartpops.com; sid:2001513; rev:7;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Snoopstick.net Related Spyware User-Agent (SnoopStick Updater)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| SnoopStick "; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007956; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Snoopstick; sid:2007956; rev:3;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 1024:5000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv5 Port 25 Inbound Request (Windows Source)"; dsize:10; flow:established,to_server; content:"|05 01 00
01|"; depth:4; content:"|00 19|"; offset:8; depth:2; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode;
reference:url,handlers.sans.org/wsalusky/rants/; reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt;
reference:url,ss5.sourceforge.net/socks4A.protocol.txt; reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt;
reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt; reference:url,doc.emergingthreats.net/bin/view/Main/2003254;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003254; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 32768:61000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv5 Port 25 Inbound Request (Linux Source)"; dsize:10; flow:established,to_server; content:"|05 01 00
01|"; depth:4; content:"|00 19|"; offset:8; depth:2; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode;
reference:url,handlers.sans.org/wsalusky/rants/; reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt;
reference:url,ss5.sourceforge.net/socks4A.protocol.txt; reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt;
reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt; reference:url,doc.emergingthreats.net/bin/view/Main/2003255;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003255; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 1024:5000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv4 Port 25 Inbound Request (Windows Source)"; dsize:9<>18; flow:established,to_server; content:"|04 01 00
19|"; depth:4; threshold:type both, track by_src, count 2, seconds 900; classtype:protocol-command-decode; reference:url,handlers.sans.org/wsalusky/rants/;
reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt; reference:url,ss5.sourceforge.net/socks4A.protocol.txt;
reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt; reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt;
reference:url,doc.emergingthreats.net/bin/view/Main/2003256; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003256; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 32768:61000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv5 Port 25 Inbound Request (Linux Source)"; dsize:9<>18; flow:established,to_server; content:"|04 01 00
19|"; depth:4; threshold:type both, track by_src, count 2, seconds 900; classtype:protocol-command-decode; reference:url,handlers.sans.org/wsalusky/rants/;
reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt; reference:url,ss5.sourceforge.net/socks4A.protocol.txt;
reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt; reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt;
reference:url,doc.emergingthreats.net/bin/view/Main/2003257; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003257; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 1024:5000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv5 DNS Inbound Request (Windows Source)"; dsize:10<>40; flow:established,to_server; content:"|05 01 00
03|"; depth:4; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode; reference:url,handlers.sans.org/wsalusky/rants/;
reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt; reference:url,ss5.sourceforge.net/socks4A.protocol.txt;
reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt; reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt;
reference:url,doc.emergingthreats.net/bin/view/Main/2003258; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003258; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 32768:61000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv5 DNS Inbound Request (Linux Source)"; dsize:10<>40; flow:established,to_server; content:"|05 01 00
03|"; depth:4; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode; reference:url,handlers.sans.org/wsalusky/rants/;
reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt; reference:url,ss5.sourceforge.net/socks4A.protocol.txt;
reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt; reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt;
reference:url,doc.emergingthreats.net/bin/view/Main/2003259; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003259; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
```

```
#
alert tcp $EXTERNAL_NET 1024:5000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv5 HTTP Proxy Inbound Request (Windows Source)"; dsize:10; flow:established,to_server; content:"|05 01 00
01|"; depth:4; content:"|00 50|"; offset:8; depth:2; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode;
reference:url,handlers.sans.org/wsalusky/rants/; reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt;
reference:url,ss5.sourceforge.net/socks4A.protocol.txt; reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt;
reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt; reference:url,doc.emergingthreats.net/bin/view/Main/2003260;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003260; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 32768:61000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv5 HTTP Proxy Inbound Request (Linux Source)"; dsize:10; flow:established,to_server; content:"|05 01 00
01|"; depth:4; content:"|00 50|"; offset:8; depth:2; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode;
reference:url,handlers.sans.org/wsalusky/rants/; reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt;
reference:url,ss5.sourceforge.net/socks4A.protocol.txt; reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt;
reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt; reference:url,doc.emergingthreats.net/bin/view/Main/2003261;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003261; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 1024:5000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv4 HTTP Proxy Inbound Request (Windows Source)"; dsize:9<>18; flow:established,to_server; content:"|04 01
00 50|"; depth:4; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode; reference:url,handlers.sans.org/wsalusky/rants/;
reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt; reference:url,ss5.sourceforge.net/socks4A.protocol.txt;
reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt; reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt;
reference:url,doc.emergingthreats.net/bin/view/Main/2003262; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003262; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 32768:61000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv4 HTTP Proxy Inbound Request (Linux Source)"; dsize:9<>18; flow:established,to_server; content:"|04 01
00 50|"; depth:4; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode; reference:url,handlers.sans.org/wsalusky/rants/;
reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt; reference:url,ss5.sourceforge.net/socks4A.protocol.txt;
reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt; reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt;
reference:url,doc.emergingthreats.net/bin/view/Main/2003263; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003263; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 1024:5000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv5 Port 443 Inbound Request (Windows Source)"; dsize:10; flow:established,to_server; content:"|05 01 00
01|"; depth:4; content:"|01 bb|"; offset:8; depth:2; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode;
reference:url,handlers.sans.org/wsalusky/rants/; reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt;
reference:url,ss5.sourceforge.net/socks4A.protocol.txt; reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt;
reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt; reference:url,doc.emergingthreats.net/bin/view/Main/2003266;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003266; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 32768:61000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv5 Port 443 Inbound Request (Linux Source)"; dsize:10; flow:established,to_server; content:"|05 01 00
01|"; depth:4; content:"|01 bb|"; offset:8; depth:2; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode;
reference:url,handlers.sans.org/wsalusky/rants/; reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt;
reference:url,ss5.sourceforge.net/socks4A.protocol.txt; reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt;
reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt; reference:url,doc.emergingthreats.net/bin/view/Main/2003267;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003267; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 1024:5000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv4 Port 443 Inbound Request (Windows Source)"; dsize:9<>18; flow:established,to_server; content:"|04 01
01 bb|"; depth:4; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode; reference:url,handlers.sans.org/wsalusky/rants/;
reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt; reference:url,ss5.sourceforge.net/socks4A.protocol.txt;
reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt; reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt;
reference:url,doc.emergingthreats.net/bin/view/Main/2003268; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003268; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 32768:61000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv4 Port 443 Inbound Request (Linux Source)"; dsize:9<>18; flow:established,to_server; content:"|04 01
01 bb|"; depth:4; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode; reference:url,handlers.sans.org/wsalusky/rants/;
reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt; reference:url,ss5.sourceforge.net/socks4A.protocol.txt;
reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt; reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt;
reference:url,doc.emergingthreats.net/bin/view/Main/2003269; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003269; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 1024:5000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv5 Port 5190 Inbound Request (Windows Source)"; dsize:10; flow:established,to_server; content:"|05 01 00
01|"; depth:4; content:"|14 46|"; offset:8; depth:2; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode;
reference:url,handlers.sans.org/wsalusky/rants/; reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt;
reference:url,ss5.sourceforge.net/socks4A.protocol.txt; reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt;
reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt; reference:url,doc.emergingthreats.net/bin/view/Main/2003270;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003270; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 32768:61000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv5 Port 5190 Inbound Request (Linux Source)"; dsize:10; flow:established,to_server; content:"|05 01 00
01|"; depth:4; content:"|14 46|"; offset:8; depth:2; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode;
reference:url,handlers.sans.org/wsalusky/rants/; reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt;
reference:url,ss5.sourceforge.net/socks4A.protocol.txt; reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt;
reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt; reference:url,doc.emergingthreats.net/bin/view/Main/2003271;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003271; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
```

```
alert tcp $EXTERNAL_NET 1024:5000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv4 Port 5190 Inbound Request (Windows Source)"; dsize:9<>18; flow:established,to_server; content:"|04 01
14 46|"; depth:4; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode; reference:url,handlers.sans.org/wsalusky/rants/;
reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt; reference:url,ss5.sourceforge.net/socks4A.protocol.txt;
reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt; reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt;
reference:url,doc.emergingthreats.net/bin/view/Main/2003272; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003272; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 32768:61000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv5 Port 5190 Inbound Request (Linux Source)"; dsize:9<>18; flow:established,to_server; content:"|04 01
14 46|"; depth:4; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode; reference:url,handlers.sans.org/wsalusky/rants/;
reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt; reference:url,ss5.sourceforge.net/socks4A.protocol.txt;
reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt; reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt;
reference:url,doc.emergingthreats.net/bin/view/Main/2003273; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003273; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 1024:5000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv5 Port 1863 Inbound Request (Windows Source)"; dsize:10; flow:established,to_server; content:"|05 01 00
01|"; depth:4; content:"|07 47|"; offset:8; depth:2; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode;
reference:url,handlers.sans.org/wsalusky/rants/; reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt;
reference:url,ss5.sourceforge.net/socks4A.protocol.txt; reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt;
reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt; reference:url,doc.emergingthreats.net/bin/view/Main/2003274;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003274; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 32768:61000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv5 Port 1863 Inbound Request (Linux Source)"; dsize:10; flow:established,to_server; content:"|05 01 00
01|"; depth:4; content:"|07 47|"; offset:8; depth:2; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode;
reference:url,handlers.sans.org/wsalusky/rants/; reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt;
reference:url,ss5.sourceforge.net/socks4A.protocol.txt; reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt;
reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt; reference:url,doc.emergingthreats.net/bin/view/Main/2003275;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003275; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 1024:5000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv4 Port 1863 Inbound Request (Windows Source)"; dsize:9<>18; flow:established,to_server; content:"|04 01
07 47|"; depth:4; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode; reference:url,handlers.sans.org/wsalusky/rants/;
reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt; reference:url,ss5.sourceforge.net/socks4A.protocol.txt;
reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt; reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt;
reference:url,doc.emergingthreats.net/bin/view/Main/2003276; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003276; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 32768:61000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv4 Port 1863 Inbound Request (Linux Source)"; dsize:9<>18; flow:established,to_server; content:"|04 01
07 47|"; depth:4; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode; reference:url,handlers.sans.org/wsalusky/rants/;
reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt; reference:url,ss5.sourceforge.net/socks4A.protocol.txt;
reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt; reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt;
reference:url,doc.emergingthreats.net/bin/view/Main/2003277; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003277; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 1024:5000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv5 Port 5050 Inbound Request (Windows Source)"; dsize:10; flow:established,to_server; content:"|05 01 00
01|"; depth:4; content:"|13 ba|"; offset:8; depth:2; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode;
reference:url,handlers.sans.org/wsalusky/rants/; reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt;
reference:url,ss5.sourceforge.net/socks4A.protocol.txt; reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt;
reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt; reference:url,doc.emergingthreats.net/bin/view/Main/2003278;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003278; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 32768:61000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv5 Port 5050 Inbound Request (Linux Source)"; dsize:10; flow:established,to_server; content:"|05 01 00
01|"; depth:4; content:"|13 ba|"; offset:8; depth:2; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode;
reference:url,handlers.sans.org/wsalusky/rants/; reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt;
reference:url,ss5.sourceforge.net/socks4A.protocol.txt; reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt;
reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt; reference:url,doc.emergingthreats.net/bin/view/Main/2003279;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003279; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 1024:5000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv4 Port 5050 Inbound Request (Windows Source)"; dsize:9<>18; flow:established,to_server; content:"|04 01
13 ba|"; depth:4; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode; reference:url,handlers.sans.org/wsalusky/rants/;
reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt; reference:url,ss5.sourceforge.net/socks4A.protocol.txt;
reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt; reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt;
reference:url,doc.emergingthreats.net/bin/view/Main/2003280; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003280; rev:5;)

#by William Salusky of the ISC (www.incidents.org)
#Details and updates available here http://handlers.sans.org/wsalusky/rants/
#Cleanup and updates by John Pritchard
#If you have any socks proxies being abused in your environment... The following four rules are MONEY.
#
alert tcp $EXTERNAL_NET 32768:61000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv4 Port 5050 Inbound Request (Linux Source)"; dsize:9<>18; flow:established,to_server; content:"|04 01
13 ba|"; depth:4; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode; reference:url,handlers.sans.org/wsalusky/rants/;
reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt; reference:url,ss5.sourceforge.net/socks4A.protocol.txt;
reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt; reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt;
reference:url,doc.emergingthreats.net/bin/view/Main/2003281; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003281; rev:5;)

#Another case of rules that fire according to RFC standards, but I haven't really witnessed this type of traffic to confirm.
#
#alert tcp $EXTERNAL_NET 1024:5000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv5 IPv6 Inbound Connect Request (Windows Source)"; dsize:10<>23; flow:established,to_server;
content:"|05 01 00 04|"; depth:4; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode; reference:url,handlers.sans.org/wsalusky/rants/;
reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt; reference:url,ss5.sourceforge.net/socks4A.protocol.txt;
reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt; reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt;
reference:url,doc.emergingthreats.net/bin/view/Main/2003284; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003284; rev:5;)

#Another case of rules that fire according to RFC standards, but I haven't really witnessed this type of traffic to confirm.
#
```

```
#alert tcp $EXTERNAL_NET 32768:61000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv5 IPv6 Inbound Connect Request (Linux Source)"; dsize:10<>23; flow:established,to_server;
content:"|05 01 00 04|"; depth:4; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode; reference:url,handlers.sans.org/wsalusky/rants/;
reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt; reference:url,ss5.sourceforge.net/socks4A.protocol.txt;
reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt; reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt;
reference:url,doc.emergingthreats.net/bin/view/Main/2003285; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003285; rev:5;)

#Another case of rules that fire according to RFC standards, but I haven't really witnessed this type of traffic to confirm.
#
alert udp $EXTERNAL_NET 1024:5000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv5 UDP Proxy Inbound Connect Request (Windows Source)"; content:"|00 00|"; depth:2; content:"|01|";
offset:3; depth:1; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode; reference:url,handlers.sans.org/wsalusky/rants/;
reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt; reference:url,ss5.sourceforge.net/socks4A.protocol.txt;
reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt; reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt;
reference:url,doc.emergingthreats.net/bin/view/Main/2003286; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003286; rev:6;)

#Another case of rules that fire according to RFC standards, but I haven't really witnessed this type of traffic to confirm.
#
alert udp $EXTERNAL_NET 32768:61000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv5 UDP Proxy Inbound Connect Request (Linux Source)"; content:"|00 00|"; depth:2; content:"|01|";
offset:3; depth:1; threshold:type both, track by_src, count 1, seconds 900; classtype:protocol-command-decode; reference:url,handlers.sans.org/wsalusky/rants/;
reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt; reference:url,ss5.sourceforge.net/socks4A.protocol.txt;
reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt; reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt;
reference:url,doc.emergingthreats.net/bin/view/Main/2003287; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003287; rev:5;)

#I keep these mostly commented, while they are correct according to RFC for BIND actions, in practice I've found only FP's which I still need to dig through and see what's really going
on there.
#
#alert tcp $EXTERNAL_NET 1024:5000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv4 Bind Inbound (Windows Source)"; dsize:9<>18; flow:established,to_server; content:"|04 02|"; depth:2;
classtype:protocol-command-decode; reference:url,handlers.sans.org/wsalusky/rants/; reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt;
reference:url,ss5.sourceforge.net/socks4A.protocol.txt; reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt;
reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt; reference:url,doc.emergingthreats.net/bin/view/Main/2003288;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003288; rev:5;)

#I keep these mostly commented, while they are correct according to RFC for BIND actions, in practice I've found only FP's which I still need to dig through and see what's really going
on there.
#
#alert tcp $EXTERNAL_NET 32768:61000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv4 Bind Inbound (Linux Source)"; dsize:9<>18; flow:established,to_server; content:"|04 02|"; depth:2;
classtype:protocol-command-decode; reference:url,handlers.sans.org/wsalusky/rants/; reference:url,en.wikipedia.org/wiki/SOCKS; reference:url,ss5.sourceforge.net/socks4.protocol.txt;
reference:url,ss5.sourceforge.net/socks4A.protocol.txt; reference:url,www.ietf.org/rfc/rfc1928.txt; reference:url,www.ietf.org/rfc/rfc1929.txt;
reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt; reference:url,doc.emergingthreats.net/bin/view/Main/2003289;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003289; rev:5;)

#I keep these mostly commented, while they are correct according to RFC for BIND actions, in practice I've found only FP's which I still need to dig through and see what's really going
on there.
#
#alert tcp $EXTERNAL_NET 32768:61000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv5 Bind Inbound (Linux Source)"; dsize:10; flow:established,to_server; content:"|05 02 00 01|";
depth:4; classtype:protocol-command-decode; reference:url,handlers.sans.org/wsalusky/rants/; reference:url,en.wikipedia.org/wiki/SOCKS;
reference:url,ss5.sourceforge.net/socks4.protocol.txt; reference:url,ss5.sourceforge.net/socks4A.protocol.txt; reference:url,www.ietf.org/rfc/rfc1928.txt;
reference:url,www.ietf.org/rfc/rfc1929.txt; reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt;
reference:url,doc.emergingthreats.net/bin/view/Main/2003290; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003290; rev:5;)

#I keep these mostly commented, while they are correct according to RFC for BIND actions, in practice I've found only FP's which I still need to dig through and see what's really going
on there.
#
#alert tcp $EXTERNAL_NET 1024:5000 -> $HOME_NET 1024:65535 (msg:"ET MALWARE SOCKSv5 Bind Inbound (Windows Source)"; dsize:10; flow:established,to_server; content:"|05 02 00 01|";
depth:4; classtype:protocol-command-decode; reference:url,handlers.sans.org/wsalusky/rants/; reference:url,en.wikipedia.org/wiki/SOCKS;
reference:url,ss5.sourceforge.net/socks4.protocol.txt; reference:url,ss5.sourceforge.net/socks4A.protocol.txt; reference:url,www.ietf.org/rfc/rfc1928.txt;
reference:url,www.ietf.org/rfc/rfc1929.txt; reference:url,www.ietf.org/rfc/rfc1961.txt; reference:url,www.ietf.org/rfc/rfc3089.txt;
reference:url,doc.emergingthreats.net/bin/view/Main/2003291; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Socks_Proxy; sid:2003291; rev:5;)

#matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Soft-Show.cn Related Fake AV Install"; flow:established,to_server; uricontent:"/setup/setup.asp?id="; nocase;
uricontent:"&pcid="; nocase; uricontent:"&ver="; nocase; uricontent:"&taday="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008135;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Soft-show.cn; sid:2008135; rev:2;)

#matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Soft-Show.cn Related Fake AV Install Ad Pull"; flow:established,to_server; uricontent:"/setup/adClick.asp?Id=";
nocase; uricontent:"&WebId="; nocase; uricontent:"&sDate="; nocase; uricontent:"&ver="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008148;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Soft-show.cn; sid:2008148; rev:2;)

#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Softcashier.com Spyware Install Checkin"; flow:established,to_server; uricontent:".php?wmid="; nocase;
uricontent:"&subid="; nocase; uricontent:"&pid="; nocase; uricontent:"&lid="; nocase; uricontent:"&hs="; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2007861; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Softcashier; sid:2007861; rev:2;)

#another fake antispyware package, by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Softspydelete.com Fake Anti-Spyware Checkin"; flow:established,to_server; uricontent:".php?"; nocase;
uricontent:"a1="; nocase; uricontent:"&a2="; nocase; uricontent:"&a3="; nocase; uricontent:"Windows%20version%20is"; nocase; uricontent:"&a4=Build"; nocase; uricontent:"&a5="; nocase;
uricontent:"&table="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007842; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Softspydelete.com; sid:2007842; rev:2;)

#by matt Jonkman, from the sandnet
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Softwarereferral.com Adware Checkin"; flow:established,to_server; uricontent:"wmid="; nocase; uricontent:"&mid=";
nocase; uricontent:"&lid="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007696; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Softwarereferral.com; sid:2007696; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024:65535 (msg:"ET USER_AGENTS Likely Spambot Web-based Control Traffic"; flow: to_server,established; content:"User-Agent|3a| Godzilla";
nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001711; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Spambots;
sid:2001711; rev:7;)

#The following rule assists in the identification of spam when SMTP 220
#responses are seen egressing your network from unusual src ports.
#You may want to consider tagging a number of following packets.
#
#alert tcp $HOME_NET !21:587 -> any any (msg:"ET MALWARE Spambot Suspicious 220 Banner on Local Port"; flow: established; content:"220 "; offset: 0; depth: 4; tag: session, 20, packets;
classtype: non-standard-protocol; reference:url,doc.emergingthreats.net/bin/view/Main/2001815; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Spambots;
sid:2001815; rev:8;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Possible Spambot Checking in to Spam"; flow:established,to_server; uricontent:"/devrandom/"; nocase; content:"dev";
nocase; content:!"User-Agent|3a|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002988; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Spambots; sid:2002988; rev:5;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Possible Spambot Pulling IP List to Spam"; flow:established,to_server; uricontent:"/devrandom/access.php"; nocase;
content:"User-Agent|3a| Mozilla/4.0 (compatible)"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002990;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Spambots; sid:2002990; rev:6;)

#Matt Jonkman
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Possible Spambot getting new exe url"; flow:established,to_server; uricontent:"404.txt"; nocase; content:"404";
content:!"User-Agent|3a|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002989; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Spambots; sid:2002989; rev:5;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Possible Spambot getting new exe"; flow:established,to_server; uricontent:"/traff/ppiigg.exe"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002991; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Spambots;
sid:2002991; rev:4;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Specificclick.net Spyware Activity"; flow: to_server,established; uricontent:"/adopt.sm?"; nocase; uricontent:"l=";
nocase; uricontent:"&sz="; nocase; uricontent:"&redir="; nocase; uricontent:"&nmv="; nocase; uricontent:"&nrsz="; nocase; uricontent:"&r="; nocase; classtype: policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2003450; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Specificclick.net; sid:2003450; rev:3;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Speedera Agent"; flow: to_server,established; uricontent:"/io/downloads"; nocase; classtype: trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2001320; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Speedera; sid:2001320; rev:5;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Speedera Agent (Specific)"; flow: to_server,established; uricontent:"/io/downloads/3/wsem302.dl"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001321; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Speedera;
sid:2001321; rev:5;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Spy-Not.com Spyware Updating"; flow:to_server,established; uricontent:"/updates1/SKVersion.ini"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003377; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Spy-not.com;
sid:2003377; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Spy-Not.com Spyware Pulling Fake Sigs"; flow:to_server,established; uricontent:"/updates1/SKSignatures.zip";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003375; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Spy-
not.com; sid:2003375; rev:3;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE SpySherriff Spyware Activity"; flow: to_server,established; uricontent:"/progs_exe/jbsrak/"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002984; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_SpySherriff;
sid:2002984; rev:4;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Jupitersatellites.biz Spyware Download"; flow: to_server,established; uricontent:"/traff/ppiigg.exe"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002987; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_SpySherriff;
sid:2002987; rev:4;)

#by Mr Magic Pants
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE SpySheriff Intial Phone Home"; flow:established,to_server; uricontent:"trial.php?rest="; nocase;
uricontent:"&ver="; nocase; uricontent:"&a="; nocase; content:"trial.php"; nocase; content:!"User-Agent|3a| "; classtype:trojan-activity;
reference:url,vil.nai.com/vil/content/v_135033.htm; reference:url,doc.emergingthreats.net/bin/view/Main/2003251; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_SpySherriff; sid:2003251; rev:5;)

#by Matt Jonkman, from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE SpyShredder Fake Anti-Spyware Install Download"; flow:established,to_server; uricontent:"&advid="; nocase;
uricontent:"&u="; nocase; uricontent:"&p="; nocase; uricontent:"?=______"; uricontent:"&vs="; nocase; uricontent:"&YZYYYYYYYYYYYYYYYYYYYYYYYYYY"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2007593; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_SpyShredder; sid:2007593; rev:3;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Spyaxe Spyware DB Update"; flow: to_server,established; uricontent:"/updates/database/dbver.php"; nocase;
content:"spywareaxe"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002804; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Spyaxe; sid:2002804; rev:4;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Spyaxe Spyware DB Version Check"; flow: to_server,established; uricontent:"/updates/database/dbver.dat"; nocase;
content:"spywareaxe"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002805; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Spyaxe; sid:2002805; rev:4;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Spyaxe Spyware Checkin"; flow: to_server,established; uricontent:"/download.php?sid="; nocase; content:"spyaxe";
nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002806; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Spyaxe;
sid:2002806; rev:4;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Spygalaxy.ws Activity"; flow: to_server,established; uricontent:"/install.php?id="; nocase; content:"Host|3a|
spygalaxy.ws"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001489; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Spygalaxy.ws; sid:2001489; rev:7;)

#from sandnet data
#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Spylog.ru Related Spyware Checkin"; flow:established,to_server; uricontent:"/cnt?"; nocase; uricontent:"cid=";
nocase; uricontent:"&p="; nocase; uricontent:"&rn="; nocase; uricontent:"&c="; nocase; uricontent:"&tl="; nocase; uricontent:"&ls="; nocase; uricontent:"&ln="; nocase; uricontent:"&t=";
nocase; uricontent:"&j="; nocase; uricontent:"&wh="; nocase; uricontent:"&px="; nocase; uricontent:"&sl="; nocase; uricontent:"&r="; nocase; uricontent:"&fr="; nocase;
uricontent:"&pg="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007649; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Spylog; sid:2007649; rev:3;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Spyspotter.com Install"; flow: to_server,established; uricontent:"/SpySpotterInstall.cab"; nocase; classtype:
trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001536; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Spyspotter.com; sid:2001536;
rev:7;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Spyspotter.com Access"; flow: to_server,established; content:"Host|3a| "; depth:200; content:"spyspotter.com|0d
0a|"; nocase; distance:0; within:30; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001537; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Spyspotter.com; sid:2001537; rev:13;)

#Submitted by Matt Jonkman
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE SpywareLabs VirtualBouncer Seeking Instructions"; flow: to_server,established; content:"instructions"; nocase;
pcre:"/instructions\/\d{2}\.xml/mi"; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.virtualbouncer.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2000587; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Spywarelabs_VirtualBouncer; sid:2000587;
rev:10;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE SpywareLabs Application Install"; flow: to_server,established; uricontent:"/DistID/BaseInstalls/V"; nocase;
content:"User-Agent|3a|"; nocase; content:"Wise"; within:120; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001522;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Spywarelabs_VirtualBouncer; sid:2001522; rev:12;)
```

```
#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Spyware Stormer Reporting Data"; flow: established,to_server; uricontent:"/showme.aspx?keyword="; nocase;
content:"ecomdata1="; nocase; classtype: trojan-activity; reference:url,www.spywarestormer.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001570;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Spywarestormer; sid:2001570; rev:7;)

#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Spyware Stormer/Error Guard Activity"; flow: established,to_server; uricontent:"/sell.cgi?errorguard/1/errorguard";
nocase; classtype: trojan-activity; reference:url,www.spywarestormer.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001571; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Spywarestormer; sid:2001571; rev:7;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Statblaster Receiving New configuration (update)"; flow: to_server,established; uricontent:"/updatestats/update";
nocase; uricontent:".xml"; nocase; classtype: policy-violation; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.statblaster.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001225; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Statblaster; sid:2001225; rev:8;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Statblaster Receiving New configuration (allfiles)"; flow: to_server,established;
uricontent:"/updatestats/all_files"; nocase; classtype: policy-violation; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.statblaster.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001523; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Statblaster; sid:2001523; rev:7;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Statblaster Code Download"; flow: to_server,established; uricontent:"/updatestats/"; nocase; uricontent:".exe";
nocase; classtype: policy-violation; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.statblaster.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001524;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Statblaster; sid:2001524; rev:6;)

#Submitted by Chris Norton
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Statblaster.MemoryWatcher Download"; flow: to_server,established; uricontent:"/memorywatcher.exe"; classtype:
trojan-activity; reference:url,www.memorywatcher.com/eula.aspx; reference:url,doc.emergingthreats.net/bin/view/Main/2001442; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Statblaster; sid:2001442; rev:9;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE SurfSidekick Activity"; flow: established,to_server; uricontent:"/Bundling/SskUpdater"; nocase; classtype: trojan-
activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.surfsidekick.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001731;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_SurfSidekick; sid:2001731; rev:6;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE SurfSidekick Download"; flow: established,to_server; uricontent:"/requestimpression.aspx?ver="; nocase;
content:"host="; nocase; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.surfsidekick.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001992; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_SurfSidekick; sid:2001992; rev:5;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE SurfSidekick Activity (ipixel)"; flow: established,to_server; uricontent:"/ipixel.htm?cid="; nocase;
content:"&pck_id="; nocase; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.surfsidekick.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001994; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_SurfSidekick; sid:2001994; rev:6;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE SurfSidekick Activity (rinfo)"; flow: established,to_server; uricontent:"/rinfo.htm?"; nocase; uricontent:"host=";
nocase; uricontent:"action="; nocase; uricontent:"client=SSK"; nocase; classtype: trojan-activity;
reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.surfsidekick.html; reference:url,doc.emergingthreats.net/bin/view/Main/2002738;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_SurfSidekick; sid:2002738; rev:3;)

#By Matt Jonkman from spywarelp data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE SurfAccuracy.com Spyware Updating"; flow:to_server,established; uricontent:"/sacc/sacc.cfg.php?"; nocase;
classtype:trojan-activity; reference:url,www.symantec.com/security_response/writeup.jsp?docid=2005-062716-0109-99; reference:url,doc.emergingthreats.net/bin/view/Main/2003390;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Surfaccuracy.com; sid:2003390; rev:3;)

#By Matt Jonkman from spywarelp data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE SurfAccuracy.com Spyware Pulling Ads"; flow:to_server,established; uricontent:"/sacc/popup.php"; nocase;
classtype:trojan-activity; reference:url,www.symantec.com/security_response/writeup.jsp?docid=2005-062716-0109-99; reference:url,doc.emergingthreats.net/bin/view/Main/2003391;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Surfaccuracy.com; sid:2003391; rev:3;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE SurfAssistant.com Spyware Install"; flow: to_server,established; uricontent:"/distribution/questmod-1.dll"; nocase;
classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.sa.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001510;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Surfassistant.com; sid:2001510; rev:7;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE SurfAssistant.com Spyware Reporting"; flow: to_server,established; uricontent:"/sa/?a="; nocase; classtype: trojan-
activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.sa.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001514;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Surfassistant.com; sid:2001514; rev:8;)

#fake av, sig by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE System-defender.com Fake AV Install Checkin"; flow:established,to_server; uricontent:"?wmid="; nocase;
uricontent:"&mid="; nocase; uricontent:"&lndid="; nocase; classtype:trojan-activity; reference:url,www.system-defender.com; reference:url,doc.emergingthreats.net/bin/view/Main/2007856;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_System-defender.com; sid:2007856; rev:2;)

#fake av package, sigs by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE SysVenFak Fake AV Package User-Agent (gh2008)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| gh20";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007944; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Sysvenfak;
sid:2007944; rev:3;)

#fake av package, sigs by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE SysVenFak Fake AV Package Victim Checkin (victim.php)"; flow:established,to_server; uricontent:"/victim.php?";
pcre:"/victim\.php\?\d\d\d\d\d\d/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007945; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Sysvenfak; sid:2007945; rev:2;)

#By Matt Jonkman from spyware lp data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Sytes.net Related Spyware Reporting"; flow:to_server,established; uricontent:"/Reporting/admin/upload.php"; nocase;
content:"POST "; depth:5; nocase; content:"sytes.net"; nocase; classtype:trojan-activity; reference:url,www.sophos.com/security/analyses/w32forbotdv.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2003533; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Sytes.net; sid:2003533; rev:4;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE TargetNetworks.net Spyware Reporting (req)"; flow: to_server,established; uricontent:"/request/req.cgi?gu=";
nocase; uricontent:"&sid="; nocase; uricontent:"&kw="; nocase; classtype: trojan-activity; reference:url,www.targetnetworks.com;
reference:url,doc.emergingthreats.net/bin/view/Main/2001997; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_TargetNetworks.net; sid:2001997; rev:6;)

#Matt Jonkman
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE TargetNetworks.net Spyware Reporting (tn)"; flow: to_server,established; uricontent:"/data/tn.dat?v="; nocase;
uricontent:"&sid="; nocase; classtype: trojan-activity; reference:url,www.targetnetworks.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002046;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_TargetNetworks.net; sid:2002046; rev:6;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE thebestsoft4u.com Spyware Install (1)"; flow: to_server,established; uricontent:"/pa/glx.exe"; nocase; classtype:
trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001482; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Thebestsoft4u; sid:2001482;
rev:6;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE thebestsoft4u.com Spyware Install (2)"; flow: to_server,established; uricontent:"/pa/proxyrnd.exe"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001485; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Thebestsoft4u;
sid:2001485; rev:6;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE thebestsoft4u.com Spyware Install (3)"; flow: to_server,established; uricontent:"/pr.exe"; nocase; classtype:
trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001486; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Thebestsoft4u; sid:2001486;
rev:6;)

#horrendous multi-install service at theinstalls.com
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Theinstalls.com Initial Checkin"; flow:established,to_server; uricontent:"/plist.php?uid="; content:"|0d
0a|Host|3a| "; content:"theinstalls.com|0d 0a|"; within:23; classtype:trojan-activity; reference:url,www.theinstalls.com; reference:url,doc.emergingthreats.net/bin/view/Main/2007788;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Theinstalls.com; sid:2007788; rev:3;)

#horrendous multi-install service at theinstalls.com
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Theinstalls.com Trojan Download"; flow:established,to_server; uricontent:"/files/programs/"; content:"|0d
0a|Host|3a| "; content:"theinstalls.com|0d 0a|"; within:23; classtype:trojan-activity; reference:url,www.theinstalls.com; reference:url,doc.emergingthreats.net/bin/view/Main/2007798;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Theinstalls.com; sid:2007798; rev:3;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Tibsystems Spyware Download"; flow: to_server,established; uricontent:"/d4.fcgi?v="; nocase; classtype: trojan-
activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001488; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Tibsystems.com; sid:2001488; rev:7;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Tibsystems Spyware Install (1)"; flow: to_server,established; uricontent:"/fcgi-bin/iza2.fcgi?m="; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001729; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Tibsystems.com;
sid:2001729; rev:5;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Tibsystems Spyware Install (2)"; flow: to_server,established; uricontent:"/tb/loader2.ocx"; nocase; classtype:
trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001734; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Tibsystems.com; sid:2001734;
rev:5;)

#by Russ McRee
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET DELETED Trojan.Downloader.Time2Pay.AQ"; flow:established,to_server; uricontent:"/progs_traff/"; nocase; classtype:trojan-
activity; reference:url,research.sunbelt-software.com; reference:url,doc.emergingthreats.net/bin/view/Main/2003034; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Time2Pay; sid:2003034; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE ToolbarPartner Spyware Agent Download (1)"; flow: established,to_server; uricontent:"/ldr.exe"; nocase; classtype:
trojan-activity; reference:url,toolbarpartner.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001890; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_ToolBarPartner; sid:2001890; rev:7;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE ToolbarPartner Spyware Spambot Retrieving Target Emails"; flow: established,to_server; uricontent:"/mailz.php?id=";
nocase; classtype: trojan-activity; reference:url,toolbarpartner.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001895; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_ToolBarPartner; sid:2001895; rev:6;)

#Submitted by Matt Jonkman
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE TopMoxie Reporting Data to External Host"; flow: to_server,established; content:"/downloads/record_download.asp";
nocase; pcre:"/(GET |GET (http|https)\:\/\/[-0-9a-z.]*)\/downloads\/record_download\.asp/i"; classtype: trojan-activity; reference:url,www.topmoxie.com;
reference:url,doc.emergingthreats.net/bin/view/Main/2000588; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_TopMoxie; sid:2000588; rev:10;)

#Submitted by Matt Jonkman
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE TopMoxie Retrieving Data (downloads)"; flow: to_server,established; uricontent:"/external/builds/downloads2/";
nocase; classtype: trojan-activity; reference:url,www.topmoxie.com; reference:url,doc.emergingthreats.net/bin/view/Main/2000589; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_TopMoxie; sid:2000589; rev:8;)

#Submitted by Matt Jonkman
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE TopMoxie Retrieving Data (common)"; flow: to_server,established; uricontent:"/external/builds/common/"; nocase;
classtype: trojan-activity; reference:url,www.topmoxie.com; reference:url,doc.emergingthreats.net/bin/view/Main/2000590; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_TopMoxie; sid:2000590; rev:8;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Toprebates.com Install (1)"; flow: established,to_server; uricontent:"/acti.asp?cl=1&gd=1&clpid="; nocase;
classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.webrebates.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001646;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_TopRebates; sid:2001646; rev:6;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Toprebates.com Install (2)"; flow: established,to_server; uricontent:"/builds/"; nocase;
uricontent:"AutoTrack_Install.exe"; nocase; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.webrebates.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001647; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_TopRebates; sid:2001647; rev:6;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Toprebates.com User Confirming Membership"; flow: established,to_server; uricontent:"/cgi/account.plx?pid=";
nocase; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.webrebates.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001648;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_TopRebates; sid:2001648; rev:5;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Ezula"; flow: to_server,established; uricontent:"/MindSet5/install/ezinstall.exe"; 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/bin/view/Main/2001334;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_TopText_ILookup; sid:2001334; rev:6;)

#Submitted by Matt Jonkman
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET MALWARE Ezula Installer Download"; flow: from_server,established; content:"|65 5a 75 6c 61 20 49 6e 73 74 61 6c 6c 61 74 69
6f 6e 00 49|"; classtype: trojan-activity; reference:url,www.ezula.com; reference:url,www.spyany.com/program/article_spw_rm_eZuLa.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001335; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_TopText_ILookup; sid:2001335; rev:7;)

#By Matt Jonkman
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Spywaremover Activity"; flow: to_server,established; uricontent:"/spywareremovers.php?"; content:"Host|3a|
topantispyware.com"; nocase; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/adware.topantispyware.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001520; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Topantispyware.com; sid:2001520; rev:8;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Topconverting Spyware Install"; flow: to_server,established; uricontent:"/activex/weirdontheweb_topc.exe"; nocase;
classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/pf/adware.180search.html; reference:url,doc.emergingthreats.net/bin/view/Main/2002004;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Topconverting.com; sid:2002004; rev:6;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Topconverting Spyware Reporting"; flow: to_server,established; uricontent:"/trigger.php?partner="; nocase;
classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/pf/adware.180search.html; reference:url,doc.emergingthreats.net/bin/view/Main/2002040;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Topconverting.com; sid:2002040; rev:5;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Topgame-online.com Ruch Casino Install User-Agent (RichCasino)"; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| RichCasino"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009831; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Topgame-online.com; sid:2009831; rev:3;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Traffic Syndicate Add/Remove"; flow: to_server,established; uricontent:"/Support/AddRemove.aspx?id="; nocase;
classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2001313; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_TrafficSyndicate;
sid:2001313; rev:6;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Traffic Syndicate Agent Updating (1)"; flow: to_server,established; uricontent:"/TbLinkConfig.asmx"; nocase;
threshold: type limit, track by_src, count 1, seconds 360; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2001315;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_TrafficSyndicate; sid:2001315; rev:8;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Traffic Syndicate Agent Updating (2)"; flow: to_server,established; uricontent:"/TbInstConfig.asmx"; nocase;
threshold: type limit, track by_src, count 1, seconds 360; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2001316;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_TrafficSyndicate; sid:2001316; rev:8;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Trafficsector.com Spyware Install"; flow: to_server,established; uricontent:"/install.php?"; nocase;
uricontent:"afid="; nocase; uricontent:"&user_id="; content:"trafficsector"; nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002736;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Trafficsector; sid:2002736; rev:3;)

#by Matt Jonkman, data from the Spyware Listening Post
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Transponder Spyware Activity"; flow:established,to_server; uricontent:"/sendROIcookie.cfm?refer="; nocase;
classtype:trojan-activity; reference:url,www.doxdesk.com/parasite/Transponder.html; reference:url,doc.emergingthreats.net/bin/view/Main/2002320;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Transponder; sid:2002320; rev:3;)

#by Matt Jonkman, from Spyware LP Hits
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Travel Update Spyware"; flow:established,to_server; uricontent:"/abt?data="; nocase; pcre:"/\/abt\?
data=\S{150}/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003297; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Travel_Update; sid:2003297; rev:3;)

#by cjeremy
#ref: 2aebe5fa5c98589bd0f169f9013715b8
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Adware/Spyware Trymedia.com EXE download"; flow:established,to_server; content:"GET "; depth:4; uricontent:".exe?
nva="; uricontent:"&aff="; uricontent:"&token="; content:"User-Agent|3a| Macrovision_DM"; nocase; classtype:policy-violation; reference:url,www.browserdefender.com/site/trymedia.com;
reference:url,www.threatexpert.com/reports.aspx?find=Adware.Trymedia; reference:url,doc.emergingthreats.net/2009091; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Trymedia; sid:2009091; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE UCMore Spyware Reporting"; flow: to_server,established; uricontent:"/iis2ucms.asp"; nocase; classtype: trojan-
activity; reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=58660; reference:url,doc.emergingthreats.net/bin/view/Main/2001995; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_UCmore; sid:2001995; rev:5;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE UCMore Spyware Downloading Ads"; flow: to_server,established; uricontent:"/iis2ucms_getsponsorlinks.asp"; nocase;
classtype: trojan-activity; reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=58660; reference:url,doc.emergingthreats.net/bin/view/Main/2001998;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_UCmore; sid:2001998; rev:5;)

#Added by Frank Knobbe on 2006-03-12
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Suspicious POST to ROBOTS.TXT"; flow:established,to_server; content:"POST "; depth:5; nocase;
uricontent:"/robots.txt"; nocase; pcre:"/Cookie\:\ +x=[0-9]*\;\ +y=[0-9]+/i"; classtype:unknown; reference:url,doc.emergingthreats.net/bin/view/Main/2002856;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Unknown; sid:2002856; rev:5;)

#Added by Frank Knobbe on 2006-07-02
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE /jk/exp.wmf Exploit Code Load Attempt"; flow:to_server,established; uricontent:"/jk/exp.wmf"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002999; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Unknown;
sid:2002999; rev:3;)

#Added by Frank Knobbe on 2006-07-02
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE PopupSh.ocx Access Attempt"; flow:to_server,established; uricontent:"/PopupSh.ocx"; nocase; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003000; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Unknown; sid:2003000; rev:4;)

#Matt Jonkman
#This appears to be a controller the above trojan uses
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Unknown Web Bot Controller Accessed"; flow:to_server,established; uricontent:"/stata/index.php?tr=ok"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003025; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Unknown;
sid:2003025; rev:3;)

#by L0rd Ch0de1m0rt
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Unknown Malware Download Request"; flow:established,to_server; content:"GET "; depth:4; nocase;
uricontent:"/images/GR_OLD_CR.EXE"; nocase; classtype:trojan-activity; reference:url,www.prevx.com/filenames/X22210989379038527-X1/GR_OLD_CR.EXE.html;
reference:url,doc.emergingthreats.net/2011148; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Unknown; sid:2011148; rev:2;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Sidelinker.com-Upspider.com Spyware Checkin"; flow:established,to_server; uricontent:"/Pro/pro.php?mac="; nocase;
uricontent:"&key="; nocase; pcre:"/\/Pro\/pro\.php\?mac=\d\d-\d\d-\d\d-\d\d-\d\d-\d\d\&key=\d+/Ui"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2008157; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Upspider.com-Sidelinker.com; sid:2008157;
rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Sidelinker.com-Upspider.com Spyware Count"; flow:established,to_server; uricontent:"/Pro/cnt.php?mac="; nocase;
```

```
uricontent:"&key="; nocase; uricontent:"&pid="; nocase; pcre:"/\/Pro\/cnt\.php\?mac=\d\d-\d\d-\d\d-\d\d-\d\d-\d\d\&key=\d+/Ui"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2008158; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Upspider.com-Sidelinker.com; sid:2008158;
rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE V-Clean.com Fake AV Checkin"; flow:established,to_server; uricontent:"/bill_mod/bill_count.php?C_FLAG=";
content:"|0d 0a|User-Agent|3a| Mozilla/4.0 (compatible|3b| MSIE 5.5|3b| Windows 98)|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008180;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_V-clean.com; sid:2008180; rev:3;)

#by Matt Jonkman from Listening Post Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE VPP Technologies Spyware"; flow:established,to_server; uricontent:"/DittoIA.jsh?pid="; nocase; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002348; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_VPPTechnologies; sid:2002348;
rev:3;)

#by Matt Jonkman from Listening Post Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE VPP Technologies Spyware Reporting URL"; flow:established,to_server; uricontent:"/js.vppimage?key="; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2002350; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_VPPTechnologies;
sid:2002350; rev:3;)

#by victor julien
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Vaccine-program.co.kr Related Spyware Checkin"; flow:established,to_server; content:"GET "; depth:4;
uricontent:"/version/controllerVersion"; nocase; content:"|0d 0a|User-Agent|3a| Mozilla/3.0 (compatible|3b| Indy Library)|0d 0a|"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2007995; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Vaccine-program.co.kr; sid:2007995; rev:3;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Virtumonde Spyware siae3123.exe GET"; flow: to_server,established; uricontent:"siae3123.exe"; nocase; classtype:
trojan-activity; reference:url,sarc.com/avcenter/venc/data/adware.virtumonde.html; reference:url,doc.emergingthreats.net/bin/view/Main/2000306;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Virtumonde; sid:2000306; rev:27;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 8081 (msg:"ET MALWARE Virtumonde Spyware siae3123.exe GET (8081)"; flow: to_server,established; uricontent:"siae3123.exe"; nocase; classtype:
trojan-activity; reference:url,sarc.com/avcenter/venc/data/adware.virtumonde.html; reference:url,doc.emergingthreats.net/bin/view/Main/2000307;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Virtumonde; sid:2000307; rev:24;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Virtumonde Spyware Information Post"; flow: to_server,established; content:"POST "; nocase;
content:"e_g_StatisticsUploadDelay"; nocase; content:"g_AffiliateID"; nocase; content:"virtumonde.com"; classtype: trojan-activity;
reference:url,sarc.com/avcenter/venc/data/adware.virtumonde.html; reference:url,doc.emergingthreats.net/bin/view/Main/2000308; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Virtumonde; sid:2000308; rev:22;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Virtumonde Spyware Code Download mmdom.exe"; flow: to_server,established; uricontent:"/mmdom.exe"; nocase;
classtype: trojan-activity; reference:url,sarc.com/avcenter/venc/data/adware.virtumonde.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001525;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Virtumonde; sid:2001525; rev:7;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Virtumonde Spyware Code Download bkinst.exe"; flow: to_server,established; uricontent:"/bkinst.exe"; nocase;
content:"virtumonde.com"; classtype: trojan-activity; reference:url,www.lurhq.com/iframeads.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001526;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Virtumonde; sid:2001526; rev:21;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Vombanetworks.com Spyware Installer Checkin"; flow:established,to_server; content:"POST "; depth:5;
uricontent:"/scripts/get_cookie.php"; nocase; content:"|0d 0a 0d 0a|vomba="; content:"&ff="; content:"&vombashots="; content:"&vombashots_ff="; content:"&hwd="; content:"&ver=";
content:"&vinfo=Windows"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2007870; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Vombanetwork.com; sid:2007870; rev:2;)

#Weatherbug - Dale Handy, PE
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Weatherbug"; flow: to_server,established; uricontent:"WxAlertIsapi"; nocase; threshold: type limit, track by_src,
count 1, seconds 3600; classtype: misc-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001235; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Weatherbug; sid:2001235; rev:11;)

#Submitted by Joel Esler
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Weatherbug Capture"; flow: to_server,established; content:"GET"; nocase; content:"Host|3a|"; nocase; within: 500;
content:"weatherbug.com"; nocase; within: 100; threshold: type limit, track by_src, count 1, seconds 3600; classtype: misc-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2001267; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Weatherbug; sid:2001267; rev:15;)

#by M Shirk
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Weatherbug Wxbug Capture"; flow: to_server,established; content:"GET"; nocase; content:"Host|3a|"; nocase; within:
500; content:"wxbug.com"; nocase; within: 100; threshold: type limit, track by_src, count 1, seconds 3600; classtype: misc-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2002364; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Weatherbug; sid:2002364; rev:5;)

#from spywarelp data, by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Weatherbug Activity"; flow:established,to_server; uricontent:"/WeatherWindow/WeatherWindow"; nocase; uricontent:"?
rnd="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003420; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Weatherbug; sid:2003420; rev:3;)

#from spywarelp data, by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Weatherbug Design60 Upload Activity"; flow:established,to_server; uricontent:"/GetDesign60.aspx?Magic="; nocase;
uricontent:"?ZipCode="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003421; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Weatherbug; sid:2003421; rev:3;)

#from spywarelp data, by Matt Jonkman
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET DELETED Weatherbug Design60 Upload Activity"; flow:established,to_server; uricontent:"/GetDesign60.aspx?Magic="; nocase;
uricontent:"?ZipCode="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003423; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Weatherbug; sid:2003423; rev:3;)

#from spywarelp data, by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Weatherbug Command Activity"; flow:established,to_server; uricontent:"/connection/connectionv"; nocase;
uricontent:"?t="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003422; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Weatherbug; sid:2003422; rev:3;)

#from spywarelp data, by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Weatherbug Vista Gadget Activity"; flow:established,to_server; uricontent:"/Command/VistaGadget_v"; nocase;
uricontent:"UserId="; nocase; uricontent:"&AppVersion="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003534;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Weatherbug; sid:2003534; rev:3;)

#by Matt Jonkman, from Spyware Listening Post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Webbuying.net Spyware Installing"; flow:established,to_server; uricontent:"/inst.php?"; nocase; uricontent:"d=";
nocase; uricontent:"&cl="; nocase; uricontent:"&l="; nocase; uricontent:"&e="; nocase; uricontent:"&v=wbi_v"; nocase; uricontent:"&uid="; nocase; uricontent:"&time="; nocase;
```

```
uricontent:"&win="; nocase; uricontent:"&un=0"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003442;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Webbuying.net; sid:2003442; rev:3;)

#Submitted by Matt Jonkman, Tweaks by Bob Grabowsky
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET MALWARE Webhancer Data Upload"; flow: from_server,established; content:"WebHancer Authority Server"; nocase; classtype:
trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/spyware.webhancer.html; reference:url,doc.emergingthreats.net/bin/view/Main/2001317;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Webhancer; sid:2001317; rev:8;)

#Submitted by Matt Jonkman, Tweaks by Bob Grabowsky
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Webhancer Data Post"; flow: to_server,established; content:"POST http|3a|//prime.webhancer.com"; nocase;
content:"AgentTag|3a|"; nocase; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/spyware.webhancer.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001677; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Webhancer; sid:2001677; rev:11;)

#Submitted by Matt Jonkman, Tweaks by Bob Grabowsky
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Webhancer Agent Activity"; flow: to_server,established; content:"Host|3a|"; nocase; content:"webhancer.com";
within:30; nocase; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/spyware.webhancer.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2001678; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Webhancer; sid:2001678; rev:10;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Websearch.com Spyware"; flow: to_server,established; uricontent:"/sitereview.asmx/GetReview"; nocase; classtype:
trojan-activity; reference:mcafee,131461; reference:url,doc.emergingthreats.net/bin/view/Main/2001325; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Websearch.com; sid:2001325; rev:8;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Websearch.com Outbound Dialer Retrieval"; flow: to_server,established; uricontent:"/1/rdgUS10.exe"; nocase;
classtype: trojan-activity; reference:mcafee,131461; reference:url,doc.emergingthreats.net/bin/view/Main/2001517; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Websearch.com; sid:2001517; rev:7;)

#Matt Jonkman, from spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Websearch.com Cab Download"; flow: to_server,established; uricontent:"/Dnl/T_"; nocase; pcre:"/\/\S+\.cab/Ui";
classtype: trojan-activity; reference:mcafee,131461; reference:url,doc.emergingthreats.net/bin/view/Main/2003242; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Websearch.com; sid:2003242; rev:7;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Weird on the Web /180 Solutions Checkin"; flow: to_server,established; uricontent:"/notifier/config.ini?v=";
nocase; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/pf/adware.180search.html; reference:url,doc.emergingthreats.net/bin/view/Main/2002036;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Weirdontheweb; sid:2002036; rev:5;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Weird on the Web /180 Solutions Update"; flow: to_server,established; uricontent:"/notifier/updates"; nocase;
classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/pf/adware.180search.html; reference:url,doc.emergingthreats.net/bin/view/Main/2002041;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Weirdontheweb; sid:2002041; rev:5;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE WhenUClick.com App and Search Bar Install (1)"; flow: to_server,established; uricontent:"/vsn/ISA/"; nocase;
classtype: policy-violation; reference:url,www.whenusearch.com; reference:url,www.kephyr.com/spywarescanner/library/whenusearch/index.phtml;
reference:url,doc.emergingthreats.net/bin/view/Main/2000908; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_WhenUSearch.com; sid:2000908; rev:10;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE WhenUClick.com App and Search Bar Install (2)"; flow: to_server,established; uricontent:"/Appinstall?app=VVSN";
nocase; classtype: policy-violation; reference:url,www.whenusearch.com; reference:url,www.kephyr.com/spywarescanner/library/whenusearch/index.phtml;
reference:url,doc.emergingthreats.net/bin/view/Main/2000909; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_WhenUSearch.com; sid:2000909; rev:9;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE WhenUClick.com Clock Sync App Checkin"; flow: to_server,established; uricontent:"/heartbeat?"; nocase;
uricontent:"=clock"; nocase; classtype: policy-violation; reference:url,www.whenusearch.com; reference:url,www.kephyr.com/spywarescanner/library/whenusearch/index.phtml;
reference:url,doc.emergingthreats.net/bin/view/Main/2000910; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_WhenUSearch.com; sid:2000910; rev:9;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE WhenUClick.com Weather App Checkin"; flow: to_server,established; uricontent:"/heartbeat?"; nocase;
uricontent:"=weather"; nocase; classtype: policy-violation; reference:url,www.whenusearch.com; reference:url,www.kephyr.com/spywarescanner/library/whenusearch/index.phtml;
reference:url,doc.emergingthreats.net/bin/view/Main/2000911; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_WhenUSearch.com; sid:2000911; rev:9;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE WhenUClick.com Clock Sync App Checkin (1)"; flow: to_server,established; uricontent:"/clock?id="; nocase;
classtype: policy-violation; reference:url,www.whenusearch.com; reference:url,www.kephyr.com/spywarescanner/library/whenusearch/index.phtml;
reference:url,doc.emergingthreats.net/bin/view/Main/2000912; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_WhenUSearch.com; sid:2000912; rev:9;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE WhenUClick.com Clock Sync App Checkin (2)"; flow: to_server,established; uricontent:"/clockDB"; nocase; classtype:
policy-violation; reference:url,www.whenusearch.com; reference:url,www.kephyr.com/spywarescanner/library/whenusearch/index.phtml;
reference:url,doc.emergingthreats.net/bin/view/Main/2000913; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_WhenUSearch.com; sid:2000913; rev:9;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE WhenUClick.com Weather App Checkin (1)"; flow: to_server,established; uricontent:"/weatherDB"; nocase; classtype:
policy-violation; reference:url,www.whenusearch.com; reference:url,www.kephyr.com/spywarescanner/library/whenusearch/index.phtml;
reference:url,doc.emergingthreats.net/bin/view/Main/2000914; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_WhenUSearch.com; sid:2000914; rev:9;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE WhenUClick.com Weather App Checkin (2)"; flow: to_server,established; uricontent:"/weather?id="; nocase; classtype:
policy-violation; reference:url,www.whenusearch.com; reference:url,www.kephyr.com/spywarescanner/library/whenusearch/index.phtml;
reference:url,doc.emergingthreats.net/bin/view/Main/2000915; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_WhenUSearch.com; sid:2000915; rev:9;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE WhenUClick.com WhenUSave App Checkin"; flow: to_server,established; uricontent:"/heartbeat?"; nocase;
uricontent:"=whenusave"; nocase; classtype: policy-violation; reference:url,www.whenusearch.com; reference:url,www.kephyr.com/spywarescanner/library/whenusearch/index.phtml;
reference:url,doc.emergingthreats.net/bin/view/Main/2000916; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_WhenUSearch.com; sid:2000916; rev:9;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE WhenUClick.com WhenUSave Data Retrieval (offersdata)"; flow: to_server,established; uricontent:"/OffersDataGZ?
update="; nocase; classtype: policy-violation; reference:url,www.whenusearch.com; reference:url,www.kephyr.com/spywarescanner/library/whenusearch/index.phtml;
reference:url,doc.emergingthreats.net/bin/view/Main/2000917; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_WhenUSearch.com; sid:2000917; rev:9;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE WhenUClick.com Desktop Bar Install"; flow: to_server,established; uricontent:"/Appinstall?app=desktop"; nocase;
classtype: policy-violation; reference:url,www.whenusearch.com; reference:url,www.kephyr.com/spywarescanner/library/whenusearch/index.phtml;
reference:url,doc.emergingthreats.net/bin/view/Main/2000918; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_WhenUSearch.com; sid:2000918; rev:8;)

#Submitted by Matt Jonkman
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE WhenUClick.com WhenUSave Data Retrieval (Searchdb)"; flow: to_server,established; uricontent:"/SearchDB?update=";
nocase; classtype: policy-violation; reference:url,www.whenusearch.com; reference:url,www.kephyr.com/spywarescanner/library/whenusearch/index.phtml;
reference:url,doc.emergingthreats.net/bin/view/Main/2000919; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_WhenUSearch.com; sid:2000919; rev:9;)

#Submitted by Chris Norton
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE WhenUClick.com Desktop Bar App Checkin"; flow: to_server,established; uricontent:"/heartbeat?"; nocase;
uricontent:"=desktop"; nocase; classtype: policy-violation; reference:url,www.whenusearch.com; reference:url,www.kephyr.com/spywarescanner/library/whenusearch/index.phtml;
reference:url,doc.emergingthreats.net/bin/view/Main/2001443; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_WhenUSearch.com; sid:2001443; rev:8;)

#Matt Jonkman from spywarelp data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE WhenUClick.com Application Version Check"; flow: to_server,established; uricontent:"/versions.html"; nocase;
content:"whenu.com"; nocase; classtype: policy-violation; reference:url,www.whenusearch.com; reference:url,www.kephyr.com/spywarescanner/library/whenusearch/index.phtml;
reference:url,doc.emergingthreats.net/bin/view/Main/2003389; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_WhenUSearch.com; sid:2003389; rev:4;)

#Matt Jonkman from spywarelp data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE WhenUClick.com WhenUSave Data Retrieval (DataChunksGZ)"; flow: to_server,established; uricontent:"/DataChunksGZ?
update="; nocase; uricontent:"ver="; nocase; uricontent:"svr="; nocase; classtype: policy-violation; reference:url,www.whenusearch.com;
reference:url,www.kephyr.com/spywarescanner/library/whenusearch/index.phtml; reference:url,doc.emergingthreats.net/bin/view/Main/2003404; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_WhenUSearch.com; sid:2003404; rev:4;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Wild Tangent Agent Installation"; flow: to_server,established; uricontent:"/Recovery/Checkin.aspx?version"; nocase;
classtype: trojan-activity; reference:url,www.spyany.com/program/article_spw_rm_WildTangent.html; reference:url,www.wildtangent.com;
reference:url,doc.emergingthreats.net/bin/view/Main/2001307; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Wild_Tangent; sid:2001307; rev:6;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Wild Tangent Agent Checking In"; flow: to_server,established; uricontent:"/CDADeliveries/Checkin.aspx"; nocase;
classtype: trojan-activity; reference:url,www.spyany.com/program/article_spw_rm_WildTangent.html; reference:url,www.wildtangent.com;
reference:url,doc.emergingthreats.net/bin/view/Main/2001309; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Wild_Tangent; sid:2001309; rev:6;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Wild Tangent Agent Traffic"; flow: to_server,established; uricontent:"/CDAFiles/DP/SysConfig"; nocase; classtype:
trojan-activity; reference:url,www.spyany.com/program/article_spw_rm_WildTangent.html; reference:url,www.wildtangent.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001310;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Wild_Tangent; sid:2001310; rev:6;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Wild Tangent Agent"; flow: to_server,established; uricontent:"/CDAFiles/"; nocase; classtype: trojan-activity;
reference:url,www.spyany.com/program/article_spw_rm_WildTangent.html; reference:url,www.wildtangent.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001314;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Wild_Tangent; sid:2001314; rev:6;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Wild Tangent New Install"; flow: to_server,established; uricontent:"/NewUser/Checkin.aspx"; nocase; classtype:
trojan-activity; reference:url,www.spyany.com/program/article_spw_rm_WildTangent.html; reference:url,www.wildtangent.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001322;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Wild_Tangent; sid:2001322; rev:6;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Wild Tangent Install"; flow: to_server,established; uricontent:"/updatestats/AI_Euro.exe"; nocase; classtype:
trojan-activity; reference:mcafee,122249; reference:url,doc.emergingthreats.net/bin/view/Main/2002008; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Wildmedia; sid:2002008; rev:8;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Windupdates.com Spyware Install"; flow: established,to_server; uricontent:"/cab/CDTInc/ie/"; nocase;
uricontent:".cab"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001700; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Windupdates.com; sid:2001700; rev:7;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Windupdates.com Spyware Loggin Data"; flow: established,to_server; uricontent:"/logging.php?p="; nocase;
content:"Host|3a| public.windupdates.com"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001701; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Windupdates.com; sid:2001701; rev:7;)

#By Matt Jonkman from spyware listening post data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Winfixmaster.com Fake Anti-Spyware Install"; flow: to_server,established; uricontent:"/dispatcher.php?action=";
nocase; content:"Host|3a| www.winfix"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003543; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Winfixmaster.com; sid:2003543; rev:4;)

#Matt jonkman from Spyware LP Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Winferno Registry Fix Spyware Download"; flow: to_server,established;
uricontent:"/freeze_rpc6bundle_us/REGISTRYFIXDLL.exe"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003353;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Wininferno.com; sid:2003353; rev:3;)

#Matt jonkman from Spyware LP Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Freeze.com Spyware Download"; flow: to_server,established; uricontent:"/WebServices/DesktopManager/"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003356; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Wininferno.com;
sid:2003356; rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Winquickupdates.com/Mycashloads.com Related Trojan Install Report"; flow:established,to_server;
uricontent:"/newuser.php?saff="; pcre:"/\/newuser\.php.saff=(\d+|x.+)/U"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2008012;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Winquickupdates.com; sid:2008012; rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Winreanimator.com Fake AV Install Attempt"; flow:established,to_server; uricontent:"/inst.php?wmid="; nocase;
uricontent:"&p="; nocase; uricontent:"&l="; nocase; uricontent:"&s="; nocase; classtype:trojan-activity; reference:url,www.winreanimator.com;
reference:url,doc.emergingthreats.net/bin/view/Main/2007865; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Winreanimator.com; sid:2007865; rev:2;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Winsoftware.com Spyware Activity"; flow: to_server,established; uricontent:"/?proto="; nocase; uricontent:"&rc=";
nocase; uricontent:"&abbr="; nocase; uricontent:"platform="; nocase; uricontent:"&os_version="; nocase; uricontent:"&appid="; nocase; classtype: trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2003471; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Winsoftware.com; sid:2003471; rev:4;)

#matt jonkman, www.winxdefender.com fake AV package
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Winxdefender.com Fake AV Package Post Install Checkin"; flow:established,to_server; content:"POST "; depth:5;
uricontent:"/checkupdate.php"; nocase; content:"|0d 0a|User-Agent|3a| Opera"; content:"Computer ID|3a| "; distance:0; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2008197; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Winxdefender.com; sid:2008197; rev:4;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Xpire.info Multiple Spyware Installs (1)"; flow: to_server,established; uricontent:"/fa/evil.html"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001461; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Xpire.info;
sid:2001461; rev:8;)
```

```
#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Xpire.info Multiple Spyware Installs Occuring"; flow: to_server,established; uricontent:"/fa/?d=get"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001462; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Xpire.info;
sid:2001462; rev:7;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Xpire.info Multiple Spyware Installs (2)"; flow: to_server,established; content:"src=http|3a|//xpire.info/i.exe";
nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001463; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Xpire.info; sid:2001463; rev:9;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Xpire.info Multiple Spyware Installs (3)"; flow: to_server,established; uricontent:"/i.exe"; nocase;
content:"xpire.info"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001464; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Xpire.info; sid:2001464; rev:8;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Xpire.info Multiple Spyware Installs (4)"; flow: to_server,established; uricontent:"/dl/adv121.php"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001466; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Xpire.info;
sid:2001466; rev:8;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Xpire.info Multiple Spyware Installs (5)"; flow: to_server,established; uricontent:"/dl/adv121/x.chm"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001467; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Xpire.info;
sid:2001467; rev:8;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Xpire.info Multiple Spyware Installs CHM Exploit"; flow: to_server,established; uricontent:"/fa/ied_s7m.chm";
nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001468; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Xpire.info; sid:2001468; rev:7;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Xpire.info Multiple Spyware Installs (6)"; flow: to_server,established; uricontent:"/fa/x.chm"; nocase; classtype:
trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001469; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Xpire.info; sid:2001469;
rev:8;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Xpire.info Multiple Spyware Installs (7)"; flow: to_server,established; uricontent:"/fa/xpl3.htm"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001470; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Xpire.info;
sid:2001470; rev:8;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Xpire.info Spyware Exploit"; flow: to_server,established; uricontent:"/2DimensionOfExploitsEnc.php"; nocase;
classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001471; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Xpire.info;
sid:2001471; rev:7;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Xpire.info Spyware Install Reporting"; flow: to_server,established; uricontent:"/xpsystem/report.php?user_id=";
nocase; uricontent:"&status=0&country_id="; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001472; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Xpire.info; sid:2001472; rev:7;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Xpire.info Install Code Download"; flow: to_server,established; uricontent:"/install.gz"; nocase; content:"Host|3a|
xpire.info"; nocase; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001491; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Xpire.info; sid:2001491; rev:8;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Xpire.info Install Report"; flow: to_server,established; content:"counter.htm"; nocase;
pcre:"//user\d+/counter\.htm/im"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2001541; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Xpire.info; sid:2001541; rev:10;)

#Thanks James Ashton
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Yesadvertising Banking Spyware RETRIEVE"; flow: to_server,established; uricontent:"/img1big.gif"; nocase;
classtype: trojan-activity; reference:url,isc.sans.org/presentations/banking_malware.pdf; reference:url,doc.emergingthreats.net/bin/view/Main/2000336;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Yesadvertising_Banking_Spyware; sid:2000336; rev:10;)

#Thanks James Ashton
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Yesadvertising Banking Spyware INFORMATION SUBMIT"; flow: to_server,established; uricontent:"/cgi-bin/yes.pl";
nocase; classtype: trojan-activity; reference:url,isc.sans.org/presentations/banking_malware.pdf; reference:url,doc.emergingthreats.net/bin/view/Main/2000337;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Yesadvertising_Banking_Spyware; sid:2000337; rev:10;)

#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE YourSiteBar Data Submision"; flow: to_server,established; uricontent:"/ist/scripts/istsvc_ads_data.php?version=";
nocase; classtype: trojan-activity; reference:url,www.ysbweb.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001698; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_YourSiteBar; sid:2001698; rev:6;)

#Matt jonkman from Spyware LP Data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Yourscreen.com Spyware Download"; flow: to_server,established; uricontent:"/data/yourscreen_data.exe"; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003354; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Yourscreen.com;
sid:2003354; rev:3;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE yupsearch.com Spyware Install - protector.exe"; flow: to_server,established; uricontent:"/protector.exe"; nocase;
classtype: trojan-activity; reference:url,www.yupsearch.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002092; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Yupsearch.com; sid:2002092; rev:6;)

#By Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE yupsearch.com Spyware Install - sideb.exe"; flow: to_server,established; uricontent:"/sideb.exe"; nocase;
classtype: trojan-activity; reference:url,www.yupsearch.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002098; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Yupsearch.com; sid:2002098; rev:6;)

#John Stewart
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Zenotecnico Adware"; flow: to_server,established; uricontent:"/cl/clientdump"; content:"zenotecnico"; nocase;
classtype: policy-violation; reference:url,www.zenotecnico.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001947; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Zenotecnico; sid:2001947; rev:5;)

#Matt Jonkman
#
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Zenotecnico Adware 2"; flow: to_server,established; uricontent:"/cl/clienthost"; content:"zenotecnico"; nocase;
classtype: policy-violation; reference:url,www.zenotecnico.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002735; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Zenotecnico; sid:2002735; rev:4;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Zenotecnico Spyware Install Report"; flow: to_server,established; uricontent:"/instreport"; content:"zenotecnico";
nocase; classtype: policy-violation; reference:url,www.zenotecnico.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002737; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Zenotecnico; sid:2002737; rev:4;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE General Malware Checkin HTTP POST"; flow:established,to_server; content:"POST "; depth:5; content:"|0d 0a 0d
0a|uid="; distance:0; content:"&ref="; distance:0; content:"&clid="; distance:0; content:"&commode="; distance:0; content:"&cmd="; distance:0; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2008757; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Zenotecnico; sid:2008757; rev:2;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Zenosearch Malware Checkin HTTP POST (2)"; flow:established,to_server; content:"POST "; depth:5; uricontent:".asp?
rnd="; content:"|0d 0a 0d 0a|uid="; content:"&ref="; distance:0; content:"&clid="; distance:0; content:"&umode="; distance:0; content:"&cn="; distance:0; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/bin/view/Main/2008798; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_Zenotecnico; sid:2008798; rev:2;)

#Matt Jonkman, from spyware lp data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE Supergames.aavalue.com Spyware"; flow: established,to_server; uricontent:"/toolbars/msg/msg_serverside.xml";
nocase; content:"aavalue.com"; nocase; classtype:trojan-activity; reference:url,research.sunbelt-software.com/threatdisplay.aspx?name=EZ-Tracks%20Toolbar&threatid=41189;
reference:url,doc.emergingthreats.net/bin/view/Main/2003525; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_aavalue.com; sid:2003525; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE adservs.com Spyware"; flow: to_server,established; uricontent:"/binaries/relevance.dat"; content:"adservs"; nocase;
classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002740; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_adservs.com;
sid:2002740; rev:3;)

#Following are requests from adware served by iframebiz.biz
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE iframebiz - adv***.php"; flow:established,to_server; content:"GET "; depth:4; nocase; uricontent:"/adv"; nocase;
pcre:"/adv\d+\.php/Ui"; classtype:trojan-activity; reference:url,iframecash.biz; reference:url,isc.sans.org/diary.php?storyid=868;
reference:url,doc.emergingthreats.net/bin/view/Main/2002707; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_iframebiz; sid:2002707; rev:6;)

#Following are requests from adware served by iframebiz.biz
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE iframebiz - sploit.anr"; flow:established,to_server; content:"GET "; depth:4; nocase; uricontent:"/sploit.anr";
nocase; classtype:trojan-activity; reference:url,iframecash.biz; reference:url,isc.sans.org/diary.php?storyid=868; reference:url,doc.emergingthreats.net/bin/view/Main/2002708;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_iframebiz; sid:2002708; rev:6;)

#Following are requests from adware served by iframebiz.biz
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE iframebiz - loaderadv***.jar"; flow:established,to_server; content:"GET "; depth:4; nocase;
uricontent:"/loaderadv"; nocase; pcre:"/loaderadv\d+\.jar/Ui"; classtype:trojan-activity; reference:url,iframecash.biz; reference:url,isc.sans.org/diary.php?storyid=868;
reference:url,doc.emergingthreats.net/bin/view/Main/2002709; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_iframebiz; sid:2002709; rev:6;)

#Following are requests from adware served by iframebiz.biz
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE iframebiz - loadadv***.exe"; flow:established,to_server; content:"GET "; depth:4; nocase; uricontent:"/loadadv";
nocase; pcre:"/loadadv\d+\.exe/Ui"; classtype:trojan-activity; reference:url,iframecash.biz; reference:url,isc.sans.org/diary.php?storyid=868;
reference:url,doc.emergingthreats.net/bin/view/Main/2002710; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_iframebiz; sid:2002710; rev:6;)

#by Deapesh Misra
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE iframebiz - /qwertyuiyw12ertyuytre/adv***.php"; flow:established,to_server; uricontent:"/qwertyuiyw12ertyuytre";
nocase; classtype:trojan-activity; reference:url,iframecash.biz; reference:url,www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_DLOADR.QC&VSect=T;
reference:url,doc.emergingthreats.net/bin/view/Main/2008681; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_iframebiz; sid:2008681; rev:4;)

#Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE K8l.info Spyware Activity"; flow: to_server,established; uricontent:"/media/servlet/view/dynamic/url/zone?";
nocase; uricontent:"zid="; nocase; uricontent:"&pid="; nocase; uricontent:"&DHWidth="; nocase; uricontent:"&DHHeight="; nocase; uricontent:"Ref="; nocase; classtype: policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2003451; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/MALWARE/MALWARE_k8l.info; sid:2003451; rev:3;)

#Matt Jonkman, from spywarelp data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P ABC Torrent User-Agent (ABC/ABC-3.1.0)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| ABC/ABC"; nocase;
classtype:trojan-activity; reference:url,pingpong-abc.sourceforge.net; reference:url,doc.emergingthreats.net/bin/view/Main/2003475; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_ABC_Torrent_client; sid:2003475; rev:7;)

#Submitted by Marcamone
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET P2P Ares traffic"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| Ares"; classtype:policy-violation;
reference:url,www.aresgalaxy.org; reference:url,doc.emergingthreats.net/bin/view/Main/2001059; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Ares; sid:2001059;
rev:8;)

#by Jeff Kell. Depth is correct, it's got 2 byte sway to compensate for 36 or 38 byte offset
#
alert udp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET P2P Ares over UDP"; content:"Ares "; offset:36; depth:7; classtype:policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2003437; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Ares; sid:2003437; rev:3;)

#by Christopher Campesi
#
alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET P2P Ares Server Connection"; flow:established,to_server; dsize:<70; content:"r|be|bloop|00|dV"; content:"Ares|00 0a|";
distance:16; classtype:policy-violation; reference:url,aresgalaxy.sourceforge.net; reference:url,doc.emergingthreats.net/bin/view/Main/2008591;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Ares; sid:2008591; rev:3;)

#by Will Metcalf
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P Azureus P2P Client User-Agent"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Azureus"; classtype:policy-
violation; reference:url,doc.emergingthreats.net/bin/view/Main/2007799; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Azureus; sid:2007799; rev:3;)

#by Philipp Seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P Bittorrent P2P Client User-Agent (BTSP)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| BTSP/";
classtype:policy-violation; reference:url,doc.emergingthreats.net/2011713; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_BTSP; sid:2011713; rev:3;)

#from spyware LP data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P BearShare P2P Gnutella Client User-Agent (BearShare 6.x.x.x)"; flow:to_server,established; content:"|0d 0a|User-
Agent|3a| BearShare "; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2006371; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_BearShare; sid:2006371; rev:6;)

#from spyware LP data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P BearShare P2P Gnutella Client HTTP Request "; flow:to_server,established; uricontent:"/gnutella/"; nocase;
uricontent:"?client=BEAR"; nocase; uricontent:"&version="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2006379;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_BearShare; sid:2006379; rev:4;)

#by Philipp Seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P Bittorrent P2P Client User-Agent (BitComet)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| BitComet/";
classtype:policy-violation; reference:url,www.bitcomet.com; reference:url,doc.emergingthreats.net/2011710; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_BitComet; sid:2011710; rev:3;)
```

```
#by Philipp Seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P Bittorrent P2P Client User-Agent (BitTornado)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
BitTornado/"; classtype:policy-violation; reference:url,www.bittornado.com; reference:url,doc.emergingthreats.net/2011702; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Bittornado; sid:2011702; rev:3;)

#By Chich Thierry
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET P2P BitTorrent peer sync"; flow: established; content:"|0000000d0600|"; offset: 0; depth: 6; classtype: policy-violation;
reference:url,bitconjurer.org/BitTorrent/protocol.html; reference:url,doc.emergingthreats.net/bin/view/Main/2000334; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Bittorrent_Traffic; sid:2000334; rev:9;)

#By Chich Thierry
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET P2P BitTorrent Traffic"; flow: established; content:"|0000400907000000|"; offset: 0; depth: 8; classtype: policy-violation;
reference:url,bitconjurer.org/BitTorrent/protocol.html; reference:url,doc.emergingthreats.net/bin/view/Main/2000357; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Bittorrent_Traffic; sid:2000357; rev:5;)

#By Chich Thierry
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 6969 (msg:"ET P2P BitTorrent Announce"; flow: to_server,established; content:"/announce"; classtype: policy-violation;
reference:url,bitconjurer.org/BitTorrent/protocol.html; reference:url,doc.emergingthreats.net/bin/view/Main/2000369; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Bittorrent_Traffic; sid:2000369; rev:6;)

#from spyware LP data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P Bittorrent P2P Client User-Agent (Bittorrent/5.x.x)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
Bittorrent"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2006372; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Bittorrent_Traffic; sid:2006372; rev:6;)

#from spyware LP data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P Bittorrent P2P Client HTTP Request "; flow:to_server,established; uricontent:"/trackerphp/announce.php?"; nocase;
uricontent:"?port="; nocase; uricontent:"&peer_id="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2006375; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Bittorrent_Traffic; sid:2006375; rev:4;)

#by Will Metcalf
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P possible torrent download"; flow:to_server,established; uricontent:".torrent"; nocase; pcre:"/(\.torrent)$/Ui";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2007727; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Bittorrent_Traffic;
sid:2007727; rev:4;)

#Trackerless torrents, by David Bianco
#
alert udp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET P2P BitTorrent DHT ping request"; content:"d1|3a|ad2|3a|id20|3a|"; depth:12; nocase; threshold: type both, count 1, seconds 300,
track by_src; classtype:policy-violation; reference:url,wiki.theory.org/BitTorrentDraftDHTProtocol; reference:url,doc.emergingthreats.net/bin/view/Main/2008581;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Bittorrent_Traffic; sid:2008581; rev:3;)

#Trackerless torrents, by David Bianco
#
alert udp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET P2P BitTorrent DHT find_node request"; content:"d1\:ad2\:id20\:"; nocase; depth:12; content:"6\:target20\:"; nocase; distance:20;
depth:11; content:"e1\:q9\:find_node1\:"; nocase; distance:20; depth:17; content:"e1\:q9\:find_node1\:"; distance:20; depth:17; nocase; threshold: type both, count 1, seconds 300, track
by_src; classtype:policy-violation; reference:url,wiki.theory.org/BitTorrentDraftDHTProtocol; reference:url,doc.emergingthreats.net/bin/view/Main/2008582;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Bittorrent_Traffic; sid:2008582; rev:2;)

#Trackerless torrents, by David Bianco
#
alert udp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET P2P BitTorrent DHT nodes reply"; content:"d1|3a|rd2|3a|id20|3a|"; nocase; depth:12; content:"5|3a|nodes"; nocase; distance:20;
depth:7; threshold: type both, count 1, seconds 300, track by_src; classtype:policy-violation; reference:url,wiki.theory.org/BitTorrentDraftDHTProtocol;
reference:url,doc.emergingthreats.net/bin/view/Main/2008583; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Bittorrent_Traffic; sid:2008583; rev:3;)

#Trackerless torrents, by David Bianco
#
alert udp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET P2P BitTorrent DHT get_peers request"; content:"d1|3a|ad2|3a|id20|3a|"; nocase; depth:12; content:"9|3a|info_hash20|3a|"; nocase;
distance:20; depth:14; content:"e1|3a|q9|3a|get_peers1|3a|"; nocase; distance:20; depth:17; threshold: type both, count 1, seconds 300, track by_src; classtype:policy-violation;
reference:url,wiki.theory.org/BitTorrentDraftDHTProtocol; reference:url,doc.emergingthreats.net/bin/view/Main/2008584; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Bittorrent_Traffic; sid:2008584; rev:3;)

#Trackerless torrents, by David Bianco
#
alert udp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET P2P BitTorrent DHT announce_peers request"; content:"d1|3a|ad2|3a|id20|3a|"; nocase; depth:14;
content:"e1|3a|q13|3a|announce_peer1|3a|"; nocase; distance:55; threshold: type both, count 1, seconds 300, track by_src; classtype:policy-violation;
reference:url,wiki.theory.org/BitTorrentDraftDHTProtocol; reference:url,doc.emergingthreats.net/bin/view/Main/2008585; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Bittorrent_Traffic; sid:2008585; rev:4;)

#by Philipp Seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P Bittorrent P2P Client User-Agent (Blizzard Downloader 2.x)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
Blizzard Downloader 2."; classtype:policy-violation; reference:url,www.worldofwarcraft.com/info/faq/blizzarddownloader.html; reference:url,doc.emergingthreats.net/2011708;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Blizzard; sid:2011708; rev:3;)

#by Philipp Seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P Bittorrent P2P Client User-Agent (Deluge 1.x.x)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Deluge 1";
classtype:policy-violation; reference:url,deluge-torrent.org; reference:url,doc.emergingthreats.net/2011704; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Deluge; sid:2011704; rev:3;)

#by markmc
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET P2P Direct Connect Traffic (client-server)"; flow:from_client,established; content:"$MyINFO"; offset:0; depth:7; classtype:policy-
violation; reference:url,en.wikipedia.org/wiki/Direct_connect_file-sharing_application; reference:url,doc.emergingthreats.net/bin/view/Main/2002814;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Direct_Connect; sid:2002814; rev:3;)

#By Chich Thierry
#
#alert tcp any any -> any 4660:4799 (msg:"ET P2P ed2k connection to server"; flow: to_server,established; content:"|e3|"; offset: 0; depth: 1; content:"|00000001|"; offset: 2; depth: 4;
classtype: policy-violation; reference:url,www.giac.org/practical/GCIH/Ian_Gosling_GCIH.pdf; reference:url,doc.emergingthreats.net/bin/view/Main/2000330;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic; sid:2000330; rev:8;)

#By Chich Thierry
#
alert tcp any any -> any 4660:4799 (msg:"ET P2P ed2k request part"; flow: to_server,established; content:"|e3|"; offset: 0; depth: 1; content:"|00000047|"; offset: 2; depth: 4;
classtype: policy-violation; reference:url,www.giac.org/practical/GCIH/Ian_Gosling_GCIH.pdf; reference:url,doc.emergingthreats.net/bin/view/Main/2000332;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic; sid:2000332; rev:8;)

#By Chich Thierry
#
alert tcp any any -> any 4660:4799 (msg:"ET P2P ed2k file request answer"; flow: to_server,established; content:"|e3|"; offset: 0; depth: 1; content:"|00000059|"; offset: 2; depth: 4;
classtype: policy-violation; reference:url,www.giac.org/practical/GCIH/Ian_Gosling_GCIH.pdf; reference:url,doc.emergingthreats.net/bin/view/Main/2000333;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic; sid:2000333; rev:8;)

#By Chich Thierry
#
alert udp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET P2P Kaaza Media desktop p2pnetworking.exe Activity"; content:"|e30cb0|"; offset: 0; depth: 6; threshold: type limit, track by_dst,
count 1 , seconds 600; classtype: policy-violation; reference:url,www.giac.org/practical/GCIH/Ian_Gosling_GCIH.pdf; reference:url,doc.emergingthreats.net/bin/view/Main/2000340;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic; sid:2000340; rev:8;)

#Submitted by Sam Evans
```

```
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 4660:4799 (msg:"ET P2P eDonkey File Status"; flow: to_server,established; content:"|e3 14|"; offset: 0; depth: 2; classtype: policy-violation;
reference:url,www.edonkey.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001296; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic;
sid:2001296; rev:7;)

#Submitted by Sam Evans
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 4660:4799 (msg:"ET P2P eDonkey File Status Request"; flow: to_server,established; content:"|e3 11|"; offset: 0; depth: 2; classtype: policy-
violation; reference:url,www.edonkey.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001297; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic; sid:2001297; rev:8;)

#Submitted by Sam Evans
#
alert udp $HOME_NET any -> $EXTERNAL_NET 4660:4799 (msg:"ET P2P eDonkey Server Status Request"; content:"|e3 96|"; offset: 0; depth: 2; classtype: policy-violation;
reference:url,www.edonkey.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001298; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic;
sid:2001298; rev:7;)

#Submitted by Sam Evans
#
alert udp $HOME_NET 4660:4799 -> $EXTERNAL_NET any (msg:"ET P2P eDonkey Server Status"; content:"|e3 97|"; offset: 0; depth: 2; classtype: policy-violation;
reference:url,www.edonkey.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001299; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic;
sid:2001299; rev:7;)

#Matt Jonkman
#
alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET 1024:65535 (msg:"ET P2P Edonkey IP Request"; dsize:4; content:"|e3 1b|"; depth:2; flowbits:set,BEedk.ip.requestect; flowbits:noalert;
classtype:policy-violation; reference:url,www.giac.org/certified_professionals/practicals/gcih/0446.php; reference:url,doc.emergingthreats.net/bin/view/Main/2003308;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic; sid:2003308; rev:4;)

#Matt Jonkman
#
alert udp $EXTERNAL_NET 1024:65535 -> $HOME_NET 1024:65535 (msg:"ET P2P Edonkey IP Reply"; flowbits:isset,BEedk.ip.requestect; dsize:<20; content:"|e3 1c|"; depth:2; classtype:policy-
violation; reference:url,www.giac.org/certified_professionals/practicals/gcih/0446.php; reference:url,doc.emergingthreats.net/bin/view/Main/2003309;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic; sid:2003309; rev:4;)

#Matt Jonkman
#
alert udp $EXTERNAL_NET 1024:65535 -> $HOME_NET 1024:65535 (msg:"ET P2P Edonkey IP Query End"; dsize:<20; content:"|e3 1d|"; depth:2; classtype:policy-violation;
reference:url,www.giac.org/certified_professionals/practicals/gcih/0446.php; reference:url,doc.emergingthreats.net/bin/view/Main/2003316; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic; sid:2003316; rev:3;)

#Matt Jonkman
#
alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET 1024:65535 (msg:"ET P2P Edonkey Publicize File"; dsize:>15; content:"|e3 0c|"; depth:2; classtype:policy-violation;
reference:url,www.giac.org/certified_professionals/practicals/gcih/0446.php; reference:url,doc.emergingthreats.net/bin/view/Main/2003310; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic; sid:2003310; rev:3;)

#Matt Jonkman
#
alert udp $EXTERNAL_NET 1024:65535 -> $HOME_NET 1024:65535 (msg:"ET P2P Edonkey Publicize File ACK"; dsize:<20; content:"|e3 0d|"; depth:2; classtype:policy-violation;
reference:url,www.giac.org/certified_professionals/practicals/gcih/0446.php; reference:url,doc.emergingthreats.net/bin/view/Main/2003311; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic; sid:2003311; rev:3;)

#Matt Jonkman
#
alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET 1024:65535 (msg:"ET P2P Edonkey Connect Request"; dsize:25; content:"|e3 0a|"; depth:2; classtype:policy-violation;
reference:url,www.giac.org/certified_professionals/practicals/gcih/0446.php; reference:url,doc.emergingthreats.net/bin/view/Main/2003312; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic; sid:2003312; rev:3;)

#Matt Jonkman
#
alert udp $EXTERNAL_NET 1024:65535 -> $HOME_NET 1024:65535 (msg:"ET P2P Edonkey Connect Reply and Server List"; dsize:>200; content:"|e3 0b|"; depth:2; classtype:policy-violation;
reference:url,www.giac.org/certified_professionals/practicals/gcih/0446.php; reference:url,doc.emergingthreats.net/bin/view/Main/2003313; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic; sid:2003313; rev:3;)

#Matt Jonkman
#
alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET 1024:65535 (msg:"ET P2P Edonkey Search Request (by file hash)"; dsize:19; content:"|e3 0e 14|"; depth:3; classtype:policy-violation;
reference:url,www.giac.org/certified_professionals/practicals/gcih/0446.php; reference:url,doc.emergingthreats.net/bin/view/Main/2003314; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic; sid:2003314; rev:3;)

#Matt Jonkman
#
alert udp $EXTERNAL_NET 1024:65535 -> $HOME_NET 1024:65535 (msg:"ET P2P Edonkey Search Reply"; dsize:>200; content:"|e3 0f|"; depth:2; classtype:policy-violation;
reference:url,www.giac.org/certified_professionals/practicals/gcih/0446.php; reference:url,doc.emergingthreats.net/bin/view/Main/2003315; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic; sid:2003315; rev:3;)

#Matt Jonkman
#
alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET 1024:65535 (msg:"ET P2P Edonkey Search Request (any type file)"; dsize:>19; content:"|e3 0e|"; depth:2; classtype:policy-violation;
reference:url,www.giac.org/certified_professionals/practicals/gcih/0446.php; reference:url,doc.emergingthreats.net/bin/view/Main/2003317; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic; sid:2003317; rev:3;)

#Matt Jonkman
#
alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET 1024:65535 (msg:"ET P2P Edonkey Get Sources Request (by hash)"; dsize:19; content:"|e3 9a|"; depth:2; classtype:policy-violation;
reference:url,www.giac.org/certified_professionals/practicals/gcih/0446.php; reference:url,doc.emergingthreats.net/bin/view/Main/2003318; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic; sid:2003318; rev:3;)

#Matt Jonkman
#
alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET 1024:65535 (msg:"ET P2P Edonkey Search Request (search by name)"; dsize:>5; content:"|e3 98|"; depth:2; content:"|01|"; within:3;
classtype:policy-violation; reference:url,www.giac.org/certified_professionals/practicals/gcih/0446.php; reference:url,doc.emergingthreats.net/bin/view/Main/2003319;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic; sid:2003319; rev:3;)

#Matt Jonkman
#
alert udp $EXTERNAL_NET 1024:65535 -> $HOME_NET 1024:65535 (msg:"ET P2P Edonkey Search Results"; dsize:>21; content:"|e3 99|"; depth:2; classtype:policy-violation;
reference:url,www.giac.org/certified_professionals/practicals/gcih/0446.php; reference:url,doc.emergingthreats.net/bin/view/Main/2003320; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic; sid:2003320; rev:3;)

#Matt Jonkman
#
#alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET 4660:4799 (msg:"ET P2P Edonkey Server Message"; flow:established; dsize:>10; content:"|e3|"; depth:1; content:"|38|"; offset:4;
within:5; classtype:policy-violation; reference:url,www.giac.org/certified_professionals/practicals/gcih/0446.php; reference:url,doc.emergingthreats.net/bin/view/Main/2003321;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic; sid:2003321; rev:4;)

#Matt Jonkman
#
#alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET 4660:4799 (msg:"ET P2P Edonkey Server List"; flow:established; dsize:>12; content:"|e3|"; depth:1; content:"|32|"; offset:4; within:5;
classtype:policy-violation; reference:url,www.giac.org/certified_professionals/practicals/gcih/0446.php; reference:url,doc.emergingthreats.net/bin/view/Main/2003322;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic; sid:2003322; rev:3;)

#Matt Jonkman
#
alert tcp $HOME_NET 4660:4799 -> $EXTERNAL_NET 1024:65535 (msg:"ET P2P Edonkey Client to Server Hello"; flow:established; dsize:>5; content:"|e3|"; depth:1; content:"|01|"; offset:4;
within:5; content:"|02 01 00 01|"; distance:26; classtype:policy-violation; reference:url,www.giac.org/certified_professionals/practicals/gcih/0446.php;
reference:url,doc.emergingthreats.net/bin/view/Main/2003323; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic; sid:2003323; rev:3;)
```

```
#Matt Jonkman
#
alert tcp $EXTERNAL_NET 1024:65535 -> $HOME_NET 4660:4799 (msg:"ET P2P Edonkey Server Status"; flow:established; dsize:14; content:"|e3 09 00 00 00 34|"; depth:6; classtype:policy-
violation; reference:url,www.giac.org/certified_professionals/practicals/gcih/0446.php; reference:url,doc.emergingthreats.net/bin/view/Main/2003324;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Edonkey_Traffic; sid:2003324; rev:3;)

#by philipp Seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P Bittorrent P2P Client User-Agent (Enhanced CTorrent 3.x)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
Enhanced-CTorrent/dnh3"; classtype:policy-violation; reference:url,www.rahul.net/dholmes/ctorrent; reference:url,doc.emergingthreats.net/2011703;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_EnhancedCtorrent; sid:2011703; rev:3;)

#by Philipp Seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P Bittorrent P2P Client User-Agent (FDM 3.x)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| FDM 3.x";
classtype:policy-violation; reference:url,www.freedownloadmanager.org; reference:url,doc.emergingthreats.net/2011712; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_FDM; sid:2011712; rev:3;)

#Submitted by Pedro Quintanilha on 2005-11-07
#
alert tcp $EXTERNAL_NET 443 -> $HOME_NET any (msg:"ET P2P MS Foldershare Login Detected"; flow:established,to_client; content:"|0b|FolderShare|30 81 9f 30|"; nocase; offset: 392; depth:
18; classtype:policy-violation; reference:url,www.foldershare.com; reference:url,doc.emergingthreats.net/bin/view/Main/2002673; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Foldershare; sid:2002673; rev:4;)

#From Cooljay
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET P2P Gnutella Connect"; flow: established,to_server; content:"GNUTELLA CONNECT/"; nocase; offset: 0; depth: 17; classtype: policy-
violation; reference:url,www.gnutella.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001664; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Gnutella;
sid:2001664; rev:5;)

#by Jeff Kell
#Looking for Gnucleus/GnucDNA UDP Ultrapeer handshakes
#
alert udp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET P2P GnucDNA UDP Ultrapeer Traffic"; content:"SCP@|83|DNA@"; threshold: type both,track by_src,count 10,seconds 600; classtype:
policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002760; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Gnutella; sid:2002760; rev:3;)

#Looking for Gnucleus/GnucDNA running Ultrapeer
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET P2P Gnutella TCP Ultrapeer Traffic"; flow: established,to_server; content:"GNUTELLA"; offset:0; depth:8; content:"X-Ultrapeer|3a|
True"; nocase; threshold: type both,track by_src,count 5,seconds 3600; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002761;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Gnutella; sid:2002761; rev:4;)

#by Matt Jonkman
#
alert tcp any 1024: -> any 1024: (msg:"ET P2P Gnutella TCP Traffic"; flow: established,to_server; content:"GNUTELLA"; offset:0; depth:8; content:"200 OK|0d 0a|"; within:15; threshold:
type both,track by_src,count 5,seconds 360; classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2007801; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Gnutella; sid:2007801; rev:2;)

#Thanks to Kevin Kolk
#
alert tcp $EXTERNAL_NET 6667 -> $HOME_NET any (msg:"ET P2P iroffer IRC Bot help message"; flow: from_server,established; content:"|54 6F 20 72 65 71 75 65 73 74 20 61 20 66 69 6C 65 20
74 79 70 65 3A 20 22 2F 6D 73 67|"; depth: 500; classtype: trojan-activity; reference:url,iroffer.org; reference:url,doc.emergingthreats.net/bin/view/Main/2000338;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Iroffer_IRC_Bot; sid:2000338; rev:5;)

#Thanks to Kevin Kolk
#
alert tcp $EXTERNAL_NET 6667 -> $HOME_NET any (msg:"ET P2P iroffer IRC Bot offered files advertisement"; flow: from_server,established; content:"|54 6F 74 61 6C 20 4F 66 66 65 72 65 64
3A|"; depth: 500; classtype: trojan-activity; reference:url,iroffer.org; reference:url,doc.emergingthreats.net/bin/view/Main/2000339; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Iroffer_IRC_Bot; sid:2000339; rev:5;)

#By Bob Grabowsky
#
alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET 1024:65535 (msg:"ET P2P Kazaa over UDP"; content:"KaZaA"; nocase; threshold: type threshold, track by_src,count 10, seconds 60;
classtype: policy-violation; reference:url,www.kazaa.com/us/index.htm; reference:url,doc.emergingthreats.net/bin/view/Main/2001796; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Kazaa; sid:2001796; rev:5;)

#By Bob Grabowsky
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET P2P KazaaClient P2P Traffic"; flow: established; content:"Agent|3a| KazaaClient"; nocase; classtype: policy-violation;
reference:url,www.kazaa.com/us/index.htm; reference:url,doc.emergingthreats.net/bin/view/Main/2001812; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Kazaa;
sid:2001812; rev:7;)

#by Philipp Seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P Bittorrent P2P Client User-Agent (KTorrent/3.x.x)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
KTorrent/3"; classtype:policy-violation; reference:url,ktorrent.org; reference:url,doc.emergingthreats.net/2011700; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Ktorrent; sid:2011700; rev:3;)

#by Philipp Seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P Bittorrent P2P Client User-Agent (KTorrent 2.x)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
ktorrent/2"; classtype:policy-violation; reference:url,ktorrent.org; reference:url,doc.emergingthreats.net/2011711; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Ktorrent; sid:2011711; rev:3;)

#by Christopher Campesi
#
alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET 1024:65535 (msg:"ET P2P KuGoo P2P Connection"; dsize:<30; content:"|64|"; offset:0; depth:1; content:"|70|"; distance:5; content:"|50
37|"; distance:4; classtype:policy-violation; reference:url,koogoo.com; reference:url,doc.emergingthreats.net/2009966; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_KuGoo; sid:2009966; rev:2;)

#By Bob Grabowsky
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET P2P LimeWire P2P Traffic"; flow: established; content:"User-Agent|3a| LimeWire"; nocase; classtype: policy-violation;
reference:url,www.limewire.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001808; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Limewire; sid:2001808;
rev:7;)

#By Bob Grabowsky
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET P2P LimeWire P2P Traffic"; flow: established; content:"Server|3a| LimeWire"; nocase; classtype: policy-violation;
reference:url,www.limewire.com; reference:url,doc.emergingthreats.net/bin/view/Main/2007800; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Limewire; sid:2007800;
rev:4;)

#Depth and offset added by Jeff Kell
#
alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET 1024:65535 (msg:"ET P2P Limewire P2P UDP Traffic"; dsize:35; content:"|49 50 40 83 53 43 50 41 00 00|"; offset:25; depth:10; threshold:
type both, track by_src, count 1, seconds 360; classtype: policy-violation; reference:url,www.limewire.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001809;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Limewire; sid:2001809; rev:6;)

#Depth and offset added by Jeff Kell
#
alert udp $HOME_NET 6345:6349 -> $EXTERNAL_NET 6345:6349 (msg:"ET P2P UDP traffic - Likely Limewire"; threshold: type threshold,track by_src,count 40, seconds 300; classtype: policy-
violation; reference:url,www.limewire.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001841; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Limewire;
sid:2001841; rev:7;)

#by Christopher Campesi
#
alert udp $EXTERNAL_NET 41170 -> $HOME_NET any (msg:"ET P2P Manolito Connection (1)"; dsize:<48; content:"|3d 4a d9|"; depth:3; classtype:policy-violation;
reference:url,doc.emergingthreats.net/2009097; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Manolito; sid:2009097; rev:2;)
```

```
#by Christopher Campesi
#
alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET 41170 (msg:"ET P2P Manolito Ping"; dsize:<24; content:"|3d|"; depth:1; content:"|d9|"; distance:1; content:"|ed bb|"; distance:13;
threshold: type limit, track by_src, seconds 300, count 1; classtype:policy-violation; reference:url,doc.emergingthreats.net/2009098; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Manolito; sid:2009098; rev:3;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P Morpheus Install"; flow: to_server,established; uricontent:"/morpheus/morpheus.exe"; nocase; classtype: policy-
violation; reference:url,www.morpheus.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001035; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Morpheus;
sid:2001035; rev:7;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P Morpheus Install ini Download"; flow: to_server,established; uricontent:"/morpheus/morpheus_sm.ini"; nocase; classtype:
policy-violation; reference:url,www.morpheus.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001036; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Morpheus; sid:2001036; rev:7;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P Morpheus Update Request"; flow: to_server,established; uricontent:"/gwebcache/gcache.asg?hostfile="; nocase; classtype:
policy-violation; reference:url,www.morpheus.com; reference:url,doc.emergingthreats.net/bin/view/Main/2001037; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Morpheus; sid:2001037; rev:7;)

#by Jack Pepper
#
alert udp $HOME_NET 8247 -> $EXTERNAL_NET 8247 (msg:"ET P2P Octoshape UDP Session"; threshold: type both, count 2, seconds 60, track by_src; classtype:trojan-activity;
reference:url,msmvps.com/blogs/bradley/archive/2009/01/20/peer-to-peer-on-cnn.aspx; reference:url,doc.emergingthreats.net/2009986; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Octoshape; sid:2009986; rev:2;)

#Scott Lazzari and Stephen Nesman
#
alert udp $HOME_NET any -> $EXTERNAL_NET 8247 (msg:"ET P2P Octoshape P2P streaming media"; content:"POST / HTTP/1."; depth:64; content:"Oshtcp-streamtype|3a|"; threshold: type limit,
track by_src, count 1, seconds 600; classtype:policy-violation; reference:url,doc.emergingthreats.net/2010008; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Octoshape; sid:2010008; rev:4;)

#by Philipp Seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P Bittorrent P2P Client User-Agent (Opera/10.x)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Opera
BitTorrent, Opera/"; classtype:policy-violation; reference:url,www.opera.com; reference:url,doc.emergingthreats.net/2011701; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Opera; sid:2011701; rev:3;)

#By Chich Thierry
#
alert udp any any -> any any (msg:"ET P2P Overnet (Edonkey) Server Announce"; content:"|00000203006c6f63|"; offset: 36; content:"|006263703a2f2f|"; distance: 1; classtype: policy-
violation; reference:url,www.overnet.com; reference:url,doc.emergingthreats.net/bin/view/Main/2000335; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Overnet_Traffic; sid:2000335; rev:7;)

#by dxp
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P Pando Client User-Agent Detected (Mozilla/4.0 (Windows U) Pando/1.xx)"; flow:established,to_server; content:"|0d
0a|User-Agent|3a| Mozilla/4.0 (Windows|3b| U) Pando/"; nocase; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2008625;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Pando; sid:2008625; rev:4;)

#
alert tcp any any -> any any (msg:"ET P2P Phatbot Control Connection"; flow: established; content:"Wonk-"; content:"|00|#waste|00|"; within: 15; classtype: trojan-activity;
reference:url,www.lurhq.com/phatbot.html; reference:url,doc.emergingthreats.net/bin/view/Main/2000015; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Phatbot_Control_Connection; sid:2000015; rev:6;)

#by Philipp Seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P Client User-Agent (Shareaza 2.x)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| Shareaza 2.";
classtype:policy-violation; reference:url,shareaza.sourceforge.net; reference:url,doc.emergingthreats.net/2011707; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Sharazaa; sid:2011707; rev:3;)

#Submitted by marcamone
#
alert tcp $HOME_NET any -> 38.115.131.0/24 2234 (msg:"ET P2P Soulseek traffic (1)"; flow: established; classtype: policy-violation; reference:url,www.slsknet.org;
reference:url,doc.emergingthreats.net/bin/view/Main/2001185; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Soulseek; sid:2001185; rev:8;)

#Submitted by marcamone
#
alert tcp $HOME_NET any -> 38.115.131.0/24 5534 (msg:"ET P2P Soulseek traffic (2)"; flow: established; classtype: policy-violation; reference:url,www.slsknet.org;
reference:url,doc.emergingthreats.net/bin/view/Main/2001186; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Soulseek; sid:2001186; rev:8;)

#Submitted by marcamone
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET P2P Soulseek"; flow: established; content:"slsknet"; classtype: policy-violation; reference:url,www.slsknet.org;
reference:url,doc.emergingthreats.net/bin/view/Main/2001188; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Soulseek; sid:2001188; rev:7;)

#Submitted by Matt Jonkman
#
alert tcp $EXTERNAL_NET 2234 -> $HOME_NET any (msg:"ET P2P Soulseek Filesearch Results"; flow: from_server,established; content:"|09 00 00 00 78|"; classtype: policy-violation;
reference:url,www.slsknet.org; reference:url,doc.emergingthreats.net/bin/view/Main/2001187; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Soulseek; sid:2001187;
rev:6;)

#christopher Campesi
#
alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 2240 (msg:"ET P2P SoulSeek P2P Server Connection"; flow:established,to_server; content:"|01 00 00 00|"; offset:4; depth:4; classtype:policy-
violation; reference:url,www.slsknet.org; reference:url,doc.emergingthreats.net/2008595; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Soulseek; sid:2008595;
rev:5;)

#christopher Campesi
#
alert tcp $EXTERNAL_NET 2240 -> $HOME_NET 1024: (msg:"ET P2P SoulSeek P2P Login Response"; flow:from_server,established; content:"|5c 01 00 00 01 00 00 00|"; offset:0; depth:8;
classtype:policy-violation; reference:url,www.slsknet.org; reference:url,doc.emergingthreats.net/2008611; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Soulseek;
sid:2008611; rev:4;)

#by Christopher Campesi
#
alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET 1024:65535 (msg:"ET P2P ThunderNetwork UDP Traffic"; dsize:<38; content:"|32 00 00 00|"; depth:4; content:"|00 00 00 00|"; distance:1;
threshold:type limit, track by_src, count 1, seconds 300; classtype:policy-violation; reference:url,xunlei.com; reference:url,en.wikipedia.org/wiki/Xunlei;
reference:url,doc.emergingthreats.net/2009099; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_ThunderNetwork; sid:2009099; rev:3;)

#by Philipp Seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P Bittorrent P2P Client User-Agent (Transmission/1.x)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
Transmission/"; classtype:policy-violation; reference:url,www.transmissionbt.com; reference:url,doc.emergingthreats.net/2011699; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Transmission; sid:2011699; rev:3;)

#by Christopher Campesi
#
alert tcp $HOME_NET 1024:65535 -> $EXTERNAL_NET 1024:65535 (msg:"ET P2P Vuze BT Connection"; flow:established; content:"|00 00|"; depth:2; content:"|05|AZVER|01|"; distance:5; depth:7;
content:"appid"; within:10; threshold:type limit, track by_src, count 10, seconds 600; classtype:policy-violation; reference:url,vuze.com; reference:url,doc.emergingthreats.net/2010139;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Vuze; sid:2010139; rev:4;)

#by Christopher Campesi
```

```
#
alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET any (msg:"ET P2P Vuze BT UDP Connection"; dsize:<80; content:!"|00 22 02 00|"; depth: 4; content:"|00 00 04|"; offset:8; depth:3;
content:"|00 00 00 00 00|"; distance:6; depth:5; classtype:policy-violation; reference:url,vuze.com; reference:url,doc.emergingthreats.net/2010140;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Vuze; sid:2010140; rev:3;)

#by Christopher Campesi
#
alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET any (msg:"ET P2P Vuze BT UDP Connection (2)"; dsize:94; content:"|00 00 04|"; offset:0; depth:3; content:"|00 00 00 00 00|"; distance:14;
depth:5; content:"|ff ff ff ff ff 00 00 00 00 02 05 21|"; distance:8; depth:11; content:"|00 00 00 00 00 00|"; distance:25; depth:6; content:"|00 00|"; distance:20; depth:2;
classtype:policy-violation; reference:url,vuze.com; reference:url,doc.emergingthreats.net/2010141; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Vuze;
sid:2010141; rev:2;)

#by Christopher Campesi
#
alert udp $EXTERNAL_NET any -> $HOME_NET 1024:65535 (msg:"ET P2P Vuze BT UDP Connection (3)"; dsize:80; content:"|00 00 04|"; depth:3; content:"|00 00 00 00 00|"; distance:14; depth:5;
content:"|02 05 21 04|"; distance:4; depth:4; threshold:type limit, track by_dst, count 10, seconds 600; classtype:policy-violation; reference:url,doc.emergingthreats.net/2010142;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Vuze; sid:2010142; rev:3;)

#by Christopher Campesi
#
alert udp $EXTERNAL_NET any -> $HOME_NET 1024:65535 (msg:"ET P2P Vuze BT UDP Connection (4)"; dsize:<300; content:"|00 00 04|"; depth:3; content:"|00 00 00 00 00|"; distance:14;
depth:5; content:"|ff ff ff ff|"; distance:8; depth:4; classtype:policy-violation; reference:url,doc.emergingthreats.net/2010143; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_Vuze; sid:2010143; rev:2;)

#by Christopher Campesi
#
alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET any (msg:"ET P2P Vuze BT UDP Connection (5)"; dsize:<20; content:"|00 00 04 17 27 10 19 80 00 00 00 00|"; offset:0; depth:12;
classtype:policy-violation; reference:url,vuze.com; reference:url,doc.emergingthreats.net/2010144; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_Vuze;
sid:2010144; rev:3;)

#by christopher campesi
#
alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET 1024:65535 (msg:"ET P2P eMule KAD Network Connection Request"; dsize:35; content:"|e4 21|"; offset:0; depth:2; classtype:policy-
violation; threshold: type limit, count 5, seconds 600, track by_src; reference:url,emule-project.net; reference:url,doc.emergingthreats.net/2009967;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_eMule; sid:2009967; rev:3;)

#by christopher campesi
#
alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET 1024:65535 (msg:"ET P2P eMule KAD Network Connection Request(2)"; dsize:35; content:"|e4 20|"; offset:0; depth:2; threshold: type limit,
count 5, seconds 600, track by_src; classtype:policy-violation; reference:url,emule-project.net; reference:url,doc.emergingthreats.net/2009968;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_eMule; sid:2009968; rev:3;)

#by christopher campesi
#
alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET 1024:65535 (msg:"ET P2P eMule KAD Network Firewalled Request"; dsize:35; content:"|e4 50|"; offset:0; depth:2; threshold: type limit,
count 5, seconds 600, track by_src; classtype:policy-violation; reference:url,emule-project.net; reference:url,doc.emergingthreats.net/2009969;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_eMule; sid:2009969; rev:3;)

#by christopher campesi
#
alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET 1024:65535 (msg:"ET P2P eMule Kademlia Hello Request"; dsize:<48; content:"|e4 11|"; offset:0; depth:2; threshold: type limit, count 5,
seconds 600, track by_src; classtype:policy-violation; reference:url,emule-project.net; reference:url,doc.emergingthreats.net/2009970; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_eMule; sid:2009970; rev:3;)

#by christopher campesi
#
alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET 1024:65535 (msg:"ET P2P eMule KAD Network Hello Request (2)"; content:"|e4 10|"; depth:2; byte_test:2,<,65535,0,relative; threshold: type
limit, count 5, seconds 600, track by_src; classtype:policy-violation; reference:url,emule-project.net; reference:url,doc.emergingthreats.net/2009971;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_eMule; sid:2009971; rev:5;)

#by christopher campesi
#
alert udp $HOME_NET 1024:65535 -> $EXTERNAL_NET 1024:65535 (msg:"ET P2P eMule KAD Network Server Status Request"; dsize:44; content:"|8c 97|"; offset:0; depth:2; threshold: type limit,
count 5, seconds 600, track by_src; classtype:policy-violation; reference:url,emule-project.net; reference:url,doc.emergingthreats.net/2009972;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_eMule; sid:2009972; rev:3;)

#by christopher campesi
#
#alert tcp $HOME_NET 1024:65535 -> $EXTERNAL_NET 1024:65535 (msg:"ET P2P eMule KAD Network Send Username"; flow:established; content:"|e3|"; offset:0; depth:1; content:"|00 00 00 01|";
depth:4; distance:1; byte_test:1,<,51,37; threshold: type limit, count 5, seconds 600, track by_src; classtype:policy-violation; reference:url, emule-project.net;
reference:url,doc.emergingthreats.net/2009973; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/P2P/P2P_eMule; sid:2009973; rev:3;)

#by Philipp Seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P Bittorrent P2P Client User-Agent (rTorrent)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| rtorrent/";
classtype:policy-violation; reference:url,libtorrent.rakshasa.no; reference:url,doc.emergingthreats.net/2011705; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_rTorrent; sid:2011705; rev:3;)

#by Philipp Seidel
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET P2P Bittorrent P2P Client User-Agent (uTorrent)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a| uTorrent/";
classtype:policy-violation; reference:url,www.utorrent.com; reference:url,doc.emergingthreats.net/2011706; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/P2P/P2P_uTorrent; sid:2011706; rev:3;)

#by Matt Jonkman
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET MALWARE 404 Response with an EXE Attached - Likely Malware Drop"; flow:established,from_server; content:"HTTP/1.1 404 Not
Found|0d 0a|"; depth:24; content:"|0d 0a 0d 0a|MZ"; distance:0; classtype:attempted-admin; reference:url,doc.emergingthreats.net/bin/view/Main/2009028;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_404_EXE; sid:2009028; rev:4;)

#by Matt Jonkman, from qru
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY AOL Toolbar User-Agent (AOLToolbar)"; flow:to_server,established; content:"AOLToolbar"; depth:300; nocase;
pcre:"/User-Agent\x3a[^\n]+AOLToolbar/i"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2003469; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_AOL_Toolbar; sid:2003469; rev:5;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY AOL Webmail Message Send"; flow:to_server,established; content:"POST "; depth:5; nocase;
uricontent:"/compose_frame.adp"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2000571; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_AOL_Webmail; sid:2000571; rev:7;)

#Submitted by Matt Jonkman
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY AOL Webmail Login"; flow: to_server,established; uricontent:"/login/login.psp?siteId="; content:"triedAimAuth";
classtype: policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2000572; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_AOL_Webmail;
sid:2000572; rev:6;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY External Unencrypted Connection To Aanval Console"; flow:established,to_server;
uricontent:"/aanval/flex/AanvalFlex"; nocase; classtype:misc-activity; reference:url,www.aanval.com; reference:url,doc.emergingthreats.net/bin/view/Main/2008561;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Aanval; sid:2008561; rev:2;)

#by chris kniseley
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Akamai Redswoosh CLIOnlineManager Connection Detected"; flow:established,to_server; content:"PUT "; depth:4;
nocase; content:"|0d 0a|User-Agent|3a|"; content:"rswin_3725.dll"; within:30; nocase; classtype:policy-violation; reference:url,doc.emergingthreats.net/2011275;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Akami; sid:2011275; rev:4;)
```

```
#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET POLICY External Connection to Altiris HelpDesk"; flow:to_server,established; uricontent:"/aexhd/worker/"; nocase;
classtype:misc-activity; reference:url,www.symantec.com/business/theme.jsp?themeid=altiris; reference:url,doc.emergingthreats.net/2009696; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Altiris; sid:2009696; rev:2;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET POLICY External Connection to Altiris Console"; flow:to_server,established; uricontent:"/altiris/ns/"; nocase;
classtype:misc-activity; reference:url,www.symantec.com/business/theme.jsp?themeid=altiris; reference:url,doc.emergingthreats.net/2009697; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Altiris; sid:2009697; rev:4;)

#by kevin ross
#
#alert tcp [174.129.0.0/16,67.202.0.0/18,79.125.0.0/17,184.72.0.0/15,75.101.128.0/17,174.129.0.0/16,204.236.128.0/17] any -> $HOME_NET any (msg:"ET POLICY Incoming Connection Attempt
From Amazon EC2 Cloud"; flow:to_server; flags:S,12; classtype:misc-activity; reference:url,doc.emergingthreats.net/2010815; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Amazon_Cloud; sid:2010815; rev:5;)

#by kevin ross
#
#alert udp [174.129.0.0/16,67.202.0.0/18,79.125.0.0/17,184.72.0.0/15,75.101.128.0/17,174.129.0.0/16,204.236.128.0/17] !53 -> $HOME_NET !53 (msg:"ET POLICY Incoming UDP Packet From
Amazon EC2 Cloud"; classtype:misc-activity; reference:url,doc.emergingthreats.net/2010816; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Amazon_Cloud;
sid:2010816; rev:6;)

#by mex
#apachebench
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET POLICY ApacheBenchmark Tool User-Agent Detected"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|
ApacheBench"; offset:30; nocase; classtype:attempted-recon; threshold: type limit, count 1, seconds 60, track by_src; reference:url,httpd.apache.org/docs/2.0/programs/ab.html/;
reference:url,doc.emergingthreats.net/2010725; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_ApacheBenchmark; sid:2010725; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Autoit Windows Automation tool User-Agent in HTTP Request - Possibly Hostile"; flow:established,to_server;
content:"|0d 0a|User-Agent|3a| AutoIt"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2008350; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Autoit; sid:2008350; rev:4;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET POLICY External Unencrypted Connection to BASE Console"; flow:to_server,established; uricontent:"/base_main.php";
classtype:misc-activity; reference:url,base.secureideas.net; reference:url,doc.emergingthreats.net/bin/view/Main/2008570; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_BASE; sid:2008570; rev:2;)

#this is not for a vuln, but for the use of an easily decrypted password in the clear
#by Adam Ellison. Use this if you have a policy of not showing passwords in the clear
#added negates of Anonymous and :, idea from Jon Schiedell
#
alert tcp $HOME_NET any -> any $HTTP_PORTS (msg:"ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted"; flow:established,to_server; content:"|0d 0a|Authorization|3a
20|Basic"; nocase; content:!"YW5vbnltb3VzOg=="; within:32; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2006380;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Basic_HTTP_Auth; sid:2006380; rev:10;)

#this is not for a vuln, but for the use of an easily decrypted password in the clear
#by Adam Ellison. Use this if you have a policy of not showing passwords in the clear
#added negates of Anonymous and :, idea from Jon Schiedell
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted"; flow:established,to_server; content:"|0d
0a|Authorization|3a 20|Basic"; nocase; content:!"YW5vbnltb3VzOg=="; within:32; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2006402;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Basic_HTTP_Auth; sid:2006402; rev:6;)

#Submitted by Joseph Gama
#Good rules, turn them on if you are interested. They are accurate.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY Executable and linking format (ELF) file download"; flow:established; content:"|7F|ELF"; content:"|00 00 00 00 00 00 00
00|"; classtype:policy-violation; reference:url,www.itee.uq.edu.au/~cristina/students/david/honoursThesis96/bff.htm; reference:url,doc.emergingthreats.net/bin/view/Main/2000418;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Binary_Downloads; sid:2000418; rev:11;)

#Submitted by Joseph Gama
#Good rules, turn them on if you are interested. They are accurate.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY PE EXE or DLL Windows file download"; flow: established; content:"MZ"; isdataat: 76,relative; content:"This program cannot
be run in DOS mode."; distance: 0; isdataat: 10,relative; content:"PE"; distance: 0; flowbits:set,ET.http.binary; classtype:policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2000419; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Binary_Downloads; sid:2000419; rev:12;)

#Submitted by Joseph Gama
#Good rules, turn them on if you are interested. They are accurate.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY REG files version 4 download"; flow:established; content:"REGEDIT4"; content:"|0D 0A|"; distance:0; content:"[";
distance:0; content:"HKEY_"; distance:0; nocase; classtype: misc-activity; reference:url,www.ss64.com/nt/regedit.html; reference:url,doc.emergingthreats.net/bin/view/Main/2000420;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Binary_Downloads; sid:2000420; rev:11;)

#Submitted by Joseph Gama
#Good rules, turn them on if you are interested. They are accurate.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY REG files version 5 download"; flow: established; content:"Windows Registry Editor Version 5.00"; content:"|0D 0A|";
content:"["; content:"HKEY_"; nocase; classtype: misc-activity; reference:url,www.ss64.com/nt/regedit.html; reference:url,doc.emergingthreats.net/bin/view/Main/2000421;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Binary_Downloads; sid:2000421; rev:10;)

#Submitted by Joseph Gama
#Good rules, turn them on if you are interested. They are accurate.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY REG files version 5 Unicode download"; flow: established; content:"W|00|i|00|n|00|d|00|o|00|w|00|s|00|
|00|R|00|e|00|g|00|i|00|s|00|t|00|r|00|y|00| |00|E|00|d|00|i|00|t|00|o|00|r|00| |00|V|00|e|00|r|00|s|00|i|00|o|00|n|00| |00|5|00|.|00|0|00|0|00|"; content:"|0D 0A|"; content:"[|00|";
content:"H|00|K|00|E|00|Y|00|_|00|"; nocase; classtype: misc-activity; reference:url,www.ss64.com/nt/regedit.html; reference:url,doc.emergingthreats.net/bin/view/Main/2000422;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Binary_Downloads; sid:2000422; rev:10;)

#Submitted by Joseph Gama
#Good rules, turn them on if you are interested. They are accurate.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY NE EXE OS2 file download"; flow: established; content:"MZ"; isdataat: 76,relative; content:"This program cannot be run in a
DOS session."; isdataat: 6,relative; content:"NE"; distance: 0; classtype: misc-activity; reference:url,www.itee.uq.edu.au/~cristina/students/david/honoursThesis96/bff.htm;
reference:url,doc.emergingthreats.net/bin/view/Main/2000423; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Binary_Downloads; sid:2000423; rev:10;)

#Submitted by Joseph Gama
#Good rules, turn them on if you are interested. They are accurate.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY LX EXE OS2 file download"; flow: established; content:"MZ"; isdataat: 76,relative; content:"This program cannot be run in a
DOS session."; isdataat: 6,relative; content:"LX"; distance: 0; classtype: misc-activity; reference:url,www.itee.uq.edu.au/~cristina/students/david/honoursThesis96/bff.htm;
reference:url,doc.emergingthreats.net/bin/view/Main/2000424; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Binary_Downloads; sid:2000424; rev:9;)

#Submitted by Joseph Gama
#Good rules, turn them on if you are interested. They are accurate.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY NE EXE Windows 3.x file download"; flow: established; content:"MZ"; isdataat: 76,relative; content:"This program requires
Microsoft Windows."; isdataat: 10,relative; content:"NE"; distance: 0; classtype: misc-activity; reference:url,www.itee.uq.edu.au/~cristina/students/david/honoursThesis96/bff.htm;
reference:url,doc.emergingthreats.net/bin/view/Main/2000425; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Binary_Downloads; sid:2000425; rev:9;)
```

```
#Submitted by Joseph Gama
#Good rules, turn them on if you are interested. They are accurate.
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY EXE compressed PKWARE Windows file download"; flow: established; content:"MZ"; isdataat: 28,relative; content:"PKLITE";
distance: 0; classtype: misc-activity; reference:url,www.program-transformation.org/Transform/PcExeFormat; reference:url,doc.emergingthreats.net/bin/view/Main/2000426;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Binary_Downloads; sid:2000426; rev:9;)

#by jaime blasco
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY PE EXE or DLL Windows file download (2)"; flow:established; content:"MZ"; isdataat:76,relative; content:"Windows Program";
distance:0; isdataat:10,relative; content:"PE"; distance:0; flowbits:set,ET.http.binary; classtype:policy-violation; reference:url,doc.emergingthreats.net/2010869;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Binary_Downloads; sid:2010869; rev:2;)

#Disabling as it overlaps with 2000419
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY PE EXE Install Windows file download"; flow: established; content:"MZ"; isdataat: 76,relative; content:"This program must
be "; distance: 0; isdataat: 140,relative; content:"PE"; distance: 0; flowbits:set,ET.http.binary; classtype:policy-violation; reference:url,www.program-
transformation.org/Transform/PcExeFormat; reference:url,doc.emergingthreats.net/bin/view/Main/2000427; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Binary_Downloads; sid:2000427; rev:12;)

#Disabling as it overlaps with 2000419
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY ZIP file download"; flow: established; content:"PK|0304|"; byte_test:1, <=, 0x14, 0, string, hex; content:"|00 00 00|";
distance: 0; classtype: misc-activity; reference:url,zziplib.sourceforge.net/zzip-parse.print.html; reference:url,doc.emergingthreats.net/bin/view/Main/2000428;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Binary_Downloads; sid:2000428; rev:10;)

#Disabling as it overlaps with 2000419
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY Download Windows Help File CHM"; flow: established; content:"ITSF|03|"; isdataat: 19,relative; content:"|7C 01 FD 10 7B AA
11 D0 9E 0C 00 A0 C9 22 E6 EC 7C 01 FD 11 7B AA 11 D0 9E 0C 00 A0 C9 22 E6 EC|"; distance: 0; classtype: misc-activity; reference:url,www.speakeasy.org/~russotto/chm/chmformat.html;
reference:url,www.securiteam.com/windowsntfocus/6V00N000AU.html; reference:url,doc.emergingthreats.net/bin/view/Main/2000489; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Binary_Downloads; sid:2000489; rev:9;)

#Disabling as it overlaps with 2000419
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY Download Windows Help File CHM 2"; flow: established; content:"ITSF|03|"; isdataat: 19,relative; content:"|10 FD 01 7C AA
7B D0 11 9E 0C 00 A0 C9 22 E6 EC 11 FD 01 7C AA 7B D0 11 9E 0C 00 A0 C9 22 E6 EC|"; distance: 0; classtype: misc-activity; reference:url,www.speakeasy.org/~russotto/chm/chmformat.html;
reference:url,www.securiteam.com/windowsntfocus/6V00N000AU.html; reference:url,doc.emergingthreats.net/bin/view/Main/2000429; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Binary_Downloads; sid:2000429; rev:9;)

#Disabling as it overlaps with 2000419
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY MSI (microsoft installer file) download"; flow:established; content:"|D0 CF 11 E0 A1 B1 1A E1|"; classtype: bad-unknown;
reference:url,doc.emergingthreats.net/bin/view/Main/2001115; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Binary_Downloads; sid:2001115; rev:7;)

#this sig JUST gets updates from external_net
#
alert udp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"ET POLICY DNS Update From External net"; byte_test:1,&,40,2; classtype:policy-violation; reference:url,doc.emergingthreats.net/2009702;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Bind; sid:2009702; rev:4;)

#Idea by David Glosser, sig by Matt Jonkman
#
#alert ip [0.0.0.0/8,39.0.0.0/8] any -> $HOME_NET any (msg:"ET POLICY Reserved IP Space Traffic - Bogon Nets 1"; classtype:bad-unknown; threshold: type limit, track by_src, count 1,
seconds 360; reference:url,www.cymru.com/Documents/bogon-list.html; reference:url,doc.emergingthreats.net/bin/view/Main/2002749; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Bogon_Nets; sid:2002749; rev:13;)

#Idea by David Glosser, sig by Matt Jonkman
#
#alert ip [102.0.0.0/7,104.0.0.0/8,106.0.0.0/8,179.0.0.0/8,185.0.0.0/8] any -> $HOME_NET any (msg:"ET POLICY Reserved IP Space Traffic - Bogon Nets 2"; classtype:bad-unknown; threshold:
type limit, track by_src, count 1, seconds 360; reference:url,www.cymru.com/Documents/bogon-list.html; reference:url,doc.emergingthreats.net/bin/view/Main/2002750;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Bogon_Nets; sid:2002750; rev:26;)

#Idea by David Glosser, sig by Matt Jonkman
#
#alert ip [192.0.0.0/24,192.0.2.0/24,198.18.0.0/15,198.51.100.0/24,203.0.113.0/24] any -> $HOME_NET any (msg:"ET POLICY Reserved IP Space Traffic - Bogon Nets 3"; classtype:bad-unknown;
threshold: type limit, track by_src, count 1, seconds 360; reference:url,www.cymru.com/Documents/bogon-list.html; reference:url,doc.emergingthreats.net/bin/view/Main/2002751;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Bogon_Nets; sid:2002751; rev:8;)

#This is for reserved internal space. Do NOT run this sig on your internal net, commented out by default.
#
#alert ip [10.0.0.0/8,169.254.0.0/16,172.16.0.0/12,192.168.0.0/16] any -> $HOME_NET any (msg:"ET POLICY Reserved Internal IP Traffic"; classtype:bad-unknown; threshold: type limit,
track by_src, count 1, seconds 360; reference:url,www.cymru.com/Documents/bogon-list.html; reference:url,doc.emergingthreats.net/bin/view/Main/2002752;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Bogon_Nets; sid:2002752; rev:4;)

#this is a distributed search engine crawling thing. I am not aware of any spyware-like activity, but it is likely not welcome on a corporate net
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Boitho.com Distributed Crawler in use - User-Agent (boitho.com-dc)"; flow:to_server,established; content:"|0d
0a|User-Agent|3a| boitho.com"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/2003653; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Boitho.com; sid:2003653; rev:4;)

#ccproxy is a legitimate program, but has been seen in use by malware to proxy remote http
#it's aproduct designed for internal network use. Run this sig externally to detect it in use remotely.
#This would likely be hostile activity
#by Matt Jonkman from sandnet analysis
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET POLICY CCProxy in use remotely - Possibly Hostile/Malware"; flow:established,from_server; content:" 200 Connection
established|0d 0a|Proxy-agent|3a| CCProxy "; depth:58; classtype:trojan-activity; reference:url,www.youngzsoft.net; reference:url,doc.emergingthreats.net/bin/view/Main/2007576;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_CCProxy; sid:2007576; rev:4;)

#by christopher Campesi
#
#alert tcp $HOME_NET any -> 38.97.75.0/24 443 (msg:"ET POLICY Carbonite Online Backup SSL Handshake"; flow:established,to_server; content:"CarboniteInc"; offset:56; classtype:policy-
violation; reference:url,doc.emergingthreats.net/2009798; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Carbonite; sid:2009798; rev:2;)

#by evilghost
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Carbonite.com Backup Software Leaking MAC Address"; flow:established,to_server; content:"GET "; depth:4;
uricontent:"/manage.old/sun/signup.aspx?MACAddresses=MAC"; nocase; uricontent:"ShowCount="; nocase; classtype:policy-violation; reference:url,doc.emergingthreats.net/2009800;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Carbonite; sid:2009800; rev:3;)

#by eoin miller
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Carbonite.com Backup Software User-Agent (Carbonite Installer)"; flow:established,to_server; content:"GET ";
depth:4; nocase; content:"|0d 0a|User-Agent|3a| Carbonite Installer|0d 0a|"; nocase; classtype:policy-violation; reference:url,doc.emergingthreats.net/2009801;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Carbonite; sid:2009801; rev:3;)

#online tools
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY Centralops.net Domain Dossier Utility Probe"; flow:established,to_server; content:"USER-Agent|3a| Domain Dossier
utility (http|3a|//CentralOps.net/)"; nocase; classtype:policy-violation; reference:url,centralops.net; reference:url,doc.emergingthreats.net/bin/view/Main/2003623;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Centralops.net; sid:2003623; rev:4;)

#online tools
#
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY Centralops.net Probe"; flow:established,to_server; content:"USER-Agent|3a| "; nocase; content:"CentralOps.net/)";
within:100; nocase; classtype:policy-violation; reference:url,centralops.net; reference:url,doc.emergingthreats.net/bin/view/Main/2003631; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Centralops.net; sid:2003631; rev:4;)

#Submitted by Matt Jonkman
#
```

```
alert tcp $HOME_NET 23 -> any any (msg:"ET POLICY Cisco Device in Config Mode"; flow: established; content:"Enter configuration commands, one per line"; nocase; classtype: not-
suspicious; reference:url,doc.emergingthreats.net/bin/view/Main/2001239; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Cisco; sid:2001239; rev:9;)

#Submitted by Matt Jonkman
#
alert tcp $HOME_NET 23 -> any any (msg:"ET POLICY Cisco Device New Config Built"; flow: established; content:"Building configuration..."; nocase; classtype: not-suspicious;
reference:url,doc.emergingthreats.net/bin/view/Main/2001240; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Cisco; sid:2001240; rev:9;)

#by Kevin Ross
#
alert tcp $HOME_NET 23 -> $EXTERNAL_NET any (msg:"ET TELNET External Telnet Attempt To Cisco Device With No Telnet Password Set (Automatically Dissalowed Until Password Set)";
flow:from_server; content:"Password required, but none set"; depth:31; classtype:misc-activity; reference:url,articles.techrepublic.com.com/5100-10878_11-5875046.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2008860; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Cisco; sid:2008860; rev:3;)

#by Kevin Ross
#
#alert tcp $HOME_NET 23 -> $EXTERNAL_NET any (msg:"ET TELNET External Telnet Login To Cisco Device"; flow:from_server,established; content:"User Access Verification"; classtype:misc-
activity; depth:24; reference:url,articles.techrepublic.com.com/5100-10878_11-5875046.html; reference:url,doc.emergingthreats.net/bin/view/Main/2008861;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Cisco; sid:2008861; rev:3;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY External Access to Cisco Aironet AP Over HTTP (Post Authentication)"; flow:to_server,established;
uricontent:"/ap_home.html"; classtype:misc-activity; reference:url,supportwiki.cisco.com/ViewWiki/index.php/How_to_configure_HTTPS_on_the_AP;
reference:url,doc.emergingthreats.net/bin/view/Main/2008862; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Cisco; sid:2008862; rev:2;)

#By Cory Bys, Particle.bored.
#These are going to increase load on a snort process, and are NOT FOOLPROOF. But they may help reveal issues
#with informaion flow. NOTE: These will not detect classified UUEncoded docs (email attachments) etc.
#Email
#Non-US Restricted
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Non-US Restricted Outbound"; flow:to_server,established; content:"Subject|3A|"; pcre:"///([A-Z]
{3}\s)+RESTRICTED//X5/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002410; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002410; rev:3;)

#Non-US Confidential
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Non-US Confidential Outbound"; flow:to_server,established; content:"Subject|3A|"; pcre:"///([A-Z]
{3}\s)+CONFIDENTIAL//X5/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002411; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002411; rev:3;)

#Non-US Top Secret
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Non-US Top Secret Outbound"; flow:to_server,established; content:"Subject|3A|"; pcre:"///([A-Z]
{3}\s)+TOP\sSECRET//X5/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002412; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002412; rev:3;)

#Non-US Secret
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Non-US Secret"; flow:to_server,established; content:"Subject|3A|"; pcre:"///([A-Z]{3}\s)+(?<!TOP\s)SECRET//X5/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002413; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002413; rev:3;)

#NATO Restricted
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP NATO Restricted"; flow:to_server,established; content:"Subject|3A|"; pcre:"////(NATO\sRESTRICTED)|NR)//MR/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002414; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002414; rev:3;)

#NATO Confidential Atomal
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP NATO Confidential Atomal"; flow:to_server,established; content:"Subject|3A|";
pcre:"////((NATO\sCONFIDENTIAL\sATOMAL)|NCA)//MR/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002415; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002415; rev:3;)

#NATO Confidential
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP NATO Confidential"; flow:to_server,established; content:"Subject|3A|"; pcre:"////((NATO\sCONFIDENTIAL)|NC)//MR/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002416; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002416; rev:3;)

#NATO COSMIC Top Secret Atomal
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP NATO COSMIC Top Secret Atomal"; flow:to_server,established; content:"Subject|3A|";
pcre:"////((COSMIC\sTOP\sSECRET\sATOMAL)|CTSA)//MR/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002417;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002417; rev:3;)

#NATO Secret Atomal
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP NATO Secret Atomal"; flow:to_server,established; content:"Subject|3A|";
pcre:"////((NATO\sSECRET\sATOMAL)|NSA)//MR/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002418; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002418; rev:3;)

#NATO Secret
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP NATO Secret"; flow:to_server,established; content:"Subject|3A|"; pcre:"////((NATO\sSECRET)|NS)//MR/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002419; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002419; rev:3;)

#US Confidential, Electronic Format
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Confidential, Electronic"; flow:to_server,established; content:"Subject|3A|"; pcre:"/QQQQ\r\n(?=
(O|P|R|Z)\r\n(CC)\r\n)/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002420; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002420; rev:3;)

#US Top Secret, Electronic Format
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Top Secret, Electronic"; flow:to_server,established; content:"Subject|3A|"; pcre:"/QQQQ\r\n(?=
(O|P|R|Z)\r\n(TT)\r\n)/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002421; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002421; rev:3;)

#US Secret, Electronic Format
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Secret, Electronic"; flow:to_server,established; content:"Subject|3A|"; pcre:"/QQQQ\r\n(?=
(O|P|R|Z)\r\n(SS)\r\n)/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002422; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002422; rev:3;)

#US Confidential Authorized for Release To
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Confidential REL TO"; flow:to_server,established; content:"Subject|3A|";
pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*REL\sTO\sUSA[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002423;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002423; rev:3;)

#US Top Secret Authorized for Release To
#
```

```
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Top Secret REL TO"; flow:to_server,established; content:"Subject|3A|";
pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*REL\sTO\sUSA[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002424;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002424; rev:3;)

#US Secret Authorized for Release To
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Secret REL TO"; flow:to_server,established; content:"Subject|3A|"; pcre:"/(?<!TOP\s|T)
(SECRET|S)//[\s\w,/-]*REL\sTO\sUSA[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002425;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002425; rev:3;)

#US Confidential Comint
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Confidential COMINT"; flow:to_server,established; content:"Subject|3A|"; pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*
(COMINT|SI)[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002426; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002426; rev:3;)

#US Top Secret Comint
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Top Secret COMINT"; flow:to_server,established; content:"Subject|3A|"; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*
(COMINT|SI)[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002427; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002427; rev:3;)

#US Secret Comint
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Secret COMINT"; flow:to_server,established; content:"Subject|3A|"; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*
(COMINT|SI)[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002428; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002428; rev:3;)

#US Unclassified Communications Security Material
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Unclassified COMSEC"; flow:to_server,established; content:"Subject|3A|";
pcre:"/(UNCLASSIFIED|U)//[\s\w,/-]*COMSEC[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002429;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002429; rev:3;)

#US Confidential Communications Security Material
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Confidential COMSEC"; flow:to_server,established; content:"Subject|3A|";
pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*COMSEC[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002430;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002430; rev:3;)

#US Top Secret Communications Security Material
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Top Secret COMSEC"; flow:to_server,established; content:"Subject|3A|";
pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*COMSEC[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002431;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002431; rev:3;)

#US Secret Communications Security Material
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Secret COMSEC"; flow:to_server,established; content:"Subject|3A|"; pcre:"/(?<!TOP\s|T)
(SECRET|S)//[\s\w,/-]*COMSEC[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002432;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002432; rev:3;)

#US Controlled Imagery
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Secret IMCON"; flow:to_server,established; content:"Subject|3A|"; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*
(IMCON|IMC)[\s\w,/-]*(?=//(X1|MR))/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002433; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002433; rev:3;)

#US Top Secret Critical Nuclear Weapon Design Information
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Top Secret CNWDI"; flow:to_server,established; content:"Subject|3A|"; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*
(CRITICAL\sNUCLEAR\sWEAPON\sDESIGN\sINFORMATION|CNWDI)[\s\w,/-]*(?=//MR)/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002434;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002434; rev:3;)

#US Secret Critical Nuclear Weapon Design Information
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Secret CNWDI"; flow:to_server,established; content:"Subject|3A|"; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*
(CRITICAL\sNUCLEAR\sWEAPON\sDESIGN\sINFORMATION|CNWDI)[\s\w,/-]*(?=//MR)/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002435;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002435; rev:3;)

#US Top Secret Talent Keyhole
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Top Secret TK"; flow:to_server,established; content:"Subject|3A|"; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*
(TALENT\sKEYHOLE|TK)[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002436; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002436; rev:3;)

#US Secret Talent Keyhole
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Secret TK"; flow:to_server,established; content:"Subject|3A|"; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*
(TALENT\sKEYHOLE|TK)[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002437; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002437; rev:3;)

#US Foreign Government Information
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US FGI"; flow:to_server,established; content:"Subject|3A|"; pcre:"///FGI[\s\w,/-]*(?=//X5)/ism"; classtype:policy-
violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002438; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002438;
rev:3;)

#US For Official Use Only
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US FOUO"; flow:to_server,established; content:"Subject|3A|";
pcre:"/(UNCLASSIFIED|U)//(FOR\sOFFICIAL\sUSE\sONLY|FOUO)/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002439;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002439; rev:3;)

#US Confidential Not Releasable to Foreign Nationals
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Confidential NOFORN"; flow:to_server,established; content:"Subject|3A|";
pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*NOFORN[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002440;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002440; rev:3;)

#US Top Secret Not Releasable to Foreign Nationals
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Top Secret NOFORN"; flow:to_server,established; content:"Subject|3A|";
pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*NOFORN[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002441;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002441; rev:3;)

#US Secret Not Releasable to Foreign Nationals
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Secret NOFORN"; flow:to_server,established; content:"Subject|3A|"; pcre:"/(?<!TOP\s|T)
(SECRET|S)//[\s\w,/-]*NOFORN[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002442;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002442; rev:3;)

#US Confidential Originator Controlled
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Confidential ORCON"; flow:to_server,established; content:"Subject|3A|"; pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*
(ORIGINATOR\sCONTROLLED|ORCON)[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002443;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002443; rev:3;)

#US Top Secret Originator Controlled
#
```

```
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Top Secret ORCON"; flow:to_server,established; content:"Subject|3A|"; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*
(ORIGINATOR\sCONTROLLED|ORCON)[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002444;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002444; rev:3;)

#US Secret Originator Controlled
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Secret ORCON"; flow:to_server,established; content:"Subject|3A|"; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*
(ORIGINATOR\sCONTROLLED|ORCON)[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002445;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002445; rev:3;)

#US Unclassified Proprietary Information
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Unclassified PROPIN"; flow:to_server,established; content:"Subject|3A|";
pcre:"/(UNCLASSIFIED|U)//[\s\w,/-]*PROPIN[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002446;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002446; rev:3;)

#US Confidential Proprietary Information
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Confidential PROPIN"; flow:to_server,established; content:"Subject|3A|";
pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*PROPIN[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002447;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002447; rev:3;)

#US Top Secret Proprietary Information
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Top Secret PROPIN"; flow:to_server,established; content:"Subject|3A|";
pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*PROPIN[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002448;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002448; rev:3;)

#US Secret Proprietary Information
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Secret PROPIN"; flow:to_server,established; content:"Subject|3A|"; pcre:"/(?<!TOP\s|T)
(SECRET|S)//[\s\w,/-]*PROPIN[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002449;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002449; rev:3;)

#US Confidential Restricted Data
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Confidential RD"; flow:to_server,established; content:"Subject|3A|"; pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*
(RESTRICTED\sDATA|RD)[\s\w,/-]*(?=//MR)/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002450; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002450; rev:3;)

#US Top Secret Restricted Data
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Top Secret RD"; flow:to_server,established; content:"Subject|3A|"; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*
(RESTRICTED\sDATA|RD)[\s\w,/-]*(?=//MR)/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002451; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002451; rev:3;)

#US Secret Restricted Data
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Secret RD"; flow:to_server,established; content:"Subject|3A|"; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*
(RESTRICTED\sDATA|RD)[\s\w,/-]*(?=//MR)/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002452; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002452; rev:3;)

#US Sources and Methods Information
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US SAMI"; flow:to_server,established; content:"Subject|3A|"; pcre:"/SAMI[\s\w,/-]*(?=//(25)?X[1-9])/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002453; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002453; rev:3;)

#US Confidential Special Category
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Confidential SPECAT"; flow:to_server,established; content:"Subject|3A|";
pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*SPECAT[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002454;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002454; rev:3;)

#US Top Secret Special Category
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Top Secret SPECAT"; flow:to_server,established; content:"Subject|3A|";
pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*SPECAT[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002455;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002455; rev:3;)

#US Secret Special Category
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Secret SPECAT"; flow:to_server,established; content:"Subject|3A|"; pcre:"/(?<!TOP\s|T)
(SECRET|S)//[\s\w,/-]*SPECAT[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002456;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002456; rev:3;)

#US Top Secret Single Integrated Operations Plan
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP US Top Secret STOP"; flow:to_server,established; content:"Subject|3A|";
pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*STOP[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002457;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002457; rev:3;)

#The word "private"
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Private"; flow:to_server,established; content:"Subject|3A|"; pcre:"/\Wprivate\W(?!/(25)?X[1-9])/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002458; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002458; rev:3;)

#The word "restricted"
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Restricted"; flow:to_server,established; content:"Subject|3A|"; pcre:"/(?<!//)\Wrestricted[^\w/]/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002459; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002459; rev:3;)

#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Secret"; flow:to_server,established; content:"Subject|3A|"; pcre:"/(?<!TOP|//)\Wsecret[^\w/a]/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002461; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002461; rev:4;)

#The phrase "top secret"
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Top Secret"; flow:to_server,established; content:"Subject|3A|"; pcre:"/(?<!//)\Wtop\ssecret[^\w/a]/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002462; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002462; rev:3;)

#The word "sealed"
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Sealed"; flow:to_server,established; content:"Subject|3A|"; pcre:"/\Wsealed\W(?!/(25)?X[1-9])/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002463; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002463; rev:3;)

#The word "sensitive"
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Sensitive"; flow:to_server,established; content:"Subject|3A|"; pcre:"/(?<!law\senforcement)\Wsensitive\W(?!/(25)?
X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002464; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002464; rev:3;)

#The word "proprietary"
#
```

```
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Proprietary"; flow:to_server,established; content:"Subject|3A|"; pcre:"/\Wproprietary\W(?!/(25)?X[1-9])/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002465; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002465; rev:3;)

#The word "protected"
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Protected"; flow:to_server,established; content:"Subject|3A|"; pcre:"/\Wprotected\W(?!/(25)?X[1-9])/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002466; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002466; rev:3;)

#The phrase "law enforcement sensitive"
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Law Enorcement Sensitive"; flow:to_server,established; content:"Subject|3A|";
pcre:"/\Wlaw\senforcement\ssensitive\W/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002467; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002467; rev:3;)

#The phrase "internal use only"
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Internal Use Only"; flow:to_server,established; content:"Subject|3A|"; pcre:"/\Winternal\suse\sonly\W/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002468; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002468; rev:3;)

#The phrase "date of birth" or its typical abbreviations
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Date of Birth"; flow:to_server,established; content:"Subject|3A|"; pcre:"/[^\w&]d(ate)?(-)?o(f)?(-)?b(irth)?
\W[\s\w,/-]*(?=([0-9]{2}[-/][0-9]{2}[-/][0-9]{2,4})|[0-9]{8})/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002469;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002469; rev:3;)

#Health Care Common Procedure Coding System (HCPCS) Codes
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP HCPCS Code"; flow:to_server,established; content:"Subject|3A|"; pcre:"/\Whcpcs\W[\s\w,/-]*(?=[a-z][0-9]{10})/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002470; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002470; rev:3;)

#International Statistical Classification of Diseases and Related Health Problems 10th Revision (ICD-10) Codes
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP ICD-10 Code"; flow:to_server,established; content:"Subject|3A|"; pcre:"/\Wicd\W[\s\w,/-]*(?=[a-z][0-9]{2}\.[0-9]
{2})/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002471; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002471; rev:3;)

#Food and Drug Administration (FDA) National Drug Code (NDC) Codes
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP FDA NDC Code"; flow:to_server,established; content:"Subject|3A|"; pcre:"/\Wndc\W[\s\w,/-]*(?=([0-9]{4}-[0-9]{4}-[0-
9]{2}|[0-9]{5}-[0-9]{3}-[0-9]{2}|[0-9]{5}-[0-9]{4}-[0-9]{1,2}))/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002472;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002472; rev:3;)

#American Dental Association (ADA) Dental Procedure Codes
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP ADA Procedure Code"; flow:to_server,established; content:"Subject|3A|"; pcre:"/\Wada\W[\s\w,/-]*(?=d[0-9]{4})/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002473; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002473; rev:3;)

#Diagnostic and Statistical Manual of Mental Disorders (DSM-IV) Codes
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP DSM-IV Code"; flow:to_server,established; content:"Subject|3A|"; pcre:"/\Wdsm\W[\s\w,/-]*(?=([2-9][0-9]{2}(\.[0-9]
{1,2}?)|(v[167][0-9]\.[0-9]{1,2})))/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002474; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002474; rev:5;)

#American Medical Association (AMA) Current Procedural Terminology (CPT) Codes
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP AMA CPT Code"; flow:to_server,established; content:"Subject|3A|"; pcre:"/\Wcpt\W[\s\w,/-]*(?=[0-9]{4}[ft]|[0-9]
{5})/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002475; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002475; rev:3;)

#Japan Credit Bureau Credit Card Number
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Credit Card, JCB"; flow:to_server,established; content:"Subject|3A|"; pcre:"/\Wj(apan\s)?c(redit\s)?b(ureau)?
\W[\s\w,/-]*(?=(3[12359][0-9]{14})|(1800|2131)[0-9]{11})/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002477;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002477; rev:3;)

#The word "password", its typical abbreviations or written/abbreviated in a few forms of "leet"
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Password"; flow:to_server,established; content:"Subject|3A|"; pcre:"/\W[p][a4@][sz5]{0,2}[w]([o0][r])?[d]\W/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002483; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002483; rev:3;)

#The word "appraisal"
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Appraisal"; flow:to_server,established; content:"Subject|3A|"; pcre:"/\Wappraisal(s)?\W/ism"; classtype:policy-
violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002484; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002484;
rev:3;)

#The phrase "account balance"
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Account Balance"; flow:to_server,established; content:"Subject|3A|"; pcre:"/\Waccount\sbalance(s)?\W/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002485; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002485; rev:3;)

#The phrase "payment history"
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Payment History"; flow:to_server,established; content:"Subject|3A|"; content:"payment history"; nocase;
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002486; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002486; rev:4;)

#The phrase "annual income"
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Annual Income"; flow:to_server,established; content:"Subject|3A|"; pcre:"/\Wannual\sincome(s)?\W/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002487; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002487; rev:4;)

#The phrase "credit history"
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Credit History"; flow:to_server,established; content:"Subject|3A|"; pcre:"/\Wcredit\shistor(y|ies)\W/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002488; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002488; rev:3;)

#The phrase "transaction history"
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Transaction History"; flow:to_server,established; content:"Subject|3A|";
pcre:"/\Wtransaction\shistor(y|ies)\W/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002489; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002489; rev:3;)

#The phrase "customer list"
#
#alert tcp $SMTP_SERVERS any -> $EXTERNAL_NET 25 (msg:"ET POLICY SMTP Customer List"; flow:to_server,established; content:"Subject|3A|"; pcre:"/\Wcustomer\slist(s)?\W/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002490; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002490; rev:3;)

########################################
```

```
#HTTP POST
#Non-US Restricted
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP Non-US Restricted"; flow:to_server,established; pcre:"////([A-Z]{3}\s)+RESTRICTED//X5/ism"; classtype:policy-
violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002495; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002495;
rev:4;)

#Non-US Confidential
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Non-US Confidential"; flow:to_server,established; pcre:"////([A-Z]{3}\s)+CONFIDENTIAL//X5/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002496; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002496; rev:4;)

#Non-US Top Secret
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Non-US Top Secret"; flow:to_server,established; pcre:"////([A-Z]{3}\s)+TOP\sSECRET//X5/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002497; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002497; rev:4;)

#Non-US Secret
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Non-US Secret"; flow:to_server,established; pcre:"////([A-Z]{3}\s)+(?<!TOP\s)SECRET//X5/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002498; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002498; rev:4;)

#NATO Restricted
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - NATO Restricted"; flow:to_server,established; pcre:"////((NATO\sRESTRICTED)|NR)//MR/ism"; classtype:policy-
violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002499; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002499;
rev:4;)

#NATO Confidential Atomal
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - NATO Confidential Atomal"; flow:to_server,established; pcre:"////((NATO\sCONFIDENTIAL\sATOMAL)|NCA)//MR/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002500; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002500; rev:4;)

#NATO Confidential
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - NATO Confidential"; flow:to_server,established; pcre:"////((NATO\sCONFIDENTIAL)|NC)//MR/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002501; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002501; rev:4;)

#NATO COSMIC Top Secret Atomal
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - NATO COSMIC Top Secret Atomal"; flow:to_server,established;
pcre:"////((COSMIC\sTOP\sSECRET\sATOMAL)|CTSA)//MR/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002502;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002502; rev:4;)

#NATO Secret Atomal
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - NATO Secret Atomal"; flow:to_server,established; pcre:"////((NATO\sSECRET\sATOMAL)|NSA)//MR/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002503; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002503; rev:4;)

#NATO Secret
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - NATO Secret"; flow:to_server,established; pcre:"////((NATO\sSECRET)|NS)//MR/ism"; classtype:policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2002504; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002504; rev:4;)

#US Confidential, Electronic Format
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Confidential, Electronic"; flow:to_server,established; pcre:"/QQQQ\r\n(?=(O|P|R|Z)\r\n(CC)\r\n)/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002505; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002505; rev:4;)

#US Top Secret, Electronic Format
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Top Secret, Electronic"; flow:to_server,established; pcre:"/QQQQ\r\n(?=(O|P|R|Z)\r\n(TT)\r\n)/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002506; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002506; rev:4;)

#US Secret, Electronic Format
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Secret, Electronic"; flow:to_server,established; pcre:"/QQQQ\r\n(?=(O|P|R|Z)\r\n(SS)\r\n)/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002507; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002507; rev:4;)

#US Confidential Authorized for Release To
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Confidential REL TO"; flow:to_server,established;
pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*REL\sTO\sUSA[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002508;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002508; rev:4;)

#US Top Secret Authorized for Release To
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Top Secret REL TO"; flow:to_server,established; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*REL\sTO\sUSA[\s\w,/-]*
(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002509; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002509; rev:4;)

#US Secret Authorized for Release To
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Secret REL TO"; flow:to_server,established; pcre:"/(?<!TOP\s|T)
(SECRET|S)//[\s\w,/-]*REL\sTO\sUSA[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002510;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002510; rev:4;)

#US Confidential Comint
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Confidential COMINT"; flow:to_server,established; pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*(COMINT|SI)
[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002511; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002511; rev:4;)

#US Top Secret Comint
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Top Secret COMINT"; flow:to_server,established; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*(COMINT|SI)[\s\w,/-]*
(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002512; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002512; rev:4;)

#US Secret Comint
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Secret COMINT"; flow:to_server,established; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*(COMINT|SI)
[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002513; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002513; rev:4;)

#US Unclassified Communications Security Material
#
```

```
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Unclassified COMSEC"; flow:to_server,established; pcre:"/(UNCLASSIFIED|U)//[\s\w,/-]*COMSEC[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002514; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002514; rev:4;)

#US Confidential Communications Security Material
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Confidential COMSEC"; flow:to_server,established; pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*COMSEC[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002515; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002515; rev:4;)

#US Top Secret Communications Security Material
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Top Secret COMSEC"; flow:to_server,established; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*COMSEC[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002516; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002516; rev:4;)

#US Secret Communications Security Material
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Secret COMSEC"; flow:to_server,established; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*COMSEC[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002517; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002517; rev:4;)

#US Controlled Imagery
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Secret IMCON"; flow:to_server,established; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*(IMCON|IMC)[\s\w,/-]*(?=//(X1|MR))/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002518; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002518; rev:4;)

#US Top Secret Critical Nuclear Weapon Design Information
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Top Secret CNWDI"; flow:to_server,established; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*(CRITICAL\sNUCLEAR\sWEAPON\sDESIGN\sINFORMATION|CNWDI)[\s\w,/-]*(?=//MR)/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002519; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002519; rev:4;)

#US Secret Critical Nuclear Weapon Design Information
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Secret CNWDI"; flow:to_server,established; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*(CRITICAL\sNUCLEAR\sWEAPON\sDESIGN\sINFORMATION|CNWDI)[\s\w,/-]*(?=//MR)/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002520; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002520; rev:4;)

#US Top Secret Talent Keyhole
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Top Secret TK"; flow:to_server,established; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*(TALENT\sKEYHOLE|TK)[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002521; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002521; rev:4;)

#US Secret Talent Keyhole
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Secret TK"; flow:to_server,established; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*(TALENT\sKEYHOLE|TK)[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002522; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002522; rev:4;)

#US Foreign Government Information
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US FGI"; flow:to_server,established; pcre:"///FGI[\s\w,/-]*(?=//X5)/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002523; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002523; rev:4;)

#US For Official Use Only
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US FOUO"; flow:to_server,established; pcre:"/(UNCLASSIFIED|U)//(FOR\sOFFICIAL\sUSE\sONLY|FOUO)/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002524; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002524; rev:4;)

#US Confidential Not Releasable to Foreign Nationals
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Confidential NOFORN"; flow:to_server,established; pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*NOFORN[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002525; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002525; rev:4;)

#US Top Secret Not Releasable to Foreign Nationals
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Top Secret NOFORN"; flow:to_server,established; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*NOFORN[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002526; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002526; rev:4;)

#US Secret Not Releasable to Foreign Nationals
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Secret NOFORN"; flow:to_server,established; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*NOFORN[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002527; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002527; rev:4;)

#US Confidential Originator Controlled
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Confidential ORCON"; flow:to_server,established; pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*(ORIGINATOR\sCONTROLLED|ORCON)[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002704; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002704; rev:3;)

#US Top Secret Originator Controlled
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Top Secret ORCON"; flow:to_server,established; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*(ORIGINATOR\sCONTROLLED|ORCON)[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002528; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002528; rev:4;)

#US Secret Originator Controlled
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Secret ORCON"; flow:to_server,established; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*(ORIGINATOR\sCONTROLLED|ORCON)[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002529; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002529; rev:4;)

#US Unclassified Proprietary Information
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Unclassified PROPIN"; flow:to_server,established; pcre:"/(UNCLASSIFIED|U)//[\s\w,/-]*PROPIN[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002530; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002530; rev:4;)

#US Confidential Proprietary Information
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Confidential PROPIN"; flow:to_server,established; pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*PROPIN[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002531; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002531; rev:4;)

#US Top Secret Proprietary Information
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Top Secret PROPIN"; flow:to_server,established; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*PROPIN[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002532; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002532; rev:4;)

#US Secret Proprietary Information
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Secret PROPIN"; flow:to_server,established; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*PROPIN[\s\w,/-]*(?
```

```
=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002533; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002533; rev:4;)

#US Confidential Restricted Data
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Confidential RD"; flow:to_server,established; pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*(RESTRICTED\sDATA|RD)
[\s\w,/-]*(?=//MR)/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002534; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002534; rev:4;)

#US Top Secret Restricted Data
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Top Secret RD"; flow:to_server,established; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*(RESTRICTED\sDATA|RD)
[\s\w,/-]*(?=//MR)/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002535; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002535; rev:4;)

#US Secret Restricted Data
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Secret RD"; flow:to_server,established; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*(RESTRICTED\sDATA|RD)
[\s\w,/-]*(?=//MR)/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002536; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002536; rev:4;)

#US Sources and Methods Information
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US SAMI"; flow:to_server,established; pcre:"/SAMI[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-
violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002537; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002537;
rev:4;)

#US Confidential Special Category
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Confidential SPECAT"; flow:to_server,established; pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*SPECAT[\s\w,/-]*(?
=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002538; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002538; rev:4;)

#US Top Secret Special Category
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Top Secret SPECAT"; flow:to_server,established; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*SPECAT[\s\w,/-]*(?
=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002539; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002539; rev:4;)

#US Secret Special Category
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Secret SPECAT"; flow:to_server,established; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*SPECAT[\s\w,/-]*(?
=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002540; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002540; rev:4;)

#US Top Secret Single Integrated Operations Plan
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - US Top Secret STOP"; flow:to_server,established; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*STOP[\s\w,/-]*(?=//(25)?
X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002541; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002541; rev:4;)

#The word "private"
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Private"; flow:to_server,established; pcre:"/\Wprivate\W(?!/(25)?X[1-9])/ism"; classtype:policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2002542; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002542; rev:4;)

#The word "restricted"
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Restricted"; flow:to_server,established; pcre:"/(?<!//)\Wrestricted[^\w/]/ism"; classtype:policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2002543; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002543; rev:4;)

#The word "confidential"
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Confidential"; flow:to_server,established; pcre:"/(?<!//)\Wconfidential[^\w/]/ism"; classtype:policy-
violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002544; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002544;
rev:4;)

#The word "secret"
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Secret"; flow:to_server,established; pcre:"/(?<!TOP|//)\Wsecret[^\w/a]/ism"; classtype:policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2002545; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002545; rev:4;)

#The phrase "top secret"
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Top Secret"; flow:to_server,established; pcre:"/(?<!//)\Wtop\ssecret[^\w/a]/ism"; classtype:policy-
violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002546; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002546;
rev:4;)

#The word "sealed"
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Sealed"; flow:to_server,established; pcre:"/\Wsealed\W(?!/(25)?X[1-9])/ism"; classtype:policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2002547; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002547; rev:4;)

#The word "sensitive"
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Sensitive"; flow:to_server,established; pcre:"/(?<!law\senforcement)\Wsensitive\W(?!/(25)?X[1-9])/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002548; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002548; rev:4;)

#The word "proprietary"
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Proprietary"; flow:to_server,established; pcre:"/\Wproprietary\W(?!/(25)?X[1-9])/ism"; classtype:policy-
violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002549; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002549;
rev:4;)

#The word "protected"
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Protected"; flow:to_server,established; pcre:"/\Wprotected\W(?!/(25)?X[1-9])/ism"; classtype:policy-
violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002550; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002550;
rev:4;)

#The phrase "law enforcement sensitive"
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Law Enorcement Sensitive"; flow:to_server,established; pcre:"/\Wlaw\senforcement\ssensitive\W/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002551; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002551; rev:4;)

#The phrase "internal use only"
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Internal Use Only"; flow:to_server,established; pcre:"/\Winternal\suse\sonly\W/ism"; classtype:policy-
violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002552; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002552;
rev:4;)

#The phrase "date of birth" or its typical abbreviations
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Date of Birth"; flow:to_server,established; pcre:"/[^\w&]d(ate)?(-)?o(f)?(-)?b(irth)?\W[\s\w,/-]*(?=([0-9]
{2}[-/][0-9]{2}[-/][0-9]{2,4})|[0-9]{8})/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002553; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002553; rev:4;)
```

```
#Health Care Common Procedure Coding System (HCPCS) Codes
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - HCPCS Code"; flow:to_server,established; pcre:"/\Whcpcs\W[\s\w,/-]*(?=[a-z][0-9]{10})/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002554; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002554; rev:4;)

#International Statistical Classification of Diseases and Related Health Problems 10th Revision (ICD-10) Codes
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - ICD-10 Code"; flow:to_server,established; pcre:"/\Wicd\W[\s\w,/-]*(?=[a-z][0-9]{2}\.[0-9]{2})/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002555; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002555; rev:4;)

#Food and Drug Administration (FDA) National Drug Code (NDC) Codes
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - FDA NDC Code"; flow:to_server,established; pcre:"/\Wndc\W[\s\w,/-]*(?=([0-9]{4}-[0-9]{4}-[0-9]{2}|[0-9]{5}-
[0-9]{3}-[0-9]{2}|[0-9]{5}-[0-9]{4}-[0-9]{1,2}))/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002556;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002556; rev:4;)

#American Dental Association (ADA) Dental Procedure Codes
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - ADA Procedure Code"; flow:to_server,established; pcre:"/\Wada\W[\s\w,/-]*(?=d[0-9]{4})/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002557; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002557; rev:4;)

#Diagnostic and Statistical Manual of Mental Disorders (DSM-IV) Codes
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - DSM-IV Code"; flow:to_server,established; pcre:"/\Wdsm\W[\s\w,/-]*(?=([2-9][0-9]{2}(\.[0-9]{1,2}?)|(v[167]
[0-9]\.[0-9]{1,2})))/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002558; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002558; rev:5;)

#American Medical Association (AMA) Current Procedural Terminology (CPT) Codes
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - AMA CPT Code"; flow:to_server,established; pcre:"/\Wcpt\W[\s\w,/-]*(?=[0-9]{4}[ft]|[0-9]{5})/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002559; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002559; rev:4;)

#Japan Credit Bureau Credit Card Number
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Credit Card, JCB"; flow:to_server,established; pcre:"/\Wj(apan\s)?c(redit\s)?b(ureau)?\W[\s\w,/-]*(?=
(3[12359][0-9]{14})|(1800|2131)[0-9]{11})/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002561; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002561; rev:4;)

#The word "password", its typical abbreviations or written/abbreviated in a few forms of "leet"
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Password"; flow:to_server,established; pcre:"/\W[p][a4@][sz5]{0,2}[w]([o0][r])?[d]\W/ism"; classtype:policy-
violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002567; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002567;
rev:4;)

#The word "appraisal"
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Appraisal"; flow:to_server,established; pcre:"/\Wappraisal(s)?\W/ism"; classtype:policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2002568; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002568; rev:4;)

#The phrase "account balance"
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Account Balance"; flow:to_server,established; pcre:"/\Waccount\sbalance(s)?\W/ism"; classtype:policy-
violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002569; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002569;
rev:4;)

#The phrase "payment history"
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Payment History"; flow:to_server,established; pcre:"/\Wpayment\shistory\W/ism"; classtype:policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2002570; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002570; rev:4;)

#The phrase "annual income"
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Annual Income"; flow:to_server,established; pcre:"/\Wannual\sincome(s)?\W/ism"; classtype:policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2002571; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002571; rev:4;)

#The phrase "credit history"
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Credit History"; flow:to_server,established; pcre:"/\Wcredit\shistor(y|ies)\W/ism"; classtype:policy-
violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002572; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002572;
rev:4;)

#The phrase "transaction history"
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Transaction History"; flow:to_server,established; pcre:"/\Wtransaction\shistor(y|ies)\W/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002573; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002573; rev:4;)

#The phrase "customer list"
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY HTTP - Customer List"; flow:to_server,established; pcre:"/\Wcustomer\slist(s)?\W/ism"; classtype:policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2002574; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002574; rev:4;)

########################################
#High Ports, possibly Passive FTP DATA
#Non-US Restricted
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Non-US Restricted"; flow:to_server,established; pcre:"///([A-Z]{3}\s)+RESTRICTED//X5/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002575; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002575; rev:4;)

#Non-US Confidential
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Non-US Confidential"; flow:to_server,established; pcre:"///([A-Z]{3}\s)+CONFIDENTIAL//X5/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002576; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002576; rev:4;)

#Non-US Top Secret
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Non-US Top Secret"; flow:to_server,established; pcre:"///([A-Z]{3}\s)+TOP\sSECRET//X5/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002577; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002577; rev:4;)

#Non-US Secret
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Non-US Secret"; flow:to_server,established; pcre:"///([A-Z]{3}\s)+(?<!TOP\s)SECRET//X5/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002578; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002578; rev:4;)

#NATO Restricted
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - NATO Restricted"; flow:to_server,established; pcre:"///((NATO\sRESTRICTED)|NR)//MR/ism"; classtype:policy-
violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002579; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002579;
rev:4;)
```

```
#NATO Confidential Atomal
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - NATO Confidential Atomal"; flow:to_server,established;
pcre:"////((NATO\sCONFIDENTIAL\sATOMAL)|NCA)//MR/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002580; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002580; rev:4;)

#NATO Confidential
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - NATO Confidential"; flow:to_server,established; pcre:"////((NATO\sCONFIDENTIAL)|NC)//MR/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002581; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002581; rev:4;)

#NATO COSMIC Top Secret Atomal
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - NATO COSMIC Top Secret Atomal"; flow:to_server,established;
pcre:"////((COSMIC\sTOP\sSECRET\sATOMAL)|CTSA)//MR/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002582;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002582; rev:4;)

#NATO Secret Atomal
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - NATO Secret Atomal"; flow:to_server,established; pcre:"////((NATO\sSECRET\sATOMAL)|NSA)//MR/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002583; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002583; rev:4;)

#NATO Secret
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - NATO Secret"; flow:to_server,established; pcre:"////((NATO\sSECRET)|NS)//MR/ism"; classtype:policy-
violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002584; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002584;
rev:4;)

#US Confidential, Electronic Format
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Confidential, Electronic"; flow:to_server,established; pcre:"/QQQQ\r\n(?=(O|P|R|Z)\r\n(CC)\r\n)/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002585; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002585; rev:4;)

#US Top Secret, Electronic Format
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Top Secret, Electronic"; flow:to_server,established; pcre:"/QQQQ\r\n(?=(O|P|R|Z)\r\n(TT)\r\n)/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002586; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002586; rev:4;)

#US Secret, Electronic Format
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Secret, Electronic"; flow:to_server,established; pcre:"/QQQQ\r\n(?=(O|P|R|Z)\r\n(SS)\r\n)/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002587; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002587; rev:4;)

#US Confidential Authorized for Release To
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Confidential REL TO"; flow:to_server,established;
pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*REL\sTO\sUSA[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002588;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002588; rev:4;)

#US Top Secret Authorized for Release To
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Top Secret REL TO"; flow:to_server,established;
pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*REL\sTO\sUSA[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002589;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002589; rev:4;)

#US Secret Authorized for Release To
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Secret REL TO"; flow:to_server,established; pcre:"/(?<!TOP\s|T)
(SECRET|S)//[\s\w,/-]*REL\sTO\sUSA[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002590;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002590; rev:4;)

#US Confidential Comint
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Confidential COMINT"; flow:to_server,established; pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*(COMINT|SI)
[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002591; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002591; rev:4;)

#US Top Secret Comint
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Top Secret COMINT"; flow:to_server,established; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*(COMINT|SI)
[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002592; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002592; rev:4;)

#US Secret Comint
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Secret COMINT"; flow:to_server,established; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*(COMINT|SI)
[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002593; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002593; rev:4;)

#US Unclassified Communications Security Material
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Unclassified COMSEC"; flow:to_server,established; pcre:"/(UNCLASSIFIED|U)//[\s\w,/-]*COMSEC[\s\w,/-]*(?
=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002594; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002594; rev:4;)

#US Confidential Communications Security Material
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Confidential COMSEC"; flow:to_server,established; pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*COMSEC[\s\w,/-]*(?
=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002595; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002595; rev:4;)

#US Top Secret Communications Security Material
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Top Secret COMSEC"; flow:to_server,established; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*COMSEC[\s\w,/-]*(?
=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002596; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002596; rev:4;)

#US Secret Communications Security Material
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Secret COMSEC"; flow:to_server,established; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*COMSEC[\s\w,/-]*(?
=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002597; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002597; rev:4;)

#US Controlled Imagery
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Secret IMCON"; flow:to_server,established; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*(IMCON|IMC)
[\s\w,/-]*(?=//(X1|MR))/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002598; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002598; rev:4;)

#US Top Secret Critical Nuclear Weapon Design Information
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Top Secret CNWDI"; flow:to_server,established; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*
(CRITICAL\sNUCLEAR\sWEAPON\sDESIGN\sINFORMATION|CNWDI)[\s\w,/-]*(?=//MR)/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002599;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002599; rev:4;)
```

```
#US Secret Critical Nuclear Weapon Design Information
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Secret CNWDI"; flow:to_server,established; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*
(CRITICAL\sNUCLEAR\sWEAPON\sDESIGN\sINFORMATION|CNWDI)[\s\w,/-]*(?=//MR)/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002600;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002600; rev:4;)

#US Top Secret Talent Keyhole
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Top Secret TK"; flow:to_server,established; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*(TALENT\sKEYHOLE|TK)
[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002601; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002601; rev:4;)

#US Secret Talent Keyhole
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Secret TK"; flow:to_server,established; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*(TALENT\sKEYHOLE|TK)
[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002602; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002602; rev:4;)

#US Foreign Government Information
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US FGI"; flow:to_server,established; pcre:"///FGI[\s\w,/-]*(?=//X5)/ism"; classtype:policy-violation;
reference:url,doc.emergingthreats.net/bin/view/Main/2002603; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002603; rev:4;)

#US For Official Use Only
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US FOUO"; flow:to_server,established; pcre:"/(UNCLASSIFIED|U)//(FOR\sOFFICIAL\sUSE\sONLY|FOUO)/ism";
classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002604; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002604; rev:4;)

#US Confidential Not Releasable to Foreign Nationals
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Confidential NOFORN"; flow:to_server,established; pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*NOFORN[\s\w,/-]*(?
=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002605; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002605; rev:4;)

#US Top Secret Not Releasable to Foreign Nationals
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Top Secret NOFORN"; flow:to_server,established; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*NOFORN[\s\w,/-]*(?
=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002606; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002606; rev:4;)

#US Secret Not Releasable to Foreign Nationals
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Secret NOFORN"; flow:to_server,established; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*NOFORN[\s\w,/-]*(?
=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002607; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002607; rev:4;)

#US Confidential Originator Controlled
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Confidential ORCON"; flow:to_server,established; pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*
(ORIGINATOR\sCONTROLLED|ORCON)[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002608;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002608; rev:4;)

#US Top Secret Originator Controlled
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Top Secret ORCON"; flow:to_server,established; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*
(ORIGINATOR\sCONTROLLED|ORCON)[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002609;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002609; rev:4;)

#US Secret Originator Controlled
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Secret ORCON"; flow:to_server,established; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*
(ORIGINATOR\sCONTROLLED|ORCON)[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002610;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002610; rev:4;)

#US Unclassified Proprietary Information
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Unclassified PROPIN"; flow:to_server,established; pcre:"/(UNCLASSIFIED|U)//[\s\w,/-]*PROPIN[\s\w,/-]*(?
=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002611; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002611; rev:4;)

#US Confidential Proprietary Information
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Confidential PROPIN"; flow:to_server,established; pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*PROPIN[\s\w,/-]*(?
=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002612; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002612; rev:4;)

#US Top Secret Proprietary Information
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Top Secret PROPIN"; flow:to_server,established; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*PROPIN[\s\w,/-]*(?
=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002613; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002613; rev:4;)

#US Secret Proprietary Information
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Secret PROPIN"; flow:to_server,established; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*PROPIN[\s\w,/-]*(?
=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002614; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002614; rev:4;)

#US Confidential Restricted Data
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Confidential RD"; flow:to_server,established; pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*(RESTRICTED\sDATA|RD)
[\s\w,/-]*(?=//MR)/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002615; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002615; rev:4;)

#US Top Secret Restricted Data
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Top Secret RD"; flow:to_server,established; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*(RESTRICTED\sDATA|RD)
[\s\w,/-]*(?=//MR)/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002616; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002616; rev:4;)

#US Secret Restricted Data
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Secret RD"; flow:to_server,established; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*(RESTRICTED\sDATA|RD)
[\s\w,/-]*(?=//MR)/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002617; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002617; rev:4;)

#US Sources and Methods Information
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US SAMI"; flow:to_server,established; pcre:"/SAMI[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-
violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002618; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002618;
rev:4;)

#US Confidential Special Category
#
```

```
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Confidential SPECAT"; flow:to_server,established; pcre:"/(CONFIDENTIAL|C)//[\s\w,/-]*SPECAT[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002619; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002619; rev:4;)

#US Top Secret Special Category
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Top Secret SPECAT"; flow:to_server,established; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*SPECAT[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002620; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002620; rev:4;)

#US Secret Special Category
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Secret SPECAT"; flow:to_server,established; pcre:"/(?<!TOP\s|T)(SECRET|S)//[\s\w,/-]*SPECAT[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/bin/view/Main/2002621; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002621; rev:4;)

#US Top Secret Single Integrated Operations Plan
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - US Top Secret STOP"; flow:to_server,established; pcre:"/(TOP\sSECRET|TS)//[\s\w,/-]*STOP[\s\w,/-]*(?=//(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002622; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002622; rev:4;)

#The word "private"
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Private"; flow:to_server,established; pcre:"/\Wprivate\W(?!/(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002623; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002623; rev:4;)

#The word "restricted"
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Restricted"; flow:to_server,established; pcre:"/(?<!//)\Wrestricted[^\w/]/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002624; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002624; rev:4;)

#The word "confidential"
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Confidential"; flow:to_server,established; pcre:"/(?<!//)\Wconfidential[^\w/]/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002625; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002625; rev:4;)

#The word "secret"
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Secret"; flow:to_server,established; pcre:"/(?<!TOP|//)\Wsecret[^\w/a]/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002626; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002626; rev:4;)

#The phrase "top secret"
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Top Secret"; flow:to_server,established; pcre:"/(?<!//)\Wtop\ssecret[^\w/a]/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002627; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002627; rev:4;)

#The word "sealed"
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Sealed"; flow:to_server,established; pcre:"/\Wsealed\W(?!/(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002628; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002628; rev:4;)

#The word "sensitive"
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Sensitive"; flow:to_server,established; pcre:"/(?<!law\senforcement)\Wsensitive\W(?!/(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002629; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002629; rev:4;)

#The word "proprietary"
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Proprietary"; flow:to_server,established; pcre:"/\Wproprietary\W(?!/(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002630; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002630; rev:5;)

#The word "protected"
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Protected"; flow:to_server,established; pcre:"/\Wprotected\W(?!/(25)?X[1-9])/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002631; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002631; rev:5;)

#The phrase "law enforcement sensitive"
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Law Enorcement Sensitive"; flow:to_server,established; pcre:"/\Wlaw\senforcement\ssensitive\W/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002632; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002632; rev:5;)

#The phrase "internal use only"
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Internal Use Only"; flow:to_server,established; pcre:"/\Winternal\suse\sonly\W/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002633; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002633; rev:5;)

#The phrase "date of birth" or its typical abbreviations
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Date of Birth"; flow:to_server,established; pcre:"/[^\w&]d(ate)?(-)?o(f)?(-)?b(irth)?\W[\s\w,/-]*(?=([0-9]{2}[-/][0-9]{2}[-/][0-9]{2,4})|[0-9]{8})/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002634; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002634; rev:5;)

#Health Care Common Procedure Coding System (HCPCS) Codes
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - HCPCS Code"; flow:to_server,established; pcre:"/\Whcpcs\W[\s\w,/-]*(?=[a-z][0-9]{10})/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002635; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002635; rev:5;)

#International Statistical Classification of Diseases and Related Health Problems 10th Revision (ICD-10) Codes
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - ICD-10 Code"; flow:to_server,established; pcre:"/\Wicd\W[\s\w,/-]*(?=[a-z][0-9]{2}\.[0-9]{2})/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002636; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002636; rev:5;)

#Food and Drug Administration (FDA) National Drug Code (NDC) Codes
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - FDA NDC Code"; flow:to_server,established; pcre:"/\Wndc\W[\s\w,/-]*(?=([0-9]{4}-[0-9]{4}-[0-9]{2}|[0-9]{5}-[0-9]{3}-[0-9]{2}|[0-9]{5}-[0-9]{4}-[0-9]{1,2}))/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002637; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002637; rev:5;)

#American Dental Association (ADA) Dental Procedure Codes
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - ADA Procedure Code"; flow:to_server,established; pcre:"/\Wada\W[\s\w,/-]*(?=d[0-9]{4})/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002638; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002638; rev:5;)

#Diagnostic and Statistical Manual of Mental Disorders (DSM-IV) Codes
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - DSM-IV Code"; flow:to_server,established; pcre:"/\Wdsm\W[\s\w,/-]*(?=([2-9][0-9]{2}(\.[0-9]{1,2}?)|(v[167][0-9]\.[0-9]{1,2})))/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002639; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002639; rev:7;)

#American Medical Association (AMA) Current Procedural Terminology (CPT) Codes
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - AMA CPT Code"; flow:to_server,established; pcre:"/\Wcpt\W[\s\w,/-]*(?=[0-9]{4}[ft]|[0-9]{5})/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002640; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002640; rev:5;)
```

```
#Japan Credit Bureau Credit Card Number
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Credit Card, JCB"; flow:to_server,established; pcre:"/\Wj(apan\s)?c(redit\s)?b(ureau)?\W[\s\w,/-]*(?=(3[12359][0-9]{14})|(1800|2131)[0-9]{11})/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002642; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002642; rev:5;)

#The word "password", its typical abbreviations or written/abbreviated in a few forms of "leet"
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Password"; flow:to_server,established; pcre:"/\W[p][a4@][sz5]{0,2}[w]([o0][r])?[d]\W/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002648; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002648; rev:5;)

#The word "appraisal"
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Appraisal"; flow:to_server,established; pcre:"/\Wappraisal(s)?\W/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002649; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002649; rev:5;)

#The phrase "account balance"
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Account Balance"; flow:to_server,established; pcre:"/\Waccount\sbalance(s)?\W/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002650; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002650; rev:5;)

#The phrase "payment history"
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Payment History"; flow:to_server,established; pcre:"/\Wpayment\shistory\W/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002651; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002651; rev:5;)

#The phrase "annual income"
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Annual Income"; flow:to_server,established; pcre:"/\Wannual\sincome(s)?\W/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002652; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002652; rev:5;)

#The phrase "credit history"
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Credit History"; flow:to_server,established; pcre:"/\Wcredit\shistor(y|ies)\W/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002653; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002653; rev:5;)

#The phrase "transaction history"
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Transaction History"; flow:to_server,established; pcre:"/\Wtransaction\shistor(y|ies)\W/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002654; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002654; rev:5;)

#The phrase "customer list"
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET POLICY High Ports - Customer List"; flow:to_server,established; pcre:"/\Wcustomer\slist(s)?\W/ism"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2002655; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Classified_Information; sid:2002655; rev:5;)

#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 Club World Casino Client in Use"; flow:established,to_server; dsize:23; content:"Club World Casinos"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2007754; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Club_World_Casinos; sid:2007754; rev:4;)

#Submitted by Matt Jonkman
#Thees rules are disabled by default. They 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 Credit Card Number Detected in Clear (16 digit spaced)"; pcre:"/ (6011|5[1-5]\d{2}|4\d{3}|3\d{3}) \d{4} \d{4} \d{4}/"; classtype:policy-violation; reference:url,www.beachnet.com/~hstiles/cardtype.html; reference:url,doc.emergingthreats.net/2001375; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Credit_Card_Numbers; sid:2001375; rev:12;)

#Submitted by Matt Jonkman
#Thees rules are disabled by default. They 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 Credit Card Number Detected in Clear (16 digit dashed)"; pcre:"/ (6011|5[1-5]\d{2}|4\d{3}|3\d{3})-\d{4}-\d{4}-\d{4}/"; classtype:policy-violation; reference:url,www.beachnet.com/~hstiles/cardtype.html; reference:url,doc.emergingthreats.net/2001376; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Credit_Card_Numbers; sid:2001376; rev:12;)

#Submitted by Matt Jonkman
#Thees rules are disabled by default. They 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 Credit Card Number Detected in Clear (16 digit)"; pcre:"/ (6011|5[1-5]\d{2}|4\d{3}|3\d{3})\d{12} /"; classtype:policy-violation; reference:url,www.beachnet.com/~hstiles/cardtype.html; reference:url,doc.emergingthreats.net/2001377; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Credit_Card_Numbers; sid:2001377; rev:12;)

#Submitted by Matt Jonkman
#Thees rules are disabled by default. They 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 Credit Card Number Detected in Clear (15 digit)"; pcre:"/ (3[4|7]\d{2}|2014|2149|2131|1800)\d{11} /"; classtype:policy-violation; reference:url,www.beachnet.com/~hstiles/cardtype.html; reference:url,doc.emergingthreats.net/2001378; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Credit_Card_Numbers; sid:2001378; rev:12;)

#Submitted by Matt Jonkman
#Thees rules are disabled by default. They 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 Credit Card Number Detected in Clear (15 digit spaced)"; pcre:"/ (3[4|7]\d{2}|2014|2149|2131|1800) \d{4} \d{4} \d{3} /"; classtype:policy-violation; reference:url,www.beachnet.com/~hstiles/cardtype.html; reference:url,doc.emergingthreats.net/2001379; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Credit_Card_Numbers; sid:2001379; rev:12;)

#Submitted by Matt Jonkman
#Thees rules are disabled by default. They 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 Credit Card Number Detected in Clear (15 digit dashed)"; pcre:"/ (3[4|7]\d{2}|2014|2149|2131|1800)-\d{4}-\d{4}-\d{3} /"; classtype:policy-violation; reference:url,www.beachnet.com/~hstiles/cardtype.html; reference:url,doc.emergingthreats.net/2001380; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Credit_Card_Numbers; sid:2001380; rev:12;)

#Submitted by Matt Jonkman
#Thees rules are disabled by default. They 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 Credit Card Number Detected in Clear (14 digit)"; pcre:"/ (30[0-5]\d|36\d{2}|38\d{2})\d{10} /"; classtype:policy-violation; reference:url,www.beachnet.com/~hstiles/cardtype.html; reference:url,doc.emergingthreats.net/2001381; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Credit_Card_Numbers; sid:2001381; rev:12;)

#Submitted by Matt Jonkman
#Thees rules are disabled by default. They 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 Credit Card Number Detected in Clear (14 digit spaced)"; pcre:"/ (30[0-5]\d|36\d{2}|38\d{2}) \d{4} \d{4} \d{2} /"; classtype:policy-violation; reference:url,www.beachnet.com/~hstiles/cardtype.html; reference:url,doc.emergingthreats.net/2001382; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Credit_Card_Numbers; sid:2001382; rev:12;)

#Submitted by Matt Jonkman
#Thees rules are disabled by default. They 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 Credit Card Number Detected in Clear (14 digit dashed)"; pcre:"/ (30[0-5]\d|36\d{2}|38\d{2})-\d{4}-\d{4}-\d{2} /"; classtype:policy-violation; reference:url,www.beachnet.com/~hstiles/cardtype.html; reference:url,doc.emergingthreats.net/2001383; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Credit_Card_Numbers; sid:2001383; rev:12;)

#Submitted by Matt Jonkman
```

```
#Thees rules are disabled by default. They 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 Credit Card Number Detected in Clear (15 digit spaced 2)"; pcre:"/ (3[4|7]\d{2}|2014|2149|2131|1800) \d{6} \d{5} /"; classtype:policy-
violation; reference:url,www.beachnet.com/~hstiles/cardtype.html; reference:url,doc.emergingthreats.net/2009293; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Credit_Card_Numbers; sid:2009293; rev:1;)

#Submitted by Matt Jonkman
#Thees rules are disabled by default. They 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 Credit Card Number Detected in Clear (15 digit dashed 2)"; pcre:"/ (3[4|7]\d{2}|2014|2149|2131|1800)-\d{6}-\d{5} /"; classtype:policy-
violation; reference:url,www.beachnet.com/~hstiles/cardtype.html; reference:url,doc.emergingthreats.net/2009294; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Credit_Card_Numbers; sid:2009294; rev:1;)

#by waldo kitty
#commented out as these should be chosen to run, not on by default. Run them if you are interested
#unsolicited inbound connection to MSSQL server port
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 1433 (msg:"ET POLICY Suspicious inbound to MSSQL port 1433"; flow:to_server; flags:S; threshold: type limit, count 5, seconds 60, track by_src;
classtype:bad-unknown; reference:url,doc.emergingthreats.net/2010935; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_DB_Connections; sid:2010935; rev:2;)

#unsolicited inbound connection to Oracle SQL server port. also ncube license manager and oracle tns listner
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 1521 (msg:"ET POLICY Suspicious inbound to Oracle SQL port 1521"; flow:to_server; flags:S; threshold: type limit, count 5, seconds 60, track
by_src; classtype:bad-unknown; reference:url,doc.emergingthreats.net/2010936; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_DB_Connections; sid:2010936;
rev:2;)

#unsolicited inbound connection to mySQL server port
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 3306 (msg:"ET POLICY Suspicious inbound to mySQL port 3306"; flow:to_server; flags:S; threshold: type limit, count 5, seconds 60, track by_src;
classtype:bad-unknown; reference:url,doc.emergingthreats.net/2010937; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_DB_Connections; sid:2010937; rev:2;)

#unsolicited inbound connection to mSQL server port
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 4333 (msg:"ET POLICY Suspicious inbound to mSQL port 4333"; flow:to_server; flags:S; threshold: type limit, count 5, seconds 60, track by_src;
classtype:bad-unknown; reference:url,doc.emergingthreats.net/2010938; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_DB_Connections; sid:2010938; rev:2;)

#unsolicited inbound connection to PostgreSQL server port
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 5432 (msg:"ET POLICY Suspicious inbound to PostgreSQL port 5432"; flow:to_server; flags:S; threshold: type limit, count 5, seconds 60, track
by_src; classtype:bad-unknown; reference:url,doc.emergingthreats.net/2010939; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_DB_Connections; sid:2010939;
rev:2;)

#Submitted by Joseph Gama
#
#alert udp $DNS_SERVERS 53 -> any any (msg:"ET DNS Standard query response, Format error"; pcre:"/..[\x81\x82\x83\x84\x85\x86\x87]\x81/"; classtype: not-suspicious;
reference:url,doc.emergingthreats.net/2001116; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_DNS_Responses; sid:2001116; rev:5;)

#Submitted by Joseph Gama
#
#alert udp $DNS_SERVERS 53 -> any any (msg:"ET DNS Standard query response, Name Error"; pcre:"/..[\x81\x82\x83\x84\x85\x86\x87]\x83/"; classtype: not-suspicious;
reference:url,doc.emergingthreats.net/2001117; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_DNS_Responses; sid:2001117; rev:5;)

#Submitted by Joseph Gama
#
#alert udp $DNS_SERVERS 53 -> any any (msg:"ET DNS Standard query response, Not Implemented"; pcre:"/..[\x81\x82\x83\x84\x85\x86\x87]\x84/"; classtype: not-suspicious;
reference:url,doc.emergingthreats.net/2001118; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_DNS_Responses; sid:2001118; rev:5;)

#Submitted by Joseph Gama
#
#alert udp $DNS_SERVERS 53 -> any any (msg:"ET DNS Standard query response, Refused"; pcre:"/..[\x81\x82\x83\x84\x85\x86\x87]\x85/"; classtype: not-suspicious;
reference:url,doc.emergingthreats.net/2001119; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_DNS_Responses; sid:2001119; rev:5;)

#Adapted from nextsoft.cz
#
alert udp any 53 -> ![$DNS_SERVERS,$SMTP_SERVERS] any (msg:"ET POLICY Unusual number of DNS No Such Name Responses"; content:"|83|"; offset:3; depth:1; threshold: type both , track
by_dst, count 50, seconds 300; classtype:bad-unknown; reference:url,doc.emergingthreats.net/2003195; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_DNS_Responses; sid:2003195; rev:5;)

#by Myron Davis
#
alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"ET POLICY nstx DNS Tunnel Outbound"; content:"cT"; offset:12; depth:3; content:"|00 10 00 01 00 00 29 08|"; within:255; classtype:bad-
unknown; reference:url,savannah.nongnu.org/projects/nstx/; reference:url,nstx.dereference.de/nstx; reference:url,doc.emergingthreats.net/2002676;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_DNS_Tunnel_nstx; sid:2002676; rev:3;)

#Submitted by Ole-Martin
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY Dameware Remote Control Service Install"; flow: to_server,established; content:"DWRCK.DLL"; nocase; classtype: successful-
admin; reference:url,doc.emergingthreats.net/2001294; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Dameware; sid:2001294; rev:5;)

#by Jack Pepper
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Gteko User-Agent Detected - Dell Remote Access"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| ";
content:"Windows 98"; within:50; content:"GtekClient"; within:50; pcre:"/User-Agent\x3a[^\n]+Windows 98[^\n]+GtekClient/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_Dell_Spyware; sid:2008037; rev:3;)

#by Jack Pepper
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Dell MyWay Remote control agent"; flow:established,to_server; content:"|0d 0a|Referer|3a| http|3a|//dell";
depth:100; content:"|0d 0a|Host|3a| "; depth:250; content:"myway.com"; nocase; within:20; distance:0; classtype:not-suspicious; threshold:type limit, track by_src, count 2, seconds 360;
reference:url,doc.emergingthreats.net/2008051; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Dell_Spyware; sid:2008051; rev:3;)

#for access to a local dlink router's config page. Some trojans try to access this
#re 20069714fc077fe197d3fc27fa905025
#
alert tcp $HOME_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET POLICY Dlink Soho Router Config Page Access Attempt"; flow:established,to_server; content:"GET /dlink/hwiz.html HTTP/1.";
depth:30; content:"|0d 0a|Host|3a| "; pcre:"/Host\: \d+\.\d+\.\d+\.\d+\x0d\x0a/"; classtype:attempted-admin; reference:url,doc.emergingthreats.net/2008942;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Dlink; sid:2008942; rev:5;)

#by Juan Manuel Lorenzo at ossim
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Megaupload file download service access"; flow:to_server,established; content:"GET "; depth:4; uricontent:"/?d=";
content:"|0d 0a|Host|3a| "; content:"megaupload.com"; within:25; nocase; classtype:policy-violation; reference:url,doc.emergingthreats.net/2009301;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Download_Services; sid:2009301; rev:3;)

#by Juan Manuel Lorenzo at ossim
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Badongo file download service access"; flow:to_server,established; content:"GET "; depth: 4; uricontent:"/file/";
content:"|0d 0a|Host|3a| "; nocase; content:"badongo.com"; nocase; within:25; content:"|0d 0a|Cookie|3a| badongoL="; classtype:policy-violation;
reference:url,doc.emergingthreats.net/2009302; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Download_Services; sid:2009302; rev:3;)

#by Juan Manuel Lorenzo at ossim
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY MediaFire file download service access"; flow:to_server,established; content:"GET "; depth:4; uricontent:"/?";
content:"|0d 0a|Host|3a|"; nocase; content:"mediafire.com"; nocase; within:25; classtype:policy-violation; reference:url,doc.emergingthreats.net/2009303;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Download_Services; sid:2009303; rev:3;)

#by Juan Manuel Lorenzo at ossim
```

```
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Gigasize file download service access"; flow:to_server,established; content:"GET "; depth: 4;
uricontent:"/get.php"; content:"|0d 0a|Host|3a| "; nocase; content:"gigasize.com"; nocase; within:25; classtype:policy-violation; reference:url,doc.emergingthreats.net/2009304;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Download_Services; sid:2009304; rev:3;)

#by marcus at unsober
#re:051892a56b8aa633fc446ec827ed1911
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY TeamViewer Dyngate User-Agent"; flow:established,to_server; content:"User-Agent|3a| Mozilla/4.0 (compatible|3b| MSIE
6.0|3b| DynGate)"; classtype:policy-violation; reference:url,www.teamviewer.com/index.aspx; reference:url,doc.emergingthreats.net/2009475; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Dyngate; sid:2009475; rev:5;)

#Blake Hartstein of Demarc
#Potentially noisy, Not recommended unless you disallow exe files. written for executable virii that spread through email
#
#alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"ET POLICY SMTP Executable attachment"; flow:established,to_server; content:"filename="; nocase; content:".exe"; nocase;
distance:0; pcre:"/filename=\s*[^\n]+\.exe/i"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2003325; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_EXE; sid:2003325; rev:4;)

#by dxp
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY Suspicious Executable (PE under 128)"; flow:established,from_server; content:"MZ"; rawbytes; byte_test:4,
<,128,58,relative,little; content:"PE|00 00|"; rawbytes; within:130; classtype:policy-violation; reference:url,doc.emergingthreats.net/2009033;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_EXE; sid:2009033; rev:3;)

#by dxp
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY Suspicious Executable (PE offset 160)"; flow:established,from_server; content:"MZ"; rawbytes;
byte_test:4,=,160,58,relative,little; content:"PE|00 00|"; rawbytes; within:162; classtype:policy-violation; reference:url,doc.emergingthreats.net/2009034;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_EXE; sid:2009034; rev:3;)

#by dxp
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY Suspicious Executable (PE offset 512)"; flow:established,from_server; content:"MZ"; rawbytes;
byte_test:4,=,512,58,relative,little; content:"PE|00 00|"; rawbytes; within:514; classtype:policy-violation; reference:url,doc.emergingthreats.net/2009035;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_EXE; sid:2009035; rev:3;)

#Matt Jonkman
#To catch generic exe downloads via http. This does not mean it's a problem, just of interest.
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY exe download via HTTP - Informational"; flow:established,to_server; uricontent:".exe"; nocase; content:"GET ";
nocase; depth:4; pcre:"/\.exe\b/Ui"; classtype:policy-violation; reference:url,doc.emergingthreats.net/2003595; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_EXE_HTTP; sid:2003595; rev:4;)

#to catch the common urls for storm worm downloads, etc
#by Jack Pepper and Reg Quinton
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Possible Ecard Trojan download"; flow:established,to_server; uricontent:".exe"; nocase;
pcre:"/(gif|car(d|tao)|jpe?g)\.exe$/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006434; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_EXE_HTTP; sid:2006434; rev:7;)

#Matt Jonkman
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY exe download without User Agent"; flow:established,to_server; content:"GET "; depth:4; uricontent:".exe"; nocase;
content:!"User-Agent|3a|"; content:!"download.windowsupdate.com"; content:!"mms|3a|//"; nocase; pcre:"/\.exe$/Ui"; classtype:policy-violation;
reference:url,doc.emergingthreats.net/2003179; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_EXE_NoUserAgent; sid:2003179; rev:9;)

#by RPG, intended to catch exe's being hidden as requested BMPs
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Set flow on bmp file get"; flow:established,to_server; content:"GET "; depth:4; uricontent:".bmp"; content:".bmp
HTTP/1."; flowbits:set,ET.bmp_seen; flowbits:noalert; classtype:not-suspicious; reference:url,doc.emergingthreats.net/2009083; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_EXE_in_BMP; sid:2009083; rev:2;)

#by RPG, intended to catch exe's being hidden as requested BMPs
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Possible Trojan File Download - BMP Requested but not received"; flow:established,from_server;
flowbits:isset,ET.bmp_seen; flowbits:unset,ET.bmp_seen; content:"200 OK"; content:"Content-Type|3a| application|2f|octet-stream"; distance:0; content:!"BM"; content:!"|00 00 00 00|";
within:4; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009084; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_EXE_in_BMP; sid:2009084;
rev:2;)

#From Charles Lacroix
#All form elements are encoded before they are sent to the server
#This makes things a bit more complicated to decode via snort at least
#for me. This rule will trigger when a user is starting to place
#an item for sale on the ebay site.
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY eBay Bid Placed"; flow: to_server,established; uricontent:"/ws/eBayISAPI.dll/"; nocase; content:"maxbid="; nocase;
content:"offer.ebay.com"; nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/2001898; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Ebay; sid:2001898; rev:6;)

#From Charles Lacroix
#All form elements are encoded before they are sent to the server
#This makes things a bit more complicated to decode via snort at least
#for me. This rule will trigger when a user is starting to place
#an item for sale on the ebay site.
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY eBay Placing Item for sale"; flow: to_server,established; uricontent:"/ws2/eBayISAPI.dll"; nocase;
content:".ebay.com"; nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/2001907; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Ebay; sid:2001907; rev:4;)

#Look for a single item
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY eBay View Item"; flow: to_server,established; uricontent:"/ws/eBayISAPI.dll"; nocase; content:"ViewItem"; nocase;
content:".ebay.com"; nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/2001908; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Ebay; sid:2001908; rev:5;)

#Mark an item to watch
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY eBay Watch This Item"; flow: to_server,established; uricontent:"/ws/eBayISAPI.dll"; nocase;
content:"MakeTrack&Item="; nocase; content:".ebay.com"; nocase; classtype: policy-violation; reference:url,doc.emergingthreats.net/2001909; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_Ebay; sid:2001909; rev:5;)

#by evilghost
#
##alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET DELETED offers.e-centives.com Coupon Printer"; flow:established,to_server; content:"|0d 0a|User-Agent\: Mozilla/4.0
(compatible\; YourApp\; AK\; Windows 95)|0d 0a|"; nocase; classtype:policy-violation; reference:url,offers.e-centives.com; reference:url,doc.emergingthreats.net/2010338;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Ecentives; sid:2010338; rev:2;)

#by Marcus at unsober
#re a0b153ea54ed61d1ac650f139dd86f54
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Eurobarre.us Setup User-Agent"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| eurobarre ";
classtype:policy-violation; nocase; reference:url,doc.emergingthreats.net/2008336; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Eurobarre; sid:2008336;
rev:3;)

#by Matt Jonkman
#sets a flowbit for viruscatch.co.kr related, win32.small.hvd and others
#
#alert tcp $EXTERNAL_NET 3306 -> $HOME_NET any (msg:"ET POLICY External MYSQL Server Connection"; flow:from_server,established; content:"|00|"; depth:1; offset:3; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/2008572; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_External_Mysql_Servers; sid:2008572; rev:3;)
```

```
#by Steven Adair at securityzone.org
#Rule to catch all FTP logins that do not start with "anonymous" or "ftp"
#and do not contain "pass " (pass followed by a space). -steven@securityzone
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET POLICY FTP Login Attempt (non-anonymous)"; flow:to_server,established; content:"USER"; content:!"PASS "; nocase; pcre:!"/^USER\s+
(anonymous|ftp)/smi"; classtype:misc-activity; reference:url,doc.emergingthreats.net/2003303; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_FTP_Login;
sid:2003303; rev:3;)

#By CunningPike
#
alert tcp $HOME_NET 21 -> $EXTERNAL_NET any (msg:"ET POLICY FTP Login Successful (non-anonymous)"; flow:from_server,established; flowbits:isset,ET.ftp.user.login;
flowbits:isnotset,ftp.user.logged_in; flowbits:set,ftp.user.logged_in; content:"230 "; pcre:!"/^230(\s+USER)?\s+(anonymous|ftp)/smi"; classtype:misc-activity;
reference:url,doc.emergingthreats.net/2003410; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_FTP_Login; sid:2003410; rev:7;)

#by jack pepper
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET POLICY FTP Frequent Administrator Login Attempts"; flow:to_server,established; content:"USER Administrator|0d0a|"; nocase;
threshold: type threshold, track by_src, count 3, seconds 30; classtype:attempted-admin; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_FTP_Login;
reference:url,doc.emergingthreats.net/2009667; sid:2009667; rev:2;)

#by jack pepper
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"ET POLICY FTP Frequent Admin Login Attempts"; flow:to_server,established; content:"USER Admin|0d0a|"; nocase; threshold: type
threshold, track by_src, count 3, seconds 30; classtype:attempted-admin; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_FTP_Login;
reference:url,doc.emergingthreats.net/2009668; sid:2009668; rev:2;)

#matt jonkman
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 22:1024 (msg:"ET POLICY FTP Conversation on Low Port - Likely Hostile (TYPE A)"; flow:established,to_server; dsize:6; content:"TYPE "; depth:5;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008589; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_FTP_Off_Ports; sid:2008589; rev:2;)

#matt jonkman
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 22:1024 (msg:"ET POLICY FTP Conversation on Low Port - Likely Hostile (PASV)"; flow:established,to_server; dsize:4; content:"PASV";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008590; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_FTP_Off_Ports; sid:2008590; rev:2;)

#by Jules Pagna Disso
#
#alert tcp $HOME_NET any -> [69.63.176.0/20,69.63.176.0/20,204.15.20.0/22] $HTTP_PORTS (msg:"ET POLICY facebook activity"; flow:established,to_server; threshold: type both, track
by_dst, count 2, seconds 120; classtype:policy-violation; reference:url,compnetworking.about.com/od/traceipaddresses/f/facebook-ip-address.htm;
reference:url,doc.emergingthreats.net/2010952; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Facebook; sid:2010952; rev:3;)

#by SpOoKeR
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Facebook Chat (send message)"; flow:established,to_server; content:"POST "; depth:5;
uricontent:"/ajax/chat/send.php"; content:"|0d 0a|Host|3a| "; content:"facebook.com|0d 0a|"; within:20; classtype:policy-violation; reference:url,doc.emergingthreats.net/2010784;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Facebook_Chat; sid:2010784; rev:3;)

#by SpOoKeR
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Facebook Chat (buddy list)"; flow:established,to_server; content:"POST "; depth:5;
uricontent:"/ajax/chat/buddy_list.php"; content:"|0d 0a|Host\: "; content:"facebook.com|0d 0a|"; within:20; classtype:policy-violation; reference:url,doc.emergingthreats.net/2010785;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Facebook_Chat; sid:2010785; rev:2;)

#by SpOoKeR
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Facebook Chat (settings)"; flow:established,to_server; content:"POST "; depth:5;
uricontent:"/ajax/chat/settings.php"; content:"|0d 0a|Host\: "; content:"facebook.com|0d 0a|"; within:20; classtype:policy-violation; reference:url,doc.emergingthreats.net/2010786;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Facebook_Chat; sid:2010786; rev:2;)

#by rodrigo and joel esler
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 5222 (msg:"ET POLICY Facebook Chat using XMPP"; flow:to_server,established; content:"chat.facebook.com"; nocase; content:"jabber|3A|client";
nocase; distance:9; within:13; threshold: type limit, track by_src, count 1, seconds 60; classtype:policy-violation; reference:url,www.facebook.com/sitetour/chat.php;
reference:url,doc.emergingthreats.net/2010819; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Facebook_Chat; sid:2010819; rev:4;)

#by Will Metcalf
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY FOX,ABC On-demand UA"; flow:to_server,established; content:"User-Agent|3a| QSP"; nocase; classtype:policy-
violation; reference:url,doc.emergingthreats.net/2007639; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Fox_ABC_On_Demand; sid:2007639; rev:5;)

#by Sandro Reis
#
alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"ET POLICY Possible External FreeGate DNS Query"; content:"|03 77 36 31 0d 7a 69 79 6f 75 6c 6f 6e 67 6c 69 76 65 03 63 6f 6d 00|";
classtype:policy-violation; threshold:type limit, track by_src,count 1, seconds 30; reference:url,doc.emergingthreats.net/2008744; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_FreeGate; sid:2008744; rev:2;)

#by Sandro Reis
#
alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"ET POLICY Possible External FreeGate DNS Query"; content:"|03 77 36 32 0d 7a 69 79 6f 75 6c 6f 6e 67 6c 69 76 65 03 63 6f 6d 00|";
classtype:policy-violation; threshold:type limit, track by_src,count 1, seconds 30; reference:url,doc.emergingthreats.net/2008745; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_FreeGate; sid:2008745; rev:2;)

#by Sandro Reis
#
alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"ET POLICY Possible External FreeGate DNS Query"; content:"|03 77 36 33 0d 7a 69 79 6f 75 6c 6f 6e 67 6c 69 76 65 03 63 6f 6d 00|";
classtype:policy-violation; threshold:type limit, track by_src,count 1, seconds 30; reference:url,doc.emergingthreats.net/2008746; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_FreeGate; sid:2008746; rev:2;)

#by Sandro Reis
#
alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"ET POLICY Possible External FreeGate DNS Query"; content:"|03 77 36 34 0d 7a 69 79 6f 75 6c 6f 6e 67 6c 69 76 65 03 63 6f 6d 00|";
classtype:policy-violation; threshold:type limit, track by_src,count 1, seconds 30; reference:url,doc.emergingthreats.net/2008747; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_FreeGate; sid:2008747; rev:2;)

#by Sandro Reis
#
alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"ET POLICY Possible External FreeGate DNS Query"; content:"|03 77 36 35 0d 7a 69 79 6f 75 6c 6f 6e 67 6c 69 76 65 03 63 6f 6d 00|";
classtype:policy-violation; threshold:type limit, track by_src,count 3, seconds 30; reference:url,doc.emergingthreats.net/2008748; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/POLICY/POLICY_FreeGate; sid:2008748; rev:3;)

#Submitted 2006-10-17 by Adam Nunn
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 80 (msg:"ET POLICY docs.google.com Activity"; flow:established,to_server; content:"Host|3a| docs.google.com"; nocase; classtype:policy-
violation; reference:url,docs.google.com; reference:url,doc.emergingthreats.net/2003121; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Google; sid:2003121;
rev:4;)

#Submitted 2006-10-17 by Adam Nunn
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 80 (msg:"ET POLICY Possible docs.google.com Activity"; flow:established,to_server; content:"WRITELY_SID"; nocase; classtype:policy-violation;
reference:url,docs.google.com; reference:url,doc.emergingthreats.net/2003122; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/POLICY/POLICY_Google; sid:2003122; rev:4;)

#Matt Jonkman
#Google calendar in the news as most entries are public
#I'm sure it's a good calendar, but folks have to realize what's public and what's not
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY Google Calendar in Use"; flow:established,to_server; uricontent:"/calendar/"; content:"Host|3a| www.google.com|0d
0a|"; nocase; threshold:type both, count 1, seconds 60, track by_src; classtype:policy-violation; reference:url,www.computerworld.com.au/index.php?id=1687889918&eid=-255;
```