


```
#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Tigger.a/Syzor Checkin"; flow:established,to_server; content:"POST "; depth:5; uricontent:"/track.cgi"; content:"|0d 0a 0d 0a|u="; content:"&t="; distance:50; content:"&b="; distance:0; content:"&v="; distance:0; content:"&f="; distance:0; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2009347; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Tigger; sid:2009347; rev:2;)

#sig by matt jonkman, researcher anonymous
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Tigger.a/Syzor Control Checkin"; flow:established,to_server; uricontent:"/track.cgi"; content:"POST "; depth:5;
content:"|0d 0a 0d 0a|u="; distance:50; content:"&t="; distance:0; content:"&v="; distance:0; content:"&f="; distance:0; content:"&z="; distance:0; classtype:trojan-
activity; reference:url,voices.washingtonpost.com/securityfix/2009/02/the_t-i-double_guh-r_trojan_ic.html?wpss=securityfix; reference:url,mmin.blogspot.com/2009/02/why-i-enjoyed-
tiggersyzor.html; reference:url,doc.emergingthreats.net/2009096; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Tigger; sid:2009096; rev:5;)

#by Daniel Clemens
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET MISC TinyPE Binary - Possibly Hostile"; flow:from_server,established; content:"MZ"; content:"PE|00 00|";
within:20;classtype:trojan-activity; reference:url,www.phreedom.org/solar/code/tinype/; reference:url,www.packetninja.net/blog/2008/11/20/ids-signature-for-extremely-small-portable-
executable-files.html; reference:url,doc.emergingthreats.net/2008576; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_TinyPE; sid:2008576; rev:4;)

#by dxp
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Tornado Pack Binary Request"; flow:established,to_server; content:"GET "; depth:4; uricontent:"?o=";
uricontent:"&t="; uricontent:"&i="; uricontent:"&e="; classtype:trojan-activity; reference:url,dxp2532.blogspot.com/2009/05/tornado-exploit-pack.html;
reference:url,doc.emergingthreats.net/2009389; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Tornado; sid:2009389; rev:2;)

#Description of parameters:
#?o= integer value to identify attacker
#&t= integer value represents time the exploit was generated
#&i= integer value represent IP address of victim
#&e= integer value represents exploit used
#Submitted by Tom Fischer, 2006-01-07
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Torpig Reporting User Activity (x25)"; flow:established,to_server; uricontent:"/x25.php"; nocase; uricontent:"?id=";
id="; nocase; uricontent:"&sv="; nocase; uricontent:"&ip="; nocase; uricontent:"&sport="; nocase; uricontent:"&hport="; nocase; uricontent:"&os="; nocase; classtype:trojan-activity;
reference:url,www.sophos.com/virusinfo/analyses/trojtorpigr.html; reference:url,doc.emergingthreats.net/2002762; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/VIRUS/TROJAN_Torpig; sid:2002762; rev:5;)

#Description of parameters:
#?o= integer value to identify attacker
#&t= integer value represents time the exploit was generated
#&i= integer value represent IP address of victim
#&e= integer value represents exploit used
#Submitted by Tom Fischer, 2006-01-07
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Torpig Reporting User Activity (wur8)"; flow:established,to_server; uricontent:"/wur8.php"; nocase; uricontent:"?
id="; nocase; uricontent:"&sv="; nocase; uricontent:"&ip="; nocase; uricontent:"&sport="; nocase; uricontent:"&hport="; nocase; uricontent:"&os="; nocase; classtype:trojan-activity;
reference:url,www.sophos.com/virusinfo/analyses/trojtorpigr.html; reference:url,doc.emergingthreats.net/2003066; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/VIRUS/TROJAN_Torpig; sid:2003066; rev:3;)

#by Michael Hale Ligh
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN VMM Detecting Torpig/Anserin/Sinowal Trojan"; flow:to_client,established; content:"|51 51 0F 01 4C 24 00 8B 44 24 02 59 59
C3 E8 ED FF FF 25 00 00 00 FF 33 C9 3D 00 00 00 80 0F 95 C1 8B C1 C3|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003094;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Torpig; sid:2003094; rev:3;)

#by Michael Hale Ligh
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN (UPX) VMM Detecting Torpig/Anserin/Sinowal Trojan"; flow:to_client,established; content:"|51 51 0F 01 27 00 C1 FB B5 D5 35
02 E2 C3 D1 66 25 32 8D 83 7F B7 4E 3D 06 80 0F 95 C1 8B C1 C3|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003095; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/VIRUS/TROJAN_Torpig; sid:2003095; rev:3;)

#Pedro Marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Sinowal/Torpig Checkin"; flow:to_server,established; content:"GET "; depth:4; uricontent:"idcomp=";
uricontent:"MyValue="; uricontent:"&load1="; uricontent:"&hist=downloaded_user_"; pcre:"/MyValue=[a-f0-9]{32}/Ui"; classtype: trojan-activity;
reference:url,doc.emergingthreats.net/2010267; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Torpig; sid:2010267; rev:2;)

#Pedro Marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Torpig Infection Reporting"; flow:established,to_server; content:"POST "; depth:5; content:"|0d 0a|User-Agent|3a|
"; content:"|0d 0a|Content-Length|3a| 0|0d 0a|"; content:"|0d 0a|Connection|3a| close|0d 0a|"; pcre:"/^\\/[0-9A-F]{16}\\/[0-9A-Za-z+\\/]{}100,}$/U"; classtype:trojan-activity;
reference:url,www2.gmcr.net/mbr/; reference:url,www.cs.ucsb.edu/~seclab/projects/torpig/torpig.pdf; reference:url,doc.emergingthreats.net/2008660; reference:url,offensivecomputing.net/?
q=node/909; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Torpig; sid:2008660; rev:7;)

#matt jonkman, re 3fac60b31a7cda96e217c86405fcc48c
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Torpig Related Fake User-Agent (Apache (compatible...))"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
Apache (compatible|3b| HSIE 6.0|3b| Windows NT 5.1|3b| SV1)"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010823; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/VIRUS/TROJAN_Torpig; sid:2010823; rev:4;)

#matt jonkman, re 3fac60b31a7cda96e217c86405fcc48c
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Torpig Ping-Pong Keepalives Outbound"; flow:to_server; dsiz:9; content:"PONG |3a|"; depth:6; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010824; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Torpig; sid:2010824; rev:3;)

#matt jonkman, re 3fac60b31a7cda96e217c86405fcc48c
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Torpig Ping-Pong Keepalives Inbound"; flow:from_server; dsiz:9; content:"PING |3a|"; depth:6; nocase;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010825; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Torpig; sid:2010825; rev:3;)

#matt jonkman, re 3fac60b31a7cda96e217c86405fcc48c
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 8392 (msg:"ET TROJAN Torpig Initial CnC Connect on port 8392"; flow:established,to_server; dsiz:4; content:"|00 00 78 e3|";
flowbits:set,ET.torpig.init; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010826; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Torpig;
sid:2010826; rev:3;)

#matt jonkman, re 3fac60b31a7cda96e217c86405fcc48c
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 8392 (msg:"ET TROJAN Torpig CnC Connect on port 8392"; flowbits:isset,ET.torpig.init; flow:established,to_server; content:"|00 00|"; depth:2;
content:"|00 00 00|"; distance:2; within:5; flowbits:set,ET.torpig.fosure; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010827;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Torpig; sid:2010827; rev:3;)

#matt jonkman, re 3fac60b31a7cda96e217c86405fcc48c
#
alert tcp $EXTERNAL_NET 8392 -> $HOME_NET any (msg:"ET TROJAN Torpig CnC IP Report Command on port 8392"; flowbits:isset,ET.torpig.fosure; flow:established,from_server; dsiz:4;
content:"|00 00 00 0d|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010828; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Torpig;
sid:2010828; rev:3;)

#matt jonkman, re 3fac60b31a7cda96e217c86405fcc48c
#
#alert tcp $EXTERNAL_NET 8392 -> $HOME_NET any (msg:"ET TROJAN Torpig CnC Report Command on port 8392"; flowbits:isset,ET.torpig.fosure; flow:established,from_server; dsiz:4;
content:"|00 00 01 6f|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2010829; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Torpig;
sid:2010829; rev:3;)

#by: Jeremy Conway at sudosecure.net
#ref: a2c745c5642f6861277e6c49eda01a40
#
```

```

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Trash Family - HTTP POST"; flow:established,to_server; content:"POST "; depth:5; content:!"User-Agent|3a|"; nocase; content:"Type="; nocase; within:200; content:"&Dvip="; nocase; within:20; content:"&Mask="; nocase; within:20; content:"&Guid="; nocase; within:23; content:"&Addr="; nocase; content:"&Protect="; nocase; content:"Url"; nocase; content:"&OSVer="; nocase; classtype:trojan-activity; reference:url,www.spywareguide.com/product_show.php?id=1935; reference:url,www.sunbeltsecurity.com/threaddisplay.aspx?name=Trojan.Trash.Gen&tid=178782&cs=03253E96A71C3EE824071E5BE3A32CCD; reference:url,doc.emergingthreats.net/2009449; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Trash; sid:2009449; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Trats.a Post-Infection Checkin"; flow:established,to_server; uricontent:"AID="; uricontent:"GUID="; nocase; content:"POST "; depth:5; offset:0; content:"|0d 0a|SPK|3a| "; within:200; content:"|0d 0a|User-Agent|3a| Mozilla/4.0 (compatible|3b| MSIE 6.0) WinNT 5.1|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008155; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Trats; sid:2008155; rev:3;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Trest1 Binary Download Attempt (multiple malware variants served)"; flow:established,to_server; content:"GET "; nocase; depth:4; content:!"|0d 0a|Referer|3a| "; nocase; uricontent:"trest1"; nocase; content:"|0d 0a|User-Agent|3a| "; nocase; pcre:"/V/(nte|ld)\/[0-9A-Z]"trest1[0-9](\.\php|\s\.\asp|\.\asp|\.\py|\.\exe|\.\htm|\.\html)\|[A-Z0-9]+$/Ui"; classtype:trojan-activity; reference:url,www.malwaredomainlist.com; reference:url,www.malwareurl.com/search.php?domain=&s=trest1&match=0&rp=200&urls=on&redirs=on&ip=on&reverse=on&as=on; reference:url,doc.emergingthreats.net/2010596; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Trest1; sid:2010596; rev:2;)

#by Christopher Campesi
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1800 (msg:"ET TROJAN TrodJan 2.0 Infection Report"; flow:established,to_server; dsize:<60; content:"Windows NT "; depth:11; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008587; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Trodjan; sid:2008587; rev:3;)

#by Christopher Campesi
#
alert tcp $EXTERNAL_NET 1802 -> $HOME_NET any (msg:"ET TROJAN TrodJan 2.0 FTP Channel Open Command"; flow:established,to_server; dsize:7; content:"ftopen"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008588; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Trodjan; sid:2008588; rev:2;)

#by Matt Jonkman, from sandnet analysis
#some kind of c&c, needs more research, but these sigs are reliable
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Trojan.Win32.Qhost C&C Traffic Outbound (case1)"; flow:established; dsize:>1000; content:"|00 00 00 28 0a 00 00 02 0f|Service Pack 1|00|"; classtype:trojan-activity; reference:url,www.viruslist.com/en/viruses/encyclopedia?virusid=142254; reference:url,doc.emergingthreats.net/2007578; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Trojan.Win32.Qhost; sid:2007578; rev:4;)

#by Matt Jonkman, from sandnet analysis
#some kind of c&c, needs more research, but these sigs are reliable
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Trojan.Win32.Qhost C&C Traffic Outbound (case2)"; flow:established; dsize:>1000; content:"|00 00 00 28 0a 00 00 02 0f|Service Pack 2|00|"; classtype:trojan-activity; reference:url,www.viruslist.com/en/viruses/encyclopedia?virusid=142254; reference:url,doc.emergingthreats.net/2007579; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Trojan.Win32.Qhost; sid:2007579; rev:4;)

#by Matt Jonkman, from sandnet analysis
#some kind of c&c, needs more research, but these sigs are reliable
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN Trojan.Win32.Qhost C&C Traffic Inbound (case1)"; flow:established; dsize:>1000; content:"|00 00 00 28 0a 00 00 02 0f|Service Pack 1|00|"; classtype:trojan-activity; reference:url,www.viruslist.com/en/viruses/encyclopedia?virusid=142254; reference:url,doc.emergingthreats.net/2007580; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Trojan.Win32.Qhost; sid:2007580; rev:4;)

#by Matt Jonkman, from sandnet analysis
#some kind of c&c, needs more research, but these sigs are reliable
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN Trojan.Win32.Qhost C&C Traffic Inbound (case2)"; flow:established; dsize:>1000; content:"|00 00 00 28 0a 00 00 02 0f|Service Pack 2|00|"; classtype:trojan-activity; reference:url,www.viruslist.com/en/viruses/encyclopedia?virusid=142254; reference:url,doc.emergingthreats.net/2007581; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Trojan.Win32.Qhost; sid:2007581; rev:4;)

#by dn1nj4
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 9295 (msg:"ET TROJAN Troxen GetSpeed Request"; flow:established,to_server; content:"GetSpeed |0d 0a|"; depth:11; classtype:trojan-activity; reference:url,www.threatexpert.com/report.aspx?md5=af89d15930fe59dcb621069abc83cc66; reference:url,doc.emergingthreats.net/2011233; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Troxen; sid:2011233; rev:2;)

#by matt jonkman and victor julien
#Backdoor.Win32.Turkojan.jv or Turkojan.gen1 or GenPack:Trojan.Agent.AHAB
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Turkojan C&C Initial Checkin (ams)"; flow:established,to_server; dsize:3; content:"ams"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008021; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Turkojan; sid:2008021; rev:3;)

#by matt jonkman and victor julien
#Backdoor.Win32.Turkojan.jv or Turkojan.gen1 or GenPack:Trojan.Agent.AHAB
#
alert tcp $EXTERNAL_NET 1024: -> $HOME_NET any (msg:"ET TROJAN Turkojan C&C Info Command (MINFO)"; flow:established,from_server; dsize:5; content:"MINFO"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008022; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Turkojan; sid:2008022; rev:3;)

#by matt jonkman and victor julien
#Backdoor.Win32.Turkojan.jv or Turkojan.gen1 or GenPack:Trojan.Agent.AHAB
#
alert tcp $EXTERNAL_NET 1024: (msg:"ET TROJAN Turkojan C&C Info Command Response (MINFO)"; flow:established,to_server; dsize:<100; content:"MINFO|7c|"; depth:6; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008023; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Turkojan; sid:2008023; rev:4;)

#by matt jonkman and victor julien
#Backdoor.Win32.Turkojan.jv or Turkojan.gen1 or GenPack:Trojan.Agent.AHAB
#
alert tcp $EXTERNAL_NET 1024: -> $HOME_NET any (msg:"ET TROJAN Turkojan C&C Logs Parse Command (LOGS1)"; flow:established,from_server; dsize:5; content:"LOGS1"; depth:5; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008024; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Turkojan; sid:2008024; rev:4;)

#by matt jonkman and victor julien
#Backdoor.Win32.Turkojan.jv or Turkojan.gen1 or GenPack:Trojan.Agent.AHAB
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Turkojan C&C Logs Parse Response Response (LOGS1)"; flow:established,to_server; content:"|08 00 00 00|LOGS1|5b|"; offset:0; depth:10; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008025; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Turkojan; sid:2008025; rev:3;)

#by matt jonkman and victor julien
#Backdoor.Win32.Turkojan.jv or Turkojan.gen1 or GenPack:Trojan.Agent.AHAB
#
alert tcp $EXTERNAL_NET 1024: (msg:"ET TROJAN Turkojan C&C Keepalive (BAGLANTI)"; flow:established,to_server; dsize:9; content:"BAGLANTI?"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008026; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Turkojan; sid:2008026; rev:3;)

#by matt jonkman and victor julien
#Backdoor.Win32.Turkojan.jv or Turkojan.gen1 or GenPack:Trojan.Agent.AHAB
#
alert tcp $EXTERNAL_NET 1024: -> $HOME_NET any (msg:"ET TROJAN Turkojan C&C Browse Drive Command (BROWSC)"; flow:established,from_server; dsize:<100; content:"BROWSC"; depth:5; content:"|3a|"; distance:1; within:2; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008027; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Turkojan; sid:2008027; rev:3;)

#by matt jonkman and victor julien
#Backdoor.Win32.Turkojan.jv or Turkojan.gen1 or GenPack:Trojan.Agent.AHAB
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Turkojan C&C Browse Drive Command Response (metin)"; flow:established,to_server; content:"|00 00|metin|0d 3a|"; offset:2; depth:11; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008028; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Turkojan; sid:2008028; rev:3;)

#c&c session 2
#

```

```

alert tcp $EXTERNAL_NET 1024: -> $HOME_NET any (msg:"ET TROJAN Turkojan C&C nxt Command (nxt)"; flow:established,from_server; dsize:3; content:"nxt"; depth:3; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008029; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Turkojan; sid:2008029; rev:3;)

#c&c session 2
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Turkojan C&C nxt Command Response (nxt)"; flow:established,from_server; dsize:16; content:"nxt|09 00 00 00|"; depth:7;
offset:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008030; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Turkojan; sid:2008030;
rev:3;)

#by Jeffrey Brown
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Lighty Variant or UltimateDefender POST"; flow:established,to_server; content:"POST "; depth:5; content:".php";
content:"gd="; content:"&affid="; content:"&subid="; content:"&prov="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008784;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_UltimateDefender; sid:2008784; rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Universal1337 FTP Upload of Compromised Data"; flow:established,to_server; content:"#####|0d 0a|";
content:"#####"; distance:0; content:" Universal1337 "; distance:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/TrojanUniversal1337;
reference:url,www.megasecurity.org/trojans/u/universal1337/Universal1337v2.html; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Universal1337; sid:2007967;
rev:6;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN Universal1337 Email Upload of Compromised Data"; flow:established,to_server; content:"#####|0d 0a|";
content:"#####"; distance:0; content:" Universal1337 "; distance:0; classtype:trojan-activity; reference:url,doc.emergingthreats.net/bin/view/Main/TrojanUniversal1337;
reference:url,www.megasecurity.org/trojans/u/universal1337/Universal1337v2.html; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Universal1337; sid:2007968;
rev:5;)

#by marcus at unsobar
#re: 1331ffcae4e8d1de36a708db0e30346b
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Password Stealing Trojan Check-in"; flow:established,to_server; content:"GET "; depth:4; uricontent:".php";
uricontent:"?action="; uricontent:"&a="; uricontent:"&c="; uricontent:"&u="; uricontent:"&l="; uricontent:"&p="; content:"Host|3a| whos.amung.us"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2009458; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Unknown; sid:2009458; rev:4;)

#by marcus at unsobar
#re: 2cb21d88a0217595455591c7345c0395
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Unknown Trojan HTTP Check-in "; flow:established,to_server; content:"GET "; depth:4; uricontent:".php";
uricontent:"?&mode="; uricontent:"&id="; uricontent:"&output="; uricontent:"&time="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009521;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Unknown; sid:2009521; rev:2;)

#by marcus at unsobar
#re: 3cc737de7ffdb084ae969a7d25dc40c6
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Unknown Trojan Check-in (3)"; flow:established,to_server; content:"GET "; depth:4; uricontent:".asp"; uricontent:"?
username="; uricontent:"&action="; content:"&edition="; pcre:"/\\.asp\\?username=+&serverMac=([0-9A-F]{2}-){5}[0-9A-F]{2}&edition=Ui"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2009532; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Unknown; sid:2009532; rev:3;)

#by Anonymous Submitter #2
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Unknown Trojan User-Agent (5.1 ...)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| 5.1 ";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009685; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Unknown; sid:2009685; rev:4;)

#by: Jeremy Conway at sudosecure.net
#ref: 13b0745b6e756120367d31fb404f360c
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Generic/Unknown Downloader Config to client"; flow:established,to_client; content:"[InstallerIni]"; nocase;
depth:300; content:"|0d 0a|Pid="; nocase; within:6; content:"|0d 0a|Product="; nocase; content:"|0d 0a|FID="; nocase; content:"|0d 0a|Title="; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2009809; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Unknown; sid:2009809; rev:2;)

#by: Jeremy Conway at sudosecure.net
#ref: 2763eedda0b2dc446adb1f84f9f35fc1
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Unknown Web Bot checkin Possible Bruteforcer for Web Forms and Accounts - HTTP POST"; flow:established,to_server;
content:"POST "; depth:5; content:"&ver="; nocase; content:"&MAX_EXECUTE_TIME="; nocase; content:"&RELOAD_JOBS="; nocase; content:"&BROWSER_DELAY="; nocase; content:"&CONTROL_PAGE=";
nocase; content:"&lastlogcount="; nocase; content:"&min_captcha_size="; nocase; content:"&REPORTS_PAGE="; nocase; content:"&TICKETS_PAGE="; nocase; content:"&botid="; nocase;
content:"&REG_NAME="; nocase; content:"&botlogin="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009830; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/VIRUS/TROJAN_Unknown; sid:2009830; rev:2;)

#by Mike Cox
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Suspicious exe.exe request - possible downloader/Oficla"; flow:to_server,established; uricontent:"/exe.exe"; nocase;
pcre:"/^\\/exe\\.exe$/Ui"; nocase; classtype:trojan-activity; reference:url,anubis.iseclab.org/?action=result&task_id=11873c8979f34c8d4fd0da512df635cac&format=txt;
reference:url,doc.emergingthreats.net/2010741; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Unknown; sid:2010741; rev:2;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Java Downloader likely malicious payload download src=xrun"; flow:established,to_server; content:"GET /get?src=xrun
HTTP/1."; nocase; content:"|0d 0a|Request|3a| "; nocase; classtype:trojan-activity; reference:url,www.bluetack.co.uk/forums/lofiversion/index.php/t18462.html;
reference:url,doc.emergingthreats.net/2010821; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Unknown; sid:2010821; rev:3;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN WScript/VBScript XMLHTTP downloader likely malicious get?src="; flow:established,to_server; content:"|0d 0a|User-
Agent|3a| Mozilla/4.0 (compatible|3b| Win32|3b| WinHttp.WinHttpRequest"; nocase; uricontent:"/get?src="; nocase; content:"|0d 0a|Request|3a| "; nocase; content:"run|0d 0a|"; within:5;
classtype:trojan-activity; reference:url,www.bluetack.co.uk/forums/lofiversion/index.php/t18462.html; reference:url,doc.emergingthreats.net/2010838;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Unknown; sid:2010838; rev:3;)

#2010-07-14 By Pedro Marinho
#7722a1c565c215c9e07b53a117958f
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Trojan.StartPage activity"; flow:to_server,established; content:"GET "; depth:4; uricontent:"stat.htm?id=";
uricontent:"&r="; uricontent:"&l="; uricontent:"&time="; uricontent:"&repeatip="; uricontent:"&rtime="; uricontent:"&cnz|5f|eid="; uricontent:"|2d|&showp="; uricontent:"&st=";
uricontent:"&sin="; uricontent:"&res="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2011228; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/VIRUS/TROJAN_Unknown; sid:2011228; rev:1;)

#by darren spruell
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Unruly Downloader Checkin"; flow:established,to_server; uricontent:".php?u="; nocase; uricontent:"@"; pcre:"/^\\.php\\?
U=vd+@vd+@vd+@vd+@[a-f0-9]+$/Ui"; classtype:trojan-activity; reference:url,ddanchev.blogspot.com/2010/03/copyright-lawsuit-filed-against-you.html;
reference:url,isc.sans.org/diary.html?storyid=8497; reference:url,threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?vName=TROJ_AGENT_STH&VSet=T;
reference:url,doc.emergingthreats.net/2010975; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Unruly; sid:2010975; rev:3;)

#by Dan Clemens
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN VMProtect Demo version Packed Binary - Likely Hostile"; flow:from_server,established; content:"|2E|rsrc|00|";
content:"vmp0|00|"; within: 50; content:"vmp1|00|"; within:50; classtype:trojan-activity; reference:url,www.vmprotect.ru; reference:url,www.packetninja.net;
reference:url,doc.emergingthreats.net/2009019; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_VMProtect; sid:2009019; rev:2;)

```

```

#from sandnet analysis, by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Vanquish Trojan HTTP Checkin"; flow:established,to_server; uricontent:"ip="; uricontent:"&v=1&s="; uricontent:"&h="; uricontent:"&kb="; uricontent:"&o="; uricontent:"&c="; uricontent:"&un="; uricontent:"&m="; uricontent:"&w="; uricontent:"&ss="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007698; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Vanquish; sid:2007698; rev:3;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Vapsup User-Agent (doshowmeanad loader v2.1)"; flow:to_server,established; content:"|0d 0a|User-Agent|3a|doshowmeanad "; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008142; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Vapsup; sid:2008142; rev:4;)

#by matt jonkman
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Vipdataend C&C Traffic - Checkin"; flow:established,to_server; dsize:<20; content:"|3a|"; depth:5; offset:2; content:"|7c| "; within:8; depth:12; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007962; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Vipdataend; sid:2007962; rev:6;)

#by matt jonkman
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Vipdataend C&C Traffic - Status OK"; flow:established,to_server; dsize:2; content:"OK"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007963; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Vipdataend; sid:2007963; rev:4;)

#by matt jonkman
#
#alert tcp $EXTERNAL_NET 1024: -> $HOME_NET 1024: (msg:"ET TROJAN Vipdataend C&C Traffic - Server Status OK"; flow:established,to_server; dsize:2; content:"OK"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007964; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Vipdataend; sid:2007964; rev:4;)

#by matt jonkman
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Vipdataend C&C Traffic - Checkin (XY)"; flow:established,to_server; dsize:<20; content:"XY|3a|2|7c|212"; offset:0; depth:9; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007970; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Vipdataend; sid:2007970; rev:7;)

#by matt jonkman
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Vipdataend C&C Traffic - Checkin (FYWL)"; flow:established,to_server; dsize:11; content:"FYWL|3a|2|7c|212"; offset:0; depth:11; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008223; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Vipdataend; sid:2008223; rev:4;)

#by matt jonkman
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Vipdataend C&C Traffic - Checkin (XYLL)"; flow:established,to_server; dsize:11; content:"XYLL|3a|2|7c|212"; offset:0; depth:11; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008224; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Vipdataend; sid:2008224; rev:4;)

#new variation, also called Ceckno now
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Vipdataend/Ceckno C&C Traffic - Checkin"; flow:established,to_server; dsize:<30; content:"VERSIONEXC|3a|2|7c|212|7c|"; depth:16; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008254; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Vipdataend; sid:2008254; rev:4;)

#greg bowser
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Beizhu/Womble/Vipdataend Checking in with Controller"; flow:established,to_server; dsize:<70; content:"|3a|Windows"; depth:11; offset:2; content:"|7c|212("; distance:0; within:15; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008334; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Vipdataend; sid:2008334; rev:9;)

#greg bowser
#
#alert tcp $EXTERNAL_NET 1024: -> $HOME_NET 1024: (msg:"ET TROJAN Beizhu/Womble/Vipdataend Controller Keepalive"; flow:established,from_server; dsize:1; content:"d"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008335; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Vipdataend; sid:2008335; rev:7;)

#matt jonkman
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Vipdataend C&C Traffic - Checkin (variant 2)"; flowbits:set,ET.vipdataend; flow:established,to_server; dsize:<22; content:"|3a|"; depth:5; offset:2; content:"|7c|win "; within:8; depth:12; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009025; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Vipdataend; sid:2009025; rev:2;)

#matt jonkman
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Vipdataend C&C Traffic - Status OK (variant 2)"; flowbits:isset,ET.vipdataend; flow:established,to_server; dsize:1; content:"1"; depth:1; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009026; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Vipdataend; sid:2009026; rev:3;)

#matt jonkman
#
#alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Vipdataend C&C Traffic - Checkin (variant 3)"; flow:established,to_server; dsize:<42; content:"|3a|Windows "; depth:11; offset:2; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009037; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Vipdataend; sid:2009037; rev:2;)

#by Daniel Clemens of packetninjas
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN VirtualProtect Packed Binary - Likely Hostile"; flow:established,from_server; content:"|2E 72 73 72 63|"; content:"|2E 70 61 63 6B 33 32 00|"; within:49; classtype:trojan-activity; reference:url,bits.packetninjas.org/eblog/?p=3; reference:url,doc.emergingthreats.net/2008509; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_VirtualProtect; sid:2008509; rev:3;)

#by Matt Jonkman, from Sandnet data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Virtumonde Variant Reporting to Controller via HTTP"; flow:established,to_server; uricontent:"?sid="; pcre:"/\?sid=[0-9A-F]{180}/U"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007142; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Virtumonde; sid:2007142; rev:3;)

#by Matt Jonkman, from Sandnet data
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Virtumonde Variant Reporting to Controller via HTTP (2)"; flow:established,to_server; uricontent:"php?"; nocase; uricontent:"cmp="; nocase; uricontent:"&guid="; nocase; uricontent:"&affid="; nocase; uricontent:"&run="; nocase; uricontent:"&dn_uid="; nocase; uricontent:"&dn_affid="; nocase; uricontent:"&vm_guid="; nocase; uricontent:"&ip="; nocase; uricontent:"&altid="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007285; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Virtumonde; sid:2007285; rev:3;)

#by jeremy at sudosecure
#ref: 196df30f6f8a8a1b42ee19ac58404553
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Virtumod/Agent.ufv/Virtumonde Get Request"; flow:established,to_server; content:"GET "; depth:4; uricontent:".php?"; nocase; uricontent:"ver="; nocase; uricontent:"aid="; nocase; uricontent:"uid="; nocase; uricontent:"adm="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008377; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Virtumonde; sid:2008377; rev:2;)

#by robert grabowsky
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Virtumonde Variant Reporting to Controller via HTTP (3)"; flow:established,to_server; uricontent:"dll.html?"; nocase; uricontent:"affid="; nocase; uricontent:"&uid="; nocase; uricontent:"&guid="; nocase; classtype:trojan-activity; reference:url,www.threatexpert.com/reports.aspx?find=apstpldr.dll.html; reference:url,doc.emergingthreats.net/2008863; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Virtumonde; sid:2008863; rev:3;)

#by Matt Jonkman
#

```

```

alert tcp $HOME_NET any -> $EXTERNAL_NET 3306 (msg:"ET TROJAN Viruscatch.co.kr/Win32.Small.hvd Mysql Command and Control Connection (user viruscatch)"; flow:established,to_server;
size:<40; content:"viruscatch|00|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008573; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Viruscatch.co.kr; sid:2008573; rev:3;)

#by Jeffrey Brown
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Virusremover2008.com Checkin"; flow:to_server,established; content:"GET "; depth:4; nocase; uricontent:"?action=";
nocase; uricontent:"pc_id="; nocase; uricontent:"abbr="; content:"|0d 0a|User-Agent|3a| Statistican"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008527;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Virusremover2008; sid:2008527; rev:4;)

#by Daniel D.L.
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 65520 (msg:"ET TROJAN W32.Virut.A joining an IRC Channel"; flow:established,to_server; content:"JOIN &virtu"; classtype:trojan-activity;
reference:url,www.bitcrank.net; reference:url,doc.emergingthreats.net/2003603; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Virut; sid:2003603; rev:3;)

#by Marcus at unsobar
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Virut Counter/Check-in "; flow:established,to_server; content:"GET "; depth:4; uricontent:".asp?mac=";
uricontent:"&ver="; pcre:"/\.asp\?mac=([0-9A-F]{2}-){5}([0-9A-F]{2}-){5}([0-9A-F]{2}-){5}([0-9A-F]{2}-){5}([0-9A-F]{2}-){5}"; classtype:trojan-activity; reference:url,www.threatexpert.com/reports.aspx?find=ipk8888.cn&x=0&y=0;
reference:url,doc.emergingthreats.net/2009374; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Virut; sid:2009374; rev:5;)

#by Marcus at unsobar
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Virut Counter/Check-in "; flow:established,to_server; content:"POST "; depth:5; uricontent:".asp?mac=";
uricontent:"&rw="; uricontent:"&ver="; pcre:"/\.asp\?mac=([0-9A-F]{2}-){5}([0-9A-F]{2}-){5}([0-9A-F]{2}-){5}([0-9A-F]{2}-){5}([0-9A-F]{2}-){5}"; classtype:trojan-activity; reference:url,www.threatexpert.com/reports.aspx?
find=ipk8888.cn&x=0&y=0; reference:url,doc.emergingthreats.net/2009457; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Virut; sid:2009457; rev:5;)

#by: Jeremy Conway at sudosecure.net
#ref: 033fc21398c0d5749c4c25264c965079 83bbad45a9feefc5dd4778d148e8117f 5749d778d71b887918f9dcf91fe886a8c 726c8cd8cf81bed3161ea5fb6e8b73e4 8cf101c6f61573f1bb24f229923393e2
2d17a20a77e298263c5ace8adfc186a5 a955101b1469ca0dbd163d995e6448c9 23a96a8b87dc3fbc8ce2f0f87c719d56
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Virut Family GET"; flow:established,to_server; content:"GET "; depth:4; uricontent:"/lgate.php?n="; pcre:"/n=[0-9A-
F]{12,24}/Ui"; classtype:trojan-activity; reference:url,www.f-secure.com/v-descs/virus_w32_virut.shtml; reference:url,www.spywareremove.com/removeVirusVirutr.html;
reference:url,www.malwaredomainlist.com/mdl.php?search=lgate.php&colsearch=All&quantity=50; reference:url,www.threatexpert.com/reports.aspx?find=virut&x=0&y=0;
reference:url,doc.emergingthreats.net/2009444; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Virut; sid:2009444; rev:2;)

#by: Jeremy Conway at sudosecure.net
#ref: 5dbc7f794a749f09cfc3b705d89ec7fe
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Virut - GET"; flow:established,to_server; content:"GET "; depth:4; uricontent:"?n="; nocase;
uricontent:"&lastid="; nocase; uricontent:"&Version="; nocase; uricontent:"&smartpic="; nocase; uricontent:"&rand="; nocase; classtype:trojan-activity;
reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fVirut; reference:url,www.avast.com/eng/win32-virut.html; reference:url,free.avg.com/66558;
reference:url,www.threatexpert.com/threats/virus-win32-virut-ce.html; reference:url,doc.emergingthreats.net/2009808; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Virut; sid:2009808; rev:2;)

#by: Jeremy Conway at sudosecure.net
#ref: 452b0c4cefeb0339d69582174954210e
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Virut/Virutas/Virtob/QQHelper Dropper Family - HTTP GET"; flow:established,to_server; content:"GET "; depth:4;
uricontent:"?SoftName="; nocase; uricontent:"&SoftVersion="; nocase; uricontent:"&UserIP="; nocase; uricontent:"&Mac="; nocase; classtype:trojan-activity;
reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=TrojanDownloader%3AWin32%2fQQHelper.gen!E8ThreatID=-2147371486;
reference:url,www.sophos.com/security/analyses/viruses-and-spyware/w32virutl.html; reference:url,www.threatexpert.com/threats/w32-virut-l.html;
reference:url,doc.emergingthreats.net/2009829; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Virut; sid:2009829; rev:2;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Visual Shock Keylogger Reporting to Controller"; flow:established,to_server; size:<150; content:"|00 00|Visual Shock
Keylogger "; offset:10; depth:34; classtype:trojan-activity; flowbits:set,ET.vskeylogger; reference:url,research.sunbelt-software.com/threatdisplay.aspx?threatid=42573;
reference:url,doc.emergingthreats.net/2008601; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Visual_Shock_Keylogger; sid:2008601; rev:2;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"ET TROJAN Visual Shock Keylogger Reporting Idle to Controller"; flowbits:isset,ET.vskeylogger; flow:established,to_server; size:8;
content:"|08 00 00 00 00 00 00 00|"; classtype:trojan-activity; reference:url,research.sunbelt-software.com/threatdisplay.aspx?threatid=42573;
reference:url,doc.emergingthreats.net/2008602; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Visual_Shock_Keylogger; sid:2008602; rev:2;)

#by Matt Jonkman
#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Vundo.dam http Checkin after infection"; flow:established,to_server; uricontent:"install.php?"; nocase;
uricontent:"&fid="; nocase; uricontent:"&user_id="; nocase; uricontent:"&version="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007572;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Vundo; sid:2007572; rev:3;)

#by Matt Jonkman
#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Vundo.dam http Update"; flow:established,to_server; uricontent:"/cgi-bin/heartbeat.php"; nocase; uricontent:"uid=";
nocase; uricontent:"&affiliate_id="; nocase; uricontent:"&db=1"; nocase; uricontent:"&version="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007573;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Vundo; sid:2007573; rev:3;)

#by victor julien
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Vundo HTTP Pre-Install Checkin"; flow:established,to_server; uricontent:"/app/preinstall.php?"; nocase;
uricontent:"t_uid="; nocase; uricontent:"&t_pid="; nocase; uricontent:"&t_mac="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007989;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Vundo; sid:2007989; rev:2;)

#by victor julien
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Vundo HTTP Post-Install Checkin"; flow:established,to_server; uricontent:"/app/install_done.php?"; nocase;
uricontent:"t_uid="; nocase; uricontent:"&t_pid="; nocase; uricontent:"&t_mac="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007990;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Vundo; sid:2007990; rev:2;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Vundo HTTP Post-Install Checkin (2)"; flow:established,to_server; uricontent:"?w="; nocase; uricontent:"&cid=";
nocase; uricontent:"&e=00"; nocase; uricontent:"&err="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008082; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Vundo; sid:2008082; rev:2;)

#by Netmonk
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Vundo Variant reporting to Controller via HTTP (1)"; flow:established,to_server; content:"POST "; depth:5;
uricontent:"/req.html?suid=&cuid="; uricontent:"&tld="; uricontent:"&cv="; uricontent:"&affid="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008976;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Vundo; sid:2008976; rev:3;)

#by Netmonk
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Vundo Variant reporting to Controller via HTTP (2)"; flow:established,to_server; content:"GET "; depth:4;
uricontent:"?cuid="; uricontent:"&suid="; uricontent:"&affid="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008977; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Vundo; sid:2008977; rev:3;)

#by Nathaniel Richmond
#Since it's a POST, there shouldn't be many false positives
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Possible Vundo Trojan Variant reporting to Controller"; flow:established,to_server; content:"POST "; depth:5;
uricontent:"/frame.html?"; urlen:> 80; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009173; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Vundo; sid:2009173; rev:2;)

```

```

#by Nathaniel Richmond
#Since it's a POST, there shouldn't be many false positives
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Possible Vundo EXE Download Attempt"; flow:established,to_server; content:"GET "; depth:4; uricontent:"/dwn/d.html?
sid="; urlen: > 80; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009174; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Vundo;
sid:2009174; rev:2;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Vundo User-Agent Check-in"; flow:established,to_server; content:"[0d 0a|User-Agent|3a| Mozilla/4.0 (compatible|3b|
MSIE 6.0) WinNT 5.1|0d 0a|"; classtype:trojan-activity; reference:url,www.symantec.com/security_response/writeup.jsp?docid=2004-112111-3912-99;
reference:url,doc.emergingthreats.net/2010490; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Vundo; sid:2010490; rev:4;)

#by Tom Fischer
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.VB.aie Reporting User Activity"; flow:established,to_server; uricontent:"php?iso="; nocase;
uricontent:"&country="; nocase; uricontent:"&proxy="; nocase; uricontent:"&tel="; nocase; uricontent:"&ftp="; nocase; uricontent:"&socks="; nocase; uricontent:"&remote="; nocase;
uricontent:"&smt="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2002857; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/VIRUS/TROJAN_W32.VB.aie; sid:2002857; rev:3;)

#by Mark Tombaugh, analysis at Nepenthes
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN w32agent.dsi Domain Update"; flow:established,to_server; uricontent:"/getgewinnspiel.php?uid="; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/2002782; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_W32Agent.dsi; sid:2002782; rev:5;)

#by Mark Tombaugh, analysis at Nepenthes
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN w32agent.dsi Posting Info"; flow:established,to_server; uricontent:"/postgewinnspiel.php"; uricontent:"uid=";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2002781; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_W32Agent.dsi; sid:2002781; rev:5;)

#by shadowserver, steven
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Waledac Beacon Traffic Detected"; flow:to_server,established; content:"POST /"; depth:6; content:"[0d 0a|Referer|3a|
Mozilla|0d 0a|"; nocase; within:50; content:"[0d 0a|User-Agent|3a| Mozilla|0d 0a|"; within:120; content:"a="; nocase; within: 100; classtype:trojan-activity;
reference:url,www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20081231; reference:url,doc.emergingthreats.net/2008958; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/VIRUS/TROJAN_Waledac; sid:2008958; rev:3;)

#Matt Jonkman
#Experimental, may only apply to a few variants, but worth testing
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Warezov/Stration Challenge"; flow:established,to_server; dsize:1; content:"|38|"; flowbits:noalert;
flowbits:set,BEposs.warezov.challenge; classtype:not-suspicious; reference:url,www.sophos.com/security/analyses/w32strationbo.html; reference:url,doc.emergingthreats.net/2003175;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Warezov; sid:2003175; rev:5;)

#Matt Jonkman
#Experimental, may only apply to a few variants, but worth testing
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN Warezov/Stration Challenge Response"; flowbits:isset,BEposs.warezov.challenge; flow:established,from_server; dsize:4;
content:"|00 00 00 00|"; classtype:trojan-activity; reference:url,www.sophos.com/security/analyses/w32strationbo.html; reference:url,doc.emergingthreats.net/2003176;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Warezov; sid:2003176; rev:5;)

#Matt Jonkman
#Experimental, may only apply to a few variants, but worth testing
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Possible Warezov/Stration Data Post to Controller"; flow:established,to_server; dsize:<400; uricontent:"/cgi-
bin/pr.cgi"; content:"POST "; depth:5; nocase; classtype:trojan-activity; reference:url,www.sophos.com/security/analyses/w32strationbo.html;
reference:url,doc.emergingthreats.net/2003180; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Warezov; sid:2003180; rev:9;)

#Matt Jonkman, strangely enough from spyware listening post hits
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Warezov/Stration Communicating with Controller 2"; flow:established,to_server; uricontent:"/chr/"; nocase;
uricontent:"/e/"; uricontent:"?lid="; nocase; pcre:"/\\chr\\d\\e\\t\\d\\?lid=Ui"; classtype:trojan-activity; reference:url,www.sophos.com/security/analyses/w32strationbo.html;
reference:url,www.avira.com/en/threats/section/fulldetails/id_vir/3242/tr_dldr.warezov.df.html; reference:url,doc.emergingthreats.net/2003436; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/VIRUS/TROJAN_Warezov; sid:2003436; rev:4;)

#from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Possible Warezov/Stration Data Post to Controller (pr2.cgi)"; flow:established,to_server; uricontent:"/cgi-
bin/pr2.cgi"; pcre:"/\\cgi-bin\\pr2\\.cgi\\?[a-zA-Z0-9]{172}/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2006414; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/VIRUS/TROJAN_Warezov; sid:2006414; rev:4;)

#by Matt Jonkman, from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Agent.ajx Trojan Reporting to Server"; flow:established,to_server; uricontent:"/count.php?fid="; nocase;
uricontent:"&id="; nocase; uricontent:"&ver="; nocase; uricontent:"&tid="; nocase; uricontent:"&sn="; nocase; uricontent:"&wc="; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2006448; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Agent.ajx; sid:2006448; rev:3;)

#by Scott Melnick
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 5190 (msg:"ET TROJAN Win32.Agent.bea C&C connection"; flow:to_server,established; dsize:24; content:"|9a 02 06 00|"; depth:4; classtype:trojan-
activity; reference:url,doc.emergingthreats.net/2007608; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Agent.bea; sid:2007608; rev:3;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Agent.cyt (Or variant) HTTP POST Checkin"; flow:established,to_server; content:"POST "; depth:5;
uricontent:".cgi"; content:"[0d 0a 0d 0a|o=i&k="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008003; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Agent.cyt; sid:2008003; rev:2;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Agent.cyt (Or variant) HTTP POST Checkin (2)"; flow:established,to_server; content:"POST "; depth:5;
uricontent:".cgi"; content:"[0d 0a 0d 0a|o=c&s="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008004; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Agent.cyt; sid:2008004; rev:2;)

#from sandnet analysis
#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Agent.pt User-Agent Detected"; flow:established,to_server; content:"[0d 0a|User-Agent|3a| Machaon|0d 0a|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007663; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Agent.pt; sid:2007663; rev:4;)

#by matt jonkman, re 31fc628bf3c76e9b446d2eac18046b87, www.kjfbk07814.com/log/proc.php?key=RC4525F0sd2
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Cloaker Related Post Infection Checkin"; flow:established,to_server; uricontent:"/log/proc.php?key=";
pcre:"/\\log\\proc\\.php\\.key=[a-z0-9]{11}/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008185; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Cloaker; sid:2008185; rev:3;)

#kind of a general inject win32 kinda thing, but seeing it frequently
#such as 7438b695c0f32cb5c3a0a89485a362c1, by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Inject.ql Checkin Post"; flow:established,to_server; content:"POST "; depth:5; content:"[0d 0a 0d 0a|MAC=";
nocase; content:"&IP="; nocase; distance:17; content:"&NAME="; nocase; distance:7; content:"&OS="; nocase; distance:0; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2007803; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Inject; sid:2007803; rev:2;)

#kind of a general inject win32 kinda thing, but seeing it frequently
#such as 7438b695c0f32cb5c3a0a89485a362c1, by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Inject.zy Checkin Post"; flow:established,to_server; dsize:8; content:"|16 00 00 00 00 00 00 00|";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007966; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Inject; sid:2007966; rev:2;)

```

```
#re Trojan.Win32.Inject.ajq, by matt jonkman
#5bb2b20d012cfe541f173881be28729
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Inject.ajq Initial Checkin to CnC"; flow:established,to_server; dsize:1; content:"|c8|";
flowbits:set,ET.inj.ajq.1; flowbits:noalert; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008055; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Inject; sid:2008055; rev:3;)

#re Trojan.Win32.Inject.ajq, by matt jonkman
#5bb2b20d012cfe541f173881be28729
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Inject.ajq Initial Checkin to CnC packet 2"; flow:established,to_server; content:"|07|F"; depth:2;
flowbits:set,ET.inj.ajq.1; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008056; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Inject; sid:2008056; rev:4;)

#re Trojan.Win32.Inject.ajq, by matt jonkman
#5bb2b20d012cfe541f173881be28729
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Win32.Inject.ajq Initial Checkin to CnC Response"; flow:established,from_server; flowbits:isset,ET.inj.ajq.1;
dsize:4; content:"|00 0e 04 00|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008057; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Inject; sid:2008057; rev:2;)

#also seeing the same on 443
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 443 (msg:"ET TROJAN Win32.Inject.ajq Initial Checkin to CnC port 443"; flow:established,to_server; dsize:1; content:"|c8|";
flowbits:set,ET.inj.ajq.1; flowbits:noalert; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008058; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Inject; sid:2008058; rev:3;)

#also seeing the same on 443
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 443 (msg:"ET TROJAN Win32.Inject.ajq Initial Checkin to CnC packet 2 port 443"; flow:established,to_server; content:"|07|F"; depth:2;
flowbits:isset,ET.inj.ajq.1; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008059; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Inject; sid:2008059; rev:4;)

#also seeing the same on 443
#
alert tcp $EXTERNAL_NET 443 -> $HOME_NET any (msg:"ET TROJAN Win32.Inject.ajq Initial Checkin to CnC Response port 443"; flow:established,from_server; flowbits:isset,ET.inj.ajq.1;
dsize:4; content:"|00 0e 04 00|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008060; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Inject; sid:2008060; rev:2;)

#matt jonkman, re: 7538138be308ffc1747ec656e932c157
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 443 (msg:"ET TROJAN Win32.Onlinegames.ajok CnC Packet to Server"; flow:established,to_server; dsize:20; content:"|7e 7e 7e|"; depth:4;
content:"|7e 7e 7e|"; distance:0; within:4; flowbits:set,ET.onlinegames.ajok; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008291;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Onlinegames; sid:2008291; rev:3;)

#matt jonkman, re: 7538138be308ffc1747ec656e932c157
#
alert tcp $EXTERNAL_NET 443 -> $HOME_NET any (msg:"ET TROJAN Win32.Onlinegames.ajok CnC Packet from Server"; flow:established,from_server; flowbits:isset,ET.onlinegames.ajok;
content:"|7e 7e 7e|"; depth:4; content:"|7e 7e 7e|"; distance:0; within:4; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008292;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Onlinegames; sid:2008292; rev:3;)

#by Jeremy at Sudosecure.net
#ref: 93ef78fea3f6a61e02091f70db01934c
#
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Win32.Small.wpx or Related Downloader Posting Data"; flow:to_server,established; content:"POST "; depth:5;
content:"|22|boturl|22|"; nocase; content:"|22|filename|22|"; nocase; content:"|22|comps|22|"; nocase; content:"|22|loadername|22|"; nocase; content:"|22|loaderid|22|"; nocase;
content:"|22|uptime|22|"; nocase; content:"|22|comptime|22|"; nocase; content:"|22|winver|22|"; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008319;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Small; sid:2008319; rev:4;)

#by victor Julien
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Small.yml or Related HTTP Checkin"; flow:established,to_server; uricontent:"/ClientReg.aspx?mac=";
uricontent:"&type="; uricontent:"&sn="; pcre:"/mac=([0-9A-F]{2}:){5}([0-9A-F]{2})/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008949;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Small; sid:2008949; rev:4;)

#by victor Julien
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Small.yml or Related HTTP Command"; flow:established,to_server; uricontent:"/ClientTask.aspx?mac=";
uricontent:"&type="; uricontent:"&sn="; pcre:"/mac=([0-9A-F]{2}:){5}([0-9A-F]{2})/Ui"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008952;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Small; sid:2008952; rev:3;)

#Ikarus: Trojan.Win32.Small.yml,
#re f01fd7ecfce8af65832a3a57d2789fa6
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Trojan.Win32.Small.yml client registration"; flow:established,to_client; content:"|0d 0a|Content-Length|3a| ";
depth:500; content:"|0d 0a 0d 0a|xxyyssign|0d 0a|xxyy|myIP="; within:27; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008950;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Small; sid:2008950; rev:3;)

#Ikarus: Trojan.Win32.Small.yml,
#re f01fd7ecfce8af65832a3a57d2789fa6
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Trojan.Win32.Small.yml client command"; flow:established,to_client; content:"|0d 0a|Content-Length|3a| "; depth:500;
content:"|0d 0a 0d 0a|xxyyssign|0d 0a|xxyy|UserNamePassword="; within:40; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008951;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Small; sid:2008951; rev:3;)

#matt jonkman
#re 3379d200ba7004dc7aa32db8ea118017
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Small.AB or related Post-infection checkin"; flow:established,to_server; uricontent:"/work.php?"; nocase;
uricontent:"method="; nocase; uricontent:"&port="; nocase; uricontent:"&winver="; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008321; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Small.AB; sid:2008321; rev:2;)

#by Matt Jonkman, from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Small.qh/xSock User-Agent Detected"; flow:established,to_server; content:"User-Agent|3a| xSock Config";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007609; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Small.qh; sid:2007609;
rev:4;)

#by Matt Jonkman, from sandnet analysis
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.Small.qh/xSock Checkin URL Detected"; flow:established,to_server; uricontent:"port="; nocase;
uricontent:"&id="; nocase; uricontent:"&v="; nocase; uricontent:"&sn="; nocase; pcre:"/port=d4/Ui"; pcre:"/id=[a-f0-9-]+&/Ui"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2007610; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Small.qh; sid:2007610; rev:3;)

#by: Jeremy Conway at sudosecure.net
#ref: 2e79af552fa6d3bd2cb654cc0f15cd76
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32.VB.tdq - Fake User-Agent"; flow:established,to_server; content:"GET "; depth:4; content:"|0d0a|User-Agent|3a|
Mozilla/4.0 (compatible|3b| MSIE 5.0|3b| Windows NT 2.1|3b| SV3)|0d0a|"; classtype:trojan-activity; reference:url,vil.nai.com/vil/content/v_187654.htm;
reference:url,home.mcafee.com/VirusInfo/VirusProfile.aspx?key=187654; reference:url,doc.emergingthreats.net/2009825; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.VB; sid:2009825; rev:4;)

#by shirkdog, from sandnet analysis
#
```

```

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Proxy.Win32.Wopla.ag Check-In"; flow:established,to_server; dsize:12; content:"|0a 00 00 00 00 00 00 00 00 00|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007603; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Wopla; sid:2007603; rev:4;)

#by shirkdog, from sandnet analysis
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Proxy.Win32.Wopla.ag Server Reply"; dsize:12; flow:established,from_server; content:"|0d 00 00 00|"; depth:4; content:"|00 00 00 00 00 00|"; distance:2; within:6; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007604; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Win32.Wopla; sid:2007604; rev:5;)

#by Kevin Ross
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Win32/Winwebsec User-Agent Detected"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| InstallNotify/1.0"; classtype:trojan-activity; reference:url,www.f-secure.com/sw-desc/rogue_w32_winwebsec.shtml; reference:url,blogs.technet.com/mmpc/archive/2009/05/13/msrt-tackles-another-rogue.aspx; reference:url,doc.emergingthreats.net/2008986; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_WinWebSec; sid:2008986; rev:2;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN WindowsEnterpriseSuite FakeAV check-in HEAD"; flow:established,to_server; content:"HEAD "; depth:5; uricontent:"? controller="; uricontent:"&abbr="; uricontent:"&setupType="; uricontent:"&ttl="; uricontent:"&pid="; classtype:trojan-activity; reference:url,www.threatexpert.com/report.aspx?md5=d9bcb4e4d650a6ed4402fab8f9ef1387; reference:url,doc.emergingthreats.net/2010240; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_WindowsEnterpriseFakeAV; sid:2010240; rev:2;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN WindowsEnterpriseSuite FakeAV check-in GET"; flow:established,to_server; content:"GET "; depth:4; uricontent:"? controller="; uricontent:"&abbr="; uricontent:"&setupType="; uricontent:"&ttl="; classtype:trojan-activity; reference:url,www.threatexpert.com/report.aspx?md5=d9bcb4e4d650a6ed4402fab8f9ef1387; reference:url,doc.emergingthreats.net/2010241; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_WindowsEnterpriseFakeAV; sid:2010241; rev:2;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN WindowsEnterpriseSuite FakeAV get_product_domains.php"; flow:established,to_server; content:"GET "; depth:4; uricontent:"/reports/get_product_domains.php?abbr="; uricontent:"&pid="; classtype:trojan-activity; reference:url,www.threatexpert.com/report.aspx?md5=d9bcb4e4d650a6ed4402fab8f9ef1387; reference:url,doc.emergingthreats.net/2010242; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_WindowsEnterpriseFakeAV; sid:2010242; rev:2;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN WindowsEnterpriseSuite FakeAV Reporting via POST"; flow:established,to_server; content:"POST "; depth:5; content:"verint="; content:"&uid="; content:"&wvv="; content:"&report="; content:"&abbr="; content:"&pid="; pcre:"/verint=d&uid=d&wvv=[A-Za-z0-9]+&report=d&abbr=[A-Za-z0-9]+&pid=d/"; classtype:trojan-activity; reference:url,www.threatexpert.com/report.aspx?md5=d9bcb4e4d650a6ed4402fab8f9ef1387; reference:url,doc.emergingthreats.net/2010247; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_WindowsEnterpriseFakeAV; sid:2010247; rev:2;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN WindowsEnterpriseSuite FakeAV Reporting via POST initial check-in"; flow:established,to_server; content:"POST "; depth:5; uricontent:"/MicroinstallServiceReport.php"; content:"report="; content:"&pid="; content:"&wvv="; pcre:"/report=d&pid=d&wvv=[A-Za-z0-9]+/"; classtype:trojan-activity; reference:url,www.threatexpert.com/report.aspx?md5=d9bcb4e4d650a6ed4402fab8f9ef1387; reference:url,doc.emergingthreats.net/2010246; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_WindowsEnterpriseFakeAV; sid:2010246; rev:3;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN WindowsEnterpriseSuite FakeAV User-Agent TALWinHttpClient"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| Mozilla/3.0(compatible|3b| TALWinHttpClient)|0d 0a|"; classtype:trojan-activity; reference:url,www.threatexpert.com/report.aspx?md5=d9bcb4e4d650a6ed4402fab8f9ef1387; reference:url,doc.emergingthreats.net/2010261; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_WindowsEnterpriseFakeAV; sid:2010261; rev:3;)

#by evilghost
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN WindowsEnterpriseSuite FakeAV Dynamic User-Agent"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| We"; isdataat:6,relative; content:"|0d 0a|"; distance:0; content:"|User-Agent|3a| Webmin|0d 0a|"; pcre:"/User-Agent: We[a-z0-9]{4}\\x0d\\x0a/"; classtype:trojan-activity; reference:url,www.threatexpert.com/report.aspx?md5=d9bcb4e4d650a6ed4402fab8f9ef1387; reference:url,doc.emergingthreats.net/2010262; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_WindowsEnterpriseFakeAV; sid:2010262; rev:4;)

#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Winspywareprotect.com Fake AV/Anti-Spyware Install Checkin"; flow:established,to_server; uricontent:"/stat.php?func=install&pid="; uricontent:"&ip="; uricontent:"&landing="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008250; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Winspywareprotect.com; sid:2008250; rev:2;)

#by Matt Jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Winspywareprotect.com Fake AV/Anti-Spyware Secondary Checkin"; flow:established,to_server; uricontent:"/stat.php?func=scanfinished&id="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008251; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Winspywareprotect.com; sid:2008251; rev:2;)

#by Chandan at secpod
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN XPantivirus2008 Download"; flow:to_server,established; content:"GET "; depth:4; uricontent:"XPantivirus20"; nocase; pcre:"/XPantivirus20(d|2)_v(d|6)\\.exe/UI/"; classtype:trojan-activity; reference:url,www.theregister.co.uk/2008/08/22/anatomy_of_a_hack/page4.html; reference:url,seo.mhvt.net/blog/?p=390; reference:url,virscan.org/report/a61cd44fc387188da2ee3fbdda10782.html; reference:url,doc.emergingthreats.net/2008516; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_XPantivirus; sid:2008516; rev:3;)

#by Chich Thierry
#
alert tcp $EXTERNAL_NET any -> $HOME_NET 25 (msg:"ET TROJAN XP keylogger v2.1 mail report - Inbound"; flow:established,to_server; content:"X-Mailer|3a| JMail 4.3.0 Free Version by Dimac"; content:"<H2=3EAbout the use of the PC</H2=3E"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2002940; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_XP_Keylogger; sid:2002940; rev:4;)

#by Chich Thierry
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET TROJAN XP keylogger v2.1 mail report - Outbound"; flow:established,to_server; content:"X-Mailer|3a| JMail 4.3.0 Free Version by Dimac"; content:"<H2=3EAbout the use of the PC</H2=3E"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2002942; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_XP_Keylogger; sid:2002942; rev:4;)

#by matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Xorer.ez HTTP Checkin to CnC"; flow:established,to_server; uricontent:"/qq.html?username="; nocase; uricontent:"&zhaoasp="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008081; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Xorer; sid:2008081; rev:2;)

#matt jonkman
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Yahoo550.com Related Downlaoder/Trojan Checkin via HTTP"; flow:established,to_server; uricontent:"/image/logo.jpg?queryid="; pcre:"/queryid=d/U/"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008049; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Yahoo550.com; sid:2008049; rev:2;)

#by Jaime Blasco
#
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN Yoda's Protector Packed Binary - VERY Likely Hostile"; flow:established,from_server; content:"|E8 03 00 00 00 EB 01|"; content:"|BB 55 00 00 00 EB 03 00 00 00 EB 01|"; within:14; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009557; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_Yoda_Protect; sid:2009557; rev:2;)

#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN AdWare.Win32.Yokbar User-Agent Detected (YOK Agent)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| YOK Agent|0d 0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008752; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/TROJAN_YokBar; sid:2008752; rev:3;)

#

```

12/21/2022 11:15:53 AM

```
#by Steven Adair
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Zlob Initial Check-in Version 2 (confirm.php?sid=)"; flow:to_server,established; content:"GET "; nocase; depth:4;
uricontent:".php?sid="; nocase; uricontent:"&sid="; nocase; uricontent:"&mn="; nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008396;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Zlob; sid:2008396; rev:3;)

#By Darren Spruell and dxp
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET VIRUS Zlob User Agent - Likely Zlob (securityinternet)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
securityinternet"; classtype:trojan-activity; reference:url,www.bitdefender.com/VIRUS-1000328-en--Trojan.Pws.Wow.NCY.html; reference:url,doc.emergingthreats.net/2009022;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Zlob; sid:2009022; rev:4;)

#marcus at unsobar
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Zlob post installation checkin (.php?inst_result=&hwid)"; flow:established,to_server; content:"GET "; depth:4;
uricontent:".php?"; uricontent:"inst_result="; uricontent:"&hwid="; pcre:"/\\.php\\?inst_result=\\.+&hwid=\\w+"; classtype:trojan-activity; reference:url,www.threatexpert.com/report.aspx?
md5=1ca43d3f5538fda49c5defb59232f9d; reference:url,doc.emergingthreats.net/2009305; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Zlob; sid:2009305;
rev:2;)

#by Pedro Marinho
#ref 483dbf6dd97ec249b0ec84a358e39260
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Trojan.Zonebac.D"; flow:established,to_server; content:"GET "; depth:4; uricontent:"cid="; nocase;
uricontent:"&aid="; nocase; uricontent:"&time="; nocase; uricontent:"&fw="; nocase; uricontent:"&hora="; nocase; uricontent:"&v="; nocase; uricontent:"&m="; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008682; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Zonebac; sid:2008682; rev:2;)

#Matt Jonkman, caught by robert kerr, re 0853fa768e3e9a3dff293676d68b3d1b
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"ET TROJAN HTTP GET Request on port 53 - Very Likely Hostile"; flow:established,to_server; content:"GET "; nocase; depth:4;
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008420; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_port53http; sid:2008420; rev:3;)

#by marcus at unsobar
#re: 286a378a2eed3559a3e1242a17bfb60a
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN s4t4n1c Trojan Check-in"; flow:established,to_server; content:"POST "; depth:5; uricontent:".php";
content:"continencia="; content:"&versao_kl="; content:"&ydf="; content:"&hora="; content:"&nome_maquina="; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009518;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_s4t4n1c; sid:2009518; rev:2;)

#by Marcus at unsobar.org
#ref: ffab3ed23240e031ad8081b067f89cc7
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN thespybot.com installation download detected"; flow:established,to_server; content:"GET "; depth:4;
uricontent:".php?"; uricontent:"m="; uricontent:"&ydf="; uricontent:"&e="; uricontent:"&m="; uricontent:"&t="; uricontent:"&p="; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008482; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_thespybot.com; sid:2008482; rev:2;)

#by jeremy at sudosecure
#ref 9b00f9947fe29f6a7a6f3bca5f416abd
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN xpsecuritycenter.com Fake AntiVirus GET-Install Checkin"; flow:established,to_server; content:"GET "; depth:4;
uricontent:".php?"; uricontent:"wmid="; nocase; uricontent:"|26|l="; nocase; uricontent:"|26|i="; nocase; uricontent:"|26|s="; nocase; classtype:trojan-activity;
reference:url,www.symantec.com/security_response/writeup.jsp?docid=2008-051910-0118-99&tabid=1; reference:url,doc.emergingthreats.net/2008329; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_xpsecuritycenter.com; sid:2008329; rev:2;)

#Matt Jonkman, info from Bob Grabowsky
#
alert tcp $HOME_NET any -> $EXTERNAL_NET 1345 (msg:"ET WORM AIM Bot Outbound Control Channel Open and Login"; flow: to_server,established; content:"PASS"; nocase; pcre:"/PASS\\s.*?
\\x0d\\x0a\\NICK\\s.*?\\x0d\\x0a\\USER\\s.*?\\s\\d\\s\\d\\s\\:\\S\\im"; classtype: trojan-activity; reference:url,doc.emergingthreats.net/2001910; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/WORM_AIM_Bot; sid:2001910; rev:5;)

#by Matt Jonkman
#
#alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET WORM Allaple ICMP Sweep Ping Outbound"; icode:0; itype:8; content:"Babcdefghijklmnopqrstuvwxyzabcedefghi"; threshold: type both,
count 1, seconds 60, track by_src; classtype:trojan-activity; reference:url,www.sophos.com/virusinfo/analyses/w32allaple.html; reference:url,isc.sans.org/diary.html?storyid=2451;
reference:url,doc.emergingthreats.net/2003292; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WORM_Allaple; sid:2003292; rev:7;)

#by Matt Jonkman
#
#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET WORM Allaple ICMP Sweep Reply Inbound"; icode:0; itype:0; content:"Babcdefghijklmnopqrstuvwxyzabcedefghi"; threshold: type both,
count 1, seconds 60, track by_dst; classtype:trojan-activity; reference:url,www.sophos.com/virusinfo/analyses/w32allaple.html; reference:url,isc.sans.org/diary.html?storyid=2451;
reference:url,doc.emergingthreats.net/2003293; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WORM_Allaple; sid:2003293; rev:9;)

#by Matt Jonkman
#
#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET WORM Allaple ICMP Sweep Ping Inbound"; icode:0; itype:8; content:"Babcdefghijklmnopqrstuvwxyzabcedefghi"; threshold: type both, count
1, seconds 60, track by_src; classtype:trojan-activity; reference:url,www.sophos.com/virusinfo/analyses/w32allaple.html; reference:url,isc.sans.org/diary.html?storyid=2451;
reference:url,doc.emergingthreats.net/2003294; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WORM_Allaple; sid:2003294; rev:6;)

#by Matt Jonkman
#
#alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET WORM Allaple ICMP Sweep Reply Outbound"; icode:0; itype:0; content:"Babcdefghijklmnopqrstuvwxyzabcedefghi"; threshold: type both,
count 1, seconds 60, track by_dst; classtype:trojan-activity; reference:url,www.sophos.com/virusinfo/analyses/w32allaple.html; reference:url,isc.sans.org/diary.html?storyid=2451;
reference:url,doc.emergingthreats.net/2003295; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WORM_Allaple; sid:2003295; rev:8;)

#Matt Jonkman
#
#alert tcp any any -> any $HTTP_PORTS (msg:"ET WORM Allaple Unique HTTP Request - Possibly part of DDOS"; flow:established,to_server; content:"GET / HTTP/1.1|0d 0a|"; rawbytes;
depth:20; threshold:type both, count 1, seconds 60, track by_src; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003484; reference:url,isc.sans.org/diary.html?
storyid=2451; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WORM_Allaple; sid:2003484; rev:8;)

#Bagle variants
#Taken from the Netsquid Rules for Bagle.I and other variants
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET WORM Beagle User Agent Detected"; flow: to_server,established; dsiz<150; content:"|0d 0a|User-Agent|3a| beagle_beagle";
nocase; classtype: trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venr/data/w32.beagle.i@mm.html; reference:url,doc.emergingthreats.net/2001269;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WORM_Bagle_Variants; sid:2001269; rev:15;)

#Bropia Worm
#From Evgeny P
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 6891:6900 (msg:"ET WORM Bropia.F Worm Propagation"; flow: established,to_server; content:"|E1 37 A2 BA 6E 5C 63 8B D6 D1 F7 3C BA 13 16 FD 77
21 5A 5C 17 1B 29 4A 4F 15 A9 29 CF FA 48 3A|"; classtype: misc-attack; reference:url,www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FBROPIA%2EF;
reference:url,doc.emergingthreats.net/2001715; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WORM_Bropia; sid:2001715; rev:8;)

#CIA
#Submitted by Chris Norton
#
#alert ip $HOME_NET any -> $EXTERNAL_NET any (msg:"ET WORM Possible CIA Trojan download/upload attempt"; content:"|6C 75 66 6A 65 6F 6F|"; classtype: trojan-activity;
reference:url,doc.emergingthreats.net/2001233; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WORM_CIA; sid:2001233; rev:8;)

#by Pedro Marinho
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Worm.Win32.Evolm1 Checkin"; flow:established,to_server; content:"GET "; depth:4; uricontent:"/cgi-bin/v.pl|3f 5f|";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008846; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WORM_Evolm1; sid:2008846; rev:2;)

#Korgo Worm
#Submitted by Nick Hatch
#
```

```

#alert tcp $HOME_NET any -> any 445 (msg:"ET WORM Korgo.P offering executable"; flow: to_server,established; content:"|FF|5HB"; depth: 10; content:"|58|http"; content:".exe"; nocase;
within: 36; classtype: trojan-activity; reference:url,www.f-secure.com/v-descs/korgo_p.shtml; reference:url,doc.emergingthreats.net/2001337; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/WORM_KORG0; sid:2001337; rev:7;)

#Korgo Worm
#Submitted by Nick Hatch
#
#alert tcp $HOME_NET any -> any any (msg:"ET WORM Korgo.P binary upload"; flow: to_server,established; content:"|aa4f7ea86c90457d686868f0de687a68689768686868|"; classtype: trojan-
activity; reference:url,www.f-secure.com/v-descs/korgo_p.shtml; reference:url,doc.emergingthreats.net/2001338; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/WORM_KORG0; sid:2001338; rev:8;)

#Matt Jonkman
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET WORM Korgo.U Reporting"; flow: to_server,established; uricontent:"/index.php?id="; nocase; uricontent:"cnt="; nocase;
uricontent:"&scn="; nocase; uricontent:"&inf="; nocase; uricontent:"&ver="; nocase; classtype: trojan-activity; reference:url,www.f-secure.com/v-descs/korgo_u.shtml;
reference:url,doc.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WORM_KORG0; sid:2003070; rev:5;)

#Matt Jonkman, variant using ? rather than &'s
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET WORM Korgo.P Reporting"; flow: to_server,established; uricontent:"/index.php?id="; nocase; uricontent:"?cnt="; nocase;
uricontent:"?scn="; nocase; uricontent:"?inf="; nocase; uricontent:"?ver="; nocase; classtype: trojan-activity; reference:url,www.f-secure.com/v-descs/korgo_p.shtml;
reference:url,doc.emergingthreats.net/2008192; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WORM_KORG0; sid:2008192; rev:2;)

#by Scott Melnick
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET WORM Possible MSN Worm Exploit php"; flow: established; content:"X-MMS-IM-"; depth:153; content:"http"; nocase; content:".php";
nocase; classtype:misc-activity; reference:url,doc.emergingthreats.net/2002322; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WORM_Kelvir; sid:2002322; rev:3;)

#by Scott Melnick
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET WORM Possible MSN Worm Exploit exe"; flow: established; content:"X-MMS-IM-"; depth:153; content:"http"; nocase; content:".exe";
nocase; classtype:misc-activity; reference:url,doc.emergingthreats.net/2002323; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WORM_Kelvir; sid:2002323; rev:3;)

#by Scott Melnick
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET WORM Possible MSN Worm Exploit pif"; flow: established; content:"X-MMS-IM-"; depth:153; content:"http"; nocase; content:".pif";
nocase; classtype:misc-activity; reference:url,doc.emergingthreats.net/2002324; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WORM_Kelvir; sid:2002324; rev:3;)

#Specific Kelvir.HI detection on MSN
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET WORM W32.kelvir.HI"; flow: established; content:"X-MMS-IM-"; depth:153; content:"search.php?data="; classtype:misc-activity;
reference:url,securityresponse.symantec.com/avcenter/venc/data/w32.kelvir.hi.html; reference:url,doc.emergingthreats.net/2002325; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/WORM_Kelvir; sid:2002325; rev:3;)

#MySQL Worm
#Submitted by unknown
#
#alert tcp $HOME_NET any -> !$SQL_SERVERS 3306 (msg:"ET WORM Potential MySQL bot scanning for SQL server"; flags:S,12; classtype: trojan-activity; reference:url,isc.sans.org/diary.php?
date=2005-01-27; reference:url,doc.emergingthreats.net/2001689; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WORM_MySQL; sid:2001689; rev:8;)

#Novarg Worm
#Taken from the Netsquid Rules
#obsoleting
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET WORM Outbound W32.Novarg.A worm"; flow: established; content:"TVqAAWIAAAAAA"; content:"BAALGAAAAAAQ"; within: 20; distance:
2; content:"UEUA..AEuBAW"; content:"DgAABBCwHAABQAAAAE"; within: 40; distance: 16; content:"ABVUFgwAAAAAABgAAAAEAAAAAAAAEA"; content:"ACAAADg"; within: 30; distance: 16; classtype:
trojan-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/w32.mydoom.a@mm.html; reference:url,doc.emergingthreats.net/2001273;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WORM_Novarg; sid:2001273; rev:13;)

#OpaServ Worm
#Submitted by Brad Doctor, 3/8/2005, for Opaserv
#
#alert tcp $HOME_NET any -> $HOME_NET 139 (msg:"ET VIRUS - W32.Opaserv Worm Infection"; flow: established; content:"|5c 73 63 72 73 76 72 2e 65 78 65|"; classtype: misc-activity;
reference:url,www.sarc.com/avcenter/venc/data/w32.opaserv.worm.html; reference:url,doc.emergingthreats.net/2001763; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/WORM_Opaserv; sid:2001763; rev:6;)

#by matt Jonkman, sample submitted anonymously
#I'm putting these sigs in current events because the worm will likely morph quickly making them obsolete.
#If it doesn't we'll move these into a permanent ruleset
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET VIRUS Worm.Pyks HTTP C&C Traffic (User-Agent skw0001)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
skw000"; depth:50; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003588; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WORM_Pyks; sid:2003588;
rev:7;)

#by matt Jonkman, sample submitted anonymously
#I'm putting these sigs in current events because the worm will likely morph quickly making them obsolete.
#If it doesn't we'll move these into a permanent ruleset
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET VIRUS Worm.Pyks HTTP C&C Post Traffic (User-Agent h9tslbw0)"; flow:established,to_server; content:"|0d 0a|User-Agent|3a|
h9tslbw0"; depth:50; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2003589; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WORM_Pyks;
sid:2003589; rev:7;)

#Rbot trojan
#by M Shirk
#
#alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET VIRUS HTTP RBot Challenge/Response Authentication"; flow: to_server,established; content:"Host|3A 20|"; nocase;
content:"|3A 20|Negotiate|20|YIIQegYgKwYBBQCOiIQbjCCEGqghBmI4IQYgOCBAEAQUBQUBQUBQUBQUB"; nocase; classtype: trojan-activity; reference:url,isc.sans.org/diary.php?date=2005-06-03;
reference:url,www.phreedom.org/solar/exploits/msasn1-bitstring; reference:url,doc.emergingthreats.net/2001985; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/WORM_RBOT; sid:2001985; rev:7;)

#by matt jonkman
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET WORM SDBot HTTP Checkin"; flow:established,to_server; content:"|0d 0a|User-Agent|3a| Mozilla/3.0 (compatible|3b| Indy
Library)|0d 0a 0d 0a|quem=dodoi&tit="; content:"&txt="; distance:0; within:40; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007914;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WORM_RBOT; sid:2007914; rev:3;)

#Sasser Worm
#Submitted by Lin Zhong for Sasser variants
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET WORM W32/Sasser.worm.a"; flow: established; content:"|BC 3B 74 0B 50 8B 3D E8 46 A7 3D 09 85 B8 F8 CD 76 40 DE 7C 5B 5C D7 2A AB
E8 58 75 62 96 25 24|"; classtype: misc-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/w32.sasser.worm.html; reference:url,doc.emergingthreats.net/2001057;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WORM_Sasser; sid:2001057; rev:7;)

#Sasser Worm
#Submitted by Lin Zhong for Sasser variants
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET WORM W32/Sasser.worm.b"; flow: established; content:"|58 BC 0C FF 59 57 32 31 BD EC 34 64 6E D6 E3 8D 65 04 68 58 62 79 DF D8 2C
25 6A B5 28 BA 13 74|"; classtype: misc-activity; reference:url,securityresponse.symantec.com/avcenter/venc/data/w32.sasser.worm.html; reference:url,doc.emergingthreats.net/2001056;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WORM_Sasser; sid:2001056; rev:7;)

#Sasser Worm
#Submitted by Lin Zhong for Sasser variants
#
#alert tcp any any -> any 5554 (msg:"ET WORM Sasser FTP Traffic"; flow: to_server,established; content:"up.exe"; classtype: misc-activity;
reference:url,vil.mcafee.com/vil/content/Print125009.htm; reference:url,doc.emergingthreats.net/2000040; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/WORM_Sasser; sid:2000040; rev:5;)

```

```

#Sasser Worm
#Submitted by Lin Zhong for Sasser variants
#
#alert tcp any any -> any 9996 (msg:"ET WORM Sasser Transfer _up.exe"; flow: established,to_server; content:"|5F75702E657865|"; depth: 250; classtype: misc-activity;
reference:url,vil.mcafeesecurity.com/vil/content/Print125009.htm; reference:url,doc.emergingthreats.net/2000047; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/VIRUS/WORM_Sasser; sid:2000047; rev:5;)

#Submitted by Joe Stewart for Sasser FTP exploit
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 5554 (msg:"ET WORM Sasser FTP exploit attempt"; flow: to_server,established; dsize: >150; content:"PORT "; depth: 5; classtype: attempted-
admin; reference:url,www.lurhq.com/dabber.html; reference:url,doc.emergingthreats.net/2001548; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/WORM_Sasser;
sid:2001548; rev:6;)

#from the SecureCIRT Team
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 1863 (msg:"ET WORM Singworm MSN message Outbound"; flow:established; content:"Here are the new smiles for MSN, they are incredible!";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007605; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/WORM_Singworm; sid:2007605; rev:3;)

#from the SecureCIRT Team
#
##alert tcp $EXTERNAL_NET 1863 -> $HOME_NET any (msg:"ET DELETED Singworm MSN message Inbound"; flow:established; content:"Here are the new smiles for MSN, they are incredible!";
classtype:trojan-activity; reference:url,doc.emergingthreats.net/2007606; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/WORM_Singworm; sid:2007606; rev:3;)

#by matt jonkman. Win32.Socks.s
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET WORM Win32.Socks.s HTTP Post Checkin"; flow:established,to_server; content:"POST "; depth:5; uricontent:".php";
content:"|0d 0a 0d 0a|proc=[System Process]|0a|"; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2008020; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/VIRUS/WORM_Socks; sid:2008020; rev:3;)

#Suspicious Extensions
#Snort.org rule 721 scaled back a bit by Matt Jonkman to not hit on xls, vcf, ppt, rtf, dot, or pdf.
#If you use this rule disable 721 in the snort sets. This rule will hit on the following:
#ade, adp, asd, asf, asx, bat, bas, chm, cli, cmd, com, crt, cpl, cpp, diz, dll, ebs, emf, eml, exe, fol, folder, hlp, hsq, hta, ini, inf, ins,
#isp, js, jse, lnk, mda, mdb, mde, mdw, mdt, mht, mht, msi, msc, msg, mst, mst, nws, ocx, pcd, pif, pl, pls, plc,plx, pm, pot, rar,
#reg, scr, sct, shs, svf, sys, url, vb, vbe, vbs, vxd, wmd, wmf, wms, wnz, wpm, wps, wpz, wsc, wsf, wsh, xlt, xlw, zip
#
#alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"ET VIRUS OUTBOUND Suspicious Email Attachment"; flow: to_server,established; content:"Content-Disposition|3A|"; nocase;
content:"filename="; distance:0; pcre:"/^\\s*=\\s*\\.?(?=([abcdehijlmnoprsvwxyz])(a[d[ep]]s[x])|c[rt][ho]m|li|pl|md|pp)|d(iz|ll)|e(m[f1]|xe|bs)|h(ip|sq|ta)|jse?
|md|abzew)|s[tcgip]|html|ht)|p(cd|if|l|xsc)|lml|ot)|r(eg|ar)|s(cr|ct)|h(y)s|w|v(b[es]?|xd)|w(m|dfsz)|p(msz)|s(cf|h)|xl|tw)|folder|fol|ba|st)|i(sp|n|sif)|lnk|nws|ocx|zip|url)
|\\x27|\\x22|\\n|\\s|'iR"; classtype: suspicious-filename-detect; reference:url,doc.emergingthreats.net/2000562; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/VIRUS/WORM_Suspicious_Extensions; sid:2000562; rev:12;)

#Submitted by Joseph Gama
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET WORM UPX compressed file download - possible worm"; 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; content:"UPX0"; content:"UPX1"; content:"UPX!"; classtype: misc-activity;
reference:url,doc.emergingthreats.net/2001046; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/WORM_Suspicious_Extensions; sid:2001046; rev:7;)

#Submitted by Joseph Gama
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET WORM UPX encrypted file download - possible worm"; 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; content:"|00|code|00|"; content:"|00 C0|text|00|"; classtype: misc-activity;
reference:url,doc.emergingthreats.net/2001047; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/WORM_Suspicious_Extensions; sid:2001047; rev:6;)

#from Jack Pepper
#Disabling, tends to false
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WORM shell bot perl code download"; flow:to_client,established; content:"# ShellBOT"; nocase; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2002683; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/WORM_Web_Bots; sid:2002683; rev:5;)

#from Jack Pepper
#Disabling, tends to false
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WORM Shell Bot Code Download"; flow:to_client,established; content:"##### IRC #####";
nocase; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2002684; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VIRUS/WORM_Web_Bots; sid:2002684; rev:4;)

#by Blake Hartstein
#
#alert udp $EXTERNAL_NET any -> $HOME_NET 5060 (msg:"ET VOIP Asterisk Register with no URI or Version DOS Attempt"; content:"REGISTER|0d 0a|"; nocase; depth:10; content:"SIP/";
distance:0; classtype: attempted-dos; reference:url,labs.musecurity.com/advisories/HU-200703-01.txt; reference:url,tools.ietf.org/html/rfc3261;
reference:url,doc.emergingthreats.net/2003474; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VOIP/VOIP_Asterisk_DOS; sid:2003474; rev:6;)

#These sigs are adapted from those at nextsoft.cz
#this set are for general SIP specific flooding
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 5060 (msg:"ET VOIP INVITE Message Flood TCP"; flow:established,to_server; content:"INVITE"; depth:6; threshold: type both , track by_src, count
100, seconds 60; classtype:attempted-dos; reference:url,doc.emergingthreats.net/2003192; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VOIP/VOIP_Flooding; sid:2003192;
rev:4;)

#These sigs are adapted from those at nextsoft.cz
#this set are for general SIP specific flooding
#
#alert udp $EXTERNAL_NET any -> $HOME_NET 5060 (msg:"ET VOIP INVITE Message Flood UDP"; content:"INVITE"; depth:6; threshold: type both , track by_src, count 100, seconds 60;
classtype:attempted-dos; reference:url,doc.emergingthreats.net/2009698; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VOIP/VOIP_Flooding; sid:2009698; rev:1;)

#These sigs are adapted from those at nextsoft.cz
#this set are for general SIP specific flooding
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 5060 (msg:"ET VOIP REGISTER Message Flood TCP"; flow:established,to_server; content:"REGISTER"; depth:8; threshold: type both , track by_src,
count 100, seconds 60; classtype:attempted-dos; reference:url,doc.emergingthreats.net/2003193; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VOIP/VOIP_Flooding;
sid:2003193; rev:5;)

#These sigs are adapted from those at nextsoft.cz
#this set are for general SIP specific flooding
#
#alert udp $EXTERNAL_NET any -> $HOME_NET 5060 (msg:"ET VOIP REGISTER Message Flood UDP"; content:"REGISTER"; depth:8; threshold: type both , track by_src, count 100, seconds 60;
classtype:attempted-dos; reference:url,doc.emergingthreats.net/2009699; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VOIP/VOIP_Flooding; sid:2009699; rev:1;)

#By Shirkdog and Blake Hartstein
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET VOIP Centrality IP Phone (PA-168 Chipset) Session Hijacking"; flow:established,to_server; content:"POST "; nocase; depth:5;
uricontent:"/g"; nocase; content:"back++Back++"; nocase; pcre:"/^\\$([#])|U/"; classtype:attempted-user; reference:url,www.milw0rm.com/exploits/3189;
reference:url,doc.emergingthreats.net/bin/view/Main/2003329; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VOIP/VOIP_IP_Phone; reference:cve,2007-0528; sid:2003329;
rev:5;)

#by Blake Hartstein of Demarc
#
#alert udp $EXTERNAL_NET any -> $HOME_NET 5060 (msg:"ET VOIP SIP UDP Softphone INVITE overflow"; dsize:>1000; content:"INVITE"; depth:6; nocase; pcre:"/r?\\n?\\n/R";
isdataat:1000,relative; classtype:attempted-user; reference:bugtraq,16213; reference:cve,2006-0189; reference:url,doc.emergingthreats.net/bin/view/Main/2002848;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/EXPLOIT/EXPLOIT_SIP; sid:2002848; rev:7;)

#by Blake Hartstein of Demarc
#
#alert udp $EXTERNAL_NET any -> $HOME_NET 5060 (msg:"ET VOIP MultiTech SIP UDP Overflow"; content:"INVITE"; nocase; depth:6; isdataat:65,relative; content:"|0a|"; within:61;
classtype:attempted-user; reference:cve,2005-4050; reference:url,doc.emergingthreats.net/2003237; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/VOIP/VOIP_Multitech;
sid:2003237; rev:8;)

```

```

#by Kevin Ross
#
alert udp $EXTERNAL_NET any -> $HOME_NET 5060 (msg:"ET SCAN SIP erase_registrations/add_registrations attempt"; content:"REGISTER "; depth:9; content:"User-Agent|3a| Hacker";
classtype:attempted-recon; reference:url,www.hackingvoip.com/sec_tools.html; reference:url,doc.emergingthreats.net/2008640; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VOIP/VOIP_SIP_erase; sid:2008640; rev:5;)

#by Kevin Ross
#
alert udp $EXTERNAL_NET any -> $HOME_NET 5060 (msg:"ET SCAN sipscan probe"; content:"sip|3a|thisisthecanary@"; content:"sip|3a|test@"; offset:30; distance:70; classtype:attempted-recon;
reference:url,www.hackingvoip.com/sec_tools.html; reference:url,doc.emergingthreats.net/2008641; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VOIP/VOIP_SIPscan;
sid:2008641; rev:3;)

#from the rules at nextsoft.cz
#intended to catch unusual numbers of unauthorized responses from sip servers
#
alert tcp $HOME_NET 5060 -> $EXTERNAL_NET any (msg:"ET VOIP Multiple Unauthorized SIP Responses TCP"; flow:established,from_server; content:"SIP/2.0 401 Unauthorized"; depth:24;
threshold: type both, track by_src, count 5, seconds 360; classtype:attempted-dos; reference:url,doc.emergingthreats.net/2003194; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VOIP/VOIP_Unauth; sid:2003194; rev:6;)

#from the rules at nextsoft.cz
#intended to catch unusual numbers of unauthorized responses from sip servers
#
alert udp $HOME_NET 5060 -> $EXTERNAL_NET any (msg:"ET VOIP Multiple Unauthorized SIP Responses UDP"; content:"SIP/2.0 401 Unauthorized"; depth:24; threshold: type both, track by_src,
count 5, seconds 360; classtype:attempted-dos; reference:url,doc.emergingthreats.net/2009700; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VOIP/VOIP_Unauth;
sid:2009700; rev:1;)

#by Akash Mahajan of Stillsecure
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX 4XEM VatDecoder VatCtrl Class ActiveX Control Url Property Buffer Overflow Vulnerability";
flow:to_client,established; content:"21000C8C-8B17-48D1-8294-1A338DD2EB3A"; nocase; content:"0x40000"; content:"Url"; nocase; classtype:web-application-attack; reference:bugtraq,28010;
reference:url,www.milw0rm.com/exploits/5193; reference:url,doc.emergingthreats.net/2007903; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_4XEM;
sid:2007903; rev:8;)

#by stillsecure
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX AOL Radio AmpX ActiveX Control ConvertFile Method Buffer Overflow"; flow:to_client,established; content:"FE0BD779-
44EE-4A48-AA2E-743C63F2E5E6"; nocase; content:"ConvertFile"; nocase; classtype:web-application-attack; reference:url,milw0rm.com/exploits/8733; reference:bugtraq,35028;
reference:url,doc.emergingthreats.net/2009469; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_AOL; sid:2009469; rev:10;)

#by kevin ross
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Possible AOL SuperBuddy ActiveX Control Remote Code Execution Attempt"; flow:from_server,established;
content:"18950488-50D1-4A48-B4D6-95C8F58A6414"; nocase; content:"SetSuperBuddy"; nocase; content:"//"; pcre:"/<OBJECT\s+[>]*classid\s*=\s*[\x22\x27]?\\s*clsid\s*\x3a\s*\x7b?\\s*18950488-
50D1-4A48-B4D6-95C8F58A6414/si"; classtype:attempted-user; reference:url,www.securityfocus.com/bid/36580/info; reference:url,www.securityfocus.com/archive/1/506889;
reference:url,doc.emergingthreats.net/2010039; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_AOL; sid:2010039; rev:4;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Possible AOL IWinAmp ActiveX ConvertFile Buffer Overflow Attempt"; flow:from_server,established;
content:"FE0BD779-44EE-4A48-AA2E-743C63F2E5E6"; nocase; content:"ConvertFile"; nocase; pcre:"/<OBJECT\s+[>]*classid\s*=\s*[\x22\x27]?\\s*clsid\s*\x3a\s*\x7b?\\s*FE0BD779-44EE-4A48-AA2E-
743C63F2E5E6/si"; classtype:attempted-user; reference:url,www.milw0rm.org/exploits/8733; reference:url,www.securityfocus.com/bid/35028; reference:url,doc.emergingthreats.net/2010160;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_AOL; sid:2010160; rev:6;)

#by Kevin Ross
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Possible AOL 9.5 BindToFile Heap Overflow Attempt"; flow:established,to_client; content:"BC8A96C6-3909-11D5-9001-
00C04F4C3B9F"; nocase; content:"BindToFile"; nocase; pcre:"/<OBJECT\s+[>]*classid\s*=\s*[\x22\x27]?\\s*clsid\s*\x3a\s*\x7b?\\s*BC8A96C6-3909-11D5-9001-00C04F4C3B9F/si";
classtype:attempted-user; reference:url,tc.hellcode.net/advisories/hellcode-adv008.txt; reference:url,doc.emergingthreats.net/2010814; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_AOL; sid:2010814; rev:4;)

#by kevin ross
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX AOL 9.5 Phobos.Playlist Import ActiveX Buffer Overflow Attempt"; flow:established,to_client; content:"A1058D70-
BF56-4D10-BC91-41C88321F47C"; nocase; content:".Import"; nocase; pcre:"/<OBJECT\s+[>]*classid\s*=\s*[\x22\x27]?\\s*clsid\s*\x3a\s*\x7b?\\s*A1058D70-BF56-4D10-BC91-41C88321F47C/si";
classtype:attempted-user; reference:url,www.rec-sec.com/2010/01/25/aol-playlist-class-buffer-overflow; reference:url,doc.emergingthreats.net/2010962;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_AOL; sid:2010962; rev:5;)

#by Kevin Ross
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Possible Acer LunchApp Arbitrary Code Exucution Attempt"; flow:established,from_server; content:"3895DD35-7573-
11D2-8FED-00606730D3AA"; nocase; content:".RUN"; nocase; distance:0; pcre:"/<OBJECT\s+[>]*classid\s*=\s*[\x22\x27]?\\s*clsid\s*\x3a\s*\x7b?\\s*3895DD35-7573-11D2-8FED-00606730D3AA/si";
classtype:attempted-user; reference:url,securitytracker.com/alerts/2009/Aug/1022752.html; reference:url,www.kb.cert.org/vuls/id/485961;
reference:url,www.securityfocus.com/bid/21207/info; reference:url,doc.emergingthreats.net/2009868; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Acer;
sid:2009868; rev:9;)

#by stillsecure
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Adobe Shockwave Player ActiveX Control Buffer Overflow clsid access"; flow:established,to_client;
content:"233C1507-6A77-46A4-9443-F871F945D258"; nocase; content:"PlayerVersion"; nocase; pcre:"/<OBJECT\s+[>]*classid\s*=\s*[\x22\x27]?\\s*clsid\s*\x3a\s*\x7b?\\s*233C1507-6A77-46A4-
9443-F871F945D258/si"; classtype:web-application-attack; reference:url,www.milw0rm.com/exploits/9682; reference:url,doc.emergingthreats.net/2010256;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Adobe; sid:2010256; rev:5;)

#by eion miller
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT PDF Containing Windows Commands Downloaded"; flow:established,to_client; content:"%PDF-"; content:"|3C 3C 0D 0A
20 2f|type|20 2f|action|0D 0A 20 2f|s|20 2f|launch|0D 0A 20 2f|win"; distance:0; nocase; classtype:bad-unknown; reference:url,doc.emergingthreats.net/2011245;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Adobe; sid:2011245; rev:2;)

#by evilghost
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT Likely Malicious PDF Containing StrReverse"; flow:established,to_client; content:"HTTP/1"; depth:7;
content:"%PDF-"; content:"StrReverse|28|"; distance:0; nocase; classtype:bad-unknown; reference:url,doc.emergingthreats.net/2011246; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Adobe; sid:2011246; rev:2;)

#by Wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Akamai Download Manager Stack Buffer Overflow CLSID Access 1"; flow:to_client,established; content:"4871A87A-BFDD-
4106-8153-FFDE28AC2967"; nocase; pcre:"/<OBJECT\s+[>]*classid\s*=\s*[\x22\x27]?\\s*clsid\s*\x3a\s*\x7b?\\s*4871A87A-BFDD-4106-8153-FFDE28AC2967/si"; classtype:web-application-attack;
reference:url,labs.iddefense.com/intelligence/vulnerabilities/display.php?id=813; reference:url,doc.emergingthreats.net/2009687; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Akamai; sid:2009687; rev:8;)

#by Wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Akamai Download Manager Stack Buffer Overflow CLSID Access 2"; flow:to_client,established; content:"2AF5BD25-
90C5-4EEC-88C5-B44DC298508B"; nocase; pcre:"/<OBJECT\s+[>]*classid\s*=\s*[\x22\x27]?\\s*clsid\s*\x3a\s*\x7b?\\s*2AF5BD25-90C5-4EEC-88C5-B44DC298508B/si"; classtype:web-application-
attack; reference:url,labs.iddefense.com/intelligence/vulnerabilities/display.php?id=813; reference:url,doc.emergingthreats.net/2009688; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Akamai; sid:2009688; rev:7;)

#by Wolvee
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Akamai Download Manager Stack Buffer Overflow CLSID Access 3"; flow:to_client,established; content:"FFB83F3B-
0A5A-4106-8E53-DFE1E2340C81"; nocase; pcre:"/<OBJECT\s+[>]*classid\s*=\s*[\x22\x27]?\\s*clsid\s*\x3a\s*\x7b?\\s*FFB83F3B-0A5A-4106-8E53-DFE1E2340C81/si"; classtype:web-application-
attack; reference:url,labs.iddefense.com/intelligence/vulnerabilities/display.php?id=813; reference:url,doc.emergingthreats.net/2009689; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Akamai; sid:2009689; rev:8;)

#by kevin ross
#

```

12/21/2022 11:15:53 AM

```
#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Avax Vector avPreview.ocx ActiveX Control Buffer Overflow"; flow:to_client,established; content:"9589AEC9-1C2D-4428-B7E8-63B39D356F9C"; nocase; content:"PrinterName"; nocase; classtype:web-application-attack; reference:url,packetstormsecurity.nl/0907-exploits/avax13-dos.txt; reference:bugtraq,35582; reference:url,juniper.net/security/auto/vulnerabilities/vuln35583.html; reference:url,doc.emergingthreats.net/2009792; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Avax; sid:2009792; rev:7;)

#by stillsecure
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Awingsoft Web3D Player Remote Buffer Overflow"; flow:to_client,established; content:"17A54E7D-A9D4-11D8-9552-00E04CBF9903"; nocase; content:"SceneURL"; nocase; classtype:web-application-attack; reference:url,secunia.com/advisories/35764/; reference:url,milw0rm.com/exploits/9116; reference:url,shinnai.net/xp1its/TXT_ns0uDeley3EHfKEV690p.html; reference:url,doc.emergingthreats.net/2009857; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Awingsoft; sid:2009857; rev:6;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Baofeng Storm ActiveX Control OnBeforeVideoDownload Method Buffer Overflow"; flow:to_client,established; content:"68E52E1D-E586-474F-A6E2-1A85A9B4D9FB"; nocase; content:"OnBeforeVideoDownload"; nocase; classtype:web-application-attack; reference:bugtraq,34789; reference:url,milw0rm.com/exploits/8579; reference:url,doc.emergingthreats.net/2009425; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Baofeng; sid:2009425; rev:9;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Baofeng Storm ActiveX Control SetAttributeValue Method Buffer Overflow"; flow:to_client,established; content:"BD103B2B-30FB-4F1E-8C17-D8F6A0B0C73E5"; nocase; content:"SetAttributeValue"; nocase; classtype:web-application-attack; reference:bugtraq,34869; reference:url,juniper.net/security/auto/vulnerabilities/vuln34869.html; reference:url,vupen.com/english/advisories/2009/1392; reference:url,milw0rm.com/exploits/8757; reference:url,doc.emergingthreats.net/2009657; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Baofeng; sid:2009657; rev:7;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Baofeng Storm mps.dll ActiveX OnBeforeVideoDownload Buffer Overflow Function Call"; flow:to_client,established; content:"ActiveXObject"; nocase; content:"HPS.StormPlayer.1"; nocase; distance:0; content:"OnBeforeVideoDownload"; nocase; classtype:attempted-user; reference:bugtraq,34789; reference:url,doc.emergingthreats.net/2010995; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Baofeng; sid:2010995; rev:3;)

#by kevin ross
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Possible Black Ice Printer Driver Resource Toolkit ActiveX Control EnableStartApplication/EnableStartBeforePrint/EnableKeepExistingFiles/EnablePassParameters Buffer Overflow Attempt"; flow:from_server,established; content:"1503569A-0AE2-4333-B6E6-466A0B0C73E5"; nocase; content:"Enable"; nocase; pcre:"/<OBJECT\s+[^\s]*classid\s*=\s*[\x22\x27]?[\s]*classid\s*=\s*\x3a\s*\x7B?\s*1503569A-0AE2-4333-B6E6-466A0B0C73E5\s*" (EnableKeepExistingFiles|EnableStartApplication|EnableStartBeforePrint|EnablePassParameters)/si"; classtype:attempted-user; reference:url,www.securityfocus.com/bid/36548; reference:url,doc.emergingthreats.net/2010203; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_BlackIce; sid:2010203; rev:5;)

#by kevin ross
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Possible Black Ice Printer Driver Resource Toolkit ActiveX Control SetApplicationPath/SetStartApplicationParamCode/SetCustomStartAppParameter Buffer Overflow Attempt"; flow:from_server,established; content:"1503569A-0AE2-4333-B6E6-466A0B0C73E5"; nocase; content:"Set"; nocase; pcre:"/<OBJECT\s+[^\s]*classid\s*=\s*[\x22\x27]?[\s]*classid\s*=\s*\x3a\s*\x7B?\s*1503569A-0AE2-4333-B6E6-466A0B0C73E5\s*" (SetApplicationPath|SetStartApplicationParamCode|SetCustomStartAppParameter)/si"; classtype:attempted-user; reference:url,www.securityfocus.com/bid/36548; reference:url,doc.emergingthreats.net/2010204; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_BlackIce; sid:2010204; rev:5;)

#by kevin ross
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Possible Black Ice Printer Driver Resource Toolkit ActiveX Control SaveBlackIceDEVMODE Buffer Overflow Attempt"; flow:from_server,established; content:"1503569A-0AE2-4333-B6E6-466A0B0C73E5"; nocase; content:"SaveBlackIceDEVMODE"; nocase; pcre:"/<OBJECT\s+[^\s]*classid\s*=\s*[\x22\x27]?[\s]*classid\s*=\s*\x3a\s*\x7B?\s*1503569A-0AE2-4333-B6E6-466A0B0C73E5/si"; classtype:attempted-user; reference:url,www.securityfocus.com/bid/36548; reference:url,doc.emergingthreats.net/2010205; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_BlackIce; sid:2010205; rev:6;)

#by kevin ross
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Possible Black Ice Printer Driver Resource Toolkit ActiveX Control ClearUserSettings Buffer Overflow Attempt"; flow:from_server,established; content:"1503569A-0AE2-4333-B6E6-466A0B0C73E5"; nocase; content:"ClearUserSettings"; nocase; pcre:"/<OBJECT\s+[^\s]*classid\s*=\s*[\x22\x27]?[\s]*classid\s*=\s*\x3a\s*\x7B?\s*1503569A-0AE2-4333-B6E6-466A0B0C73E5/si"; classtype:attempted-user; reference:url,www.securityfocus.com/bid/36548; reference:url,doc.emergingthreats.net/2010206; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_BlackIce; sid:2010206; rev:5;)

#by kevin ross
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Possible Black Ice Printer Driver Resource Toolkit ActiveX Control ControlJob Buffer Overflow Attempt"; flow:from_server,established; content:"1503569A-0AE2-4333-B6E6-466A0B0C73E5"; nocase; content:"ControlJob"; nocase; pcre:"/<OBJECT\s+[^\s]*classid\s*=\s*[\x22\x27]?[\s]*classid\s*=\s*\x3a\s*\x7B?\s*1503569A-0AE2-4333-B6E6-466A0B0C73E5/si"; classtype:attempted-user; reference:url,www.securityfocus.com/bid/36548; reference:url,doc.emergingthreats.net/2010207; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_BlackIce; sid:2010207; rev:5;)

#by kevin ross
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Possible Black Ice Printer Driver Resource Toolkit ActiveX Control EnableStartApplication/EnableStartBeforePrint/EnableKeepExistingFiles/EnablePassParameters Function Call Attempt"; flow:to_client,established; content:"ActiveXObject"; nocase; content:"BlackIceDEVMODECtrl.1"; nocase; distance:0; pcre:"/(EnableStartApplication|EnableStartBeforePrint|EnableKeepExistingFiles|EnablePassParameters)/i"; classtype:attempted-user; reference:url,www.securityfocus.com/bid/36548; reference:url,doc.emergingthreats.net/2010208; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_BlackIce; sid:2010208; rev:3;)

#by kevin ross
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Possible Black Ice Printer Driver Resource Toolkit ActiveX Control SetApplicationPath/SetStartApplicationParamCode/SetCustomStartAppParameter Function Call Attempt"; flow:to_client,established; content:"ActiveXObject"; nocase; content:"BlackIceDEVMODECtrl.1"; nocase; distance:0; pcre:"/(SetApplicationPath|SetStartApplicationParamCode|SetCustomStartAppParameter)/i"; classtype:attempted-user; reference:url,www.securityfocus.com/bid/36548; reference:url,doc.emergingthreats.net/2010209; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_BlackIce; sid:2010209; rev:3;)

#by kevin ross
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Possible Black Ice Printer Driver Resource Toolkit ActiveX Control SaveBlackIceDEVMODE Function Call Attempt"; flow:to_client,established; content:"ActiveXObject"; nocase; content:"BlackIceDEVMODECtrl.1"; nocase; distance:0; content:"SaveBlackIceDEVMODE"; nocase; classtype:attempted-user; reference:url,www.securityfocus.com/bid/36548; reference:url,doc.emergingthreats.net/2010210; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_BlackIce; sid:2010210; rev:3;)

#by kevin ross
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Possible Black Ice Printer Driver Resource Toolkit ActiveX Control ClearUserSettings Function Call Attempt"; flow:to_client,established; content:"ActiveXObject"; nocase; content:"BlackIceDEVMODECtrl.1"; nocase; distance:0; content:"ClearUserSettings"; nocase; classtype:attempted-user; reference:url,www.securityfocus.com/bid/36548; reference:url,doc.emergingthreats.net/2010211; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_BlackIce; sid:2010211; rev:3;)

#by kevin ross
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Possible Black Ice Printer Driver Resource Toolkit ActiveX Control ControlJob Function Call Attempt"; flow:to_client,established; content:"ActiveXObject"; nocase; content:"BlackIceDEVMODECtrl.1"; nocase; distance:0; content:"ControlJob"; nocase; classtype:attempted-user; reference:url,www.securityfocus.com/bid/36548; reference:url,doc.emergingthreats.net/2010212; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_BlackIce; sid:2010212; rev:3;)

#by stillsecure
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET WEB_SPECIFIC_APPS Campsite article_id Parameter SELECT FROM SQL Injection Attempt"; flow:established,to_server; content:"GET "; depth:4; uricontent:"/plugins/campsiteattachment/attachments.php?"; nocase; uricontent:"article_id="; nocase; uricontent:"SELECT"; nocase; uricontent:"FROM"; nocase; pcre:"/SELECT.+FROM/ui"; classtype:web-application-attack; reference:url,secunia.com/advisories/39580/; reference:url,doc.emergingthreats.net/2011215; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Campsite; sid:2011215; rev:2;)

#by stillsecure
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET WEB_SPECIFIC_APPS Campsite article_id Parameter DELETE FROM SQL Injection Attempt"; flow:established,to_server;
```

```

content:"GET "; depth:4; uricontent:"/plugins/campsiteattachment/attachments.php?"; nocase; uricontent:"article_id="; nocase; uricontent:"DELETE"; nocase; uricontent:"FROM"; nocase;
pcrcr:"/DELETE.+FROM/Ui"; classtype:web-application-attack; reference:url,secunia.com/advisories/39580; reference:url,doc.emergingthreats.net/2011216;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_Campsite; sid:2011216; rev:2;)

#by stillsecure
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET WEB_SPECIFIC_APPS Campsite article_id Parameter UNION SELECT SQL Injection Attempt"; flow:established,to_server;
content:"GET "; depth:4; uricontent:"/plugins/campsiteattachment/attachments.php?"; nocase; uricontent:"article_id="; nocase; uricontent:"UNION"; nocase; uricontent:"SELECT"; nocase;
pcrcr:"/UNION.+SELECT/Ui"; classtype:web-application-attack; reference:url,secunia.com/advisories/39580; reference:url,doc.emergingthreats.net/2011217;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_Campsite; sid:2011217; rev:2;)

#by stillsecure
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET WEB_SPECIFIC_APPS Campsite article_id Parameter INSERT INTO SQL Injection Attempt"; flow:established,to_server;
content:"GET "; depth:4; uricontent:"/plugins/campsiteattachment/attachments.php?"; nocase; uricontent:"article_id="; nocase; uricontent:"INSERT"; nocase; uricontent:"INTO"; nocase;
pcrcr:"/INSERT.+INTO/Ui"; classtype:web-application-attack; reference:url,secunia.com/advisories/39580; reference:url,doc.emergingthreats.net/2011218;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_Campsite; sid:2011218; rev:2;)

#by stillsecure
#
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET WEB_SPECIFIC_APPS Campsite article_id Parameter UPDATE SET SQL Injection Attempt"; flow:established,to_server;
content:"GET "; depth:4; uricontent:"/plugins/campsiteattachment/attachments.php?"; nocase; uricontent:"article_id="; nocase; uricontent:"UPDATE"; nocase; uricontent:"SET"; nocase;
pcrcr:"/UPDATE.+SET/Ui"; classtype:web-application-attack; reference:url,secunia.com/advisories/39580; reference:url,doc.emergingthreats.net/2011219;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_Campsite; sid:2011219; rev:2;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Charm Real Converter pro 6.6 Activex Control DOS clsid access attempt"; flow:established,to_client;
content:"F4F647AD-B160-11D2-A3EF-00104BD4755"; nocase; content:"GetCodeModule"; nocase; pcrcr:"/<OBJECT s[^>]*classid s*=s*[\x22\x27]?s*classid s*\x3a\s*\x7b?s*F4F647AD-B160-11D2-
A3EF-00104BD4755/si"; classtype:web-application-attack; reference:url,secunia.com/advisories/39580; reference:url,doc.emergingthreats.net/2010280;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_CharmReal; sid:2010280; rev:5;)

#by Chandon S at Stillsecure
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX ChilkatHttp ActiveX 2.3 Arbitrary Files Overwrite"; flow:to_client,established; content:"B973393F-27C7-4781-877D-
8626AAEDF119"; nocase; pcrcr:"/.\.(ini|exe|dll|bat|com|cab|txt)/R1"; content:"SaveLastError"; nocase; classtype:web-application-attack; reference:bugtraq,28546;
reference:url,www.milw0rm.com/exploits/5338; reference:url,doc.emergingthreats.net/2008099; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_Chilkat;
sid:2008099; rev:7;)

#by Stillsecure
#
##alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ACTIVEX Chilkat IMAP ActiveX File Execution and IE DoS"; flow:to_client,established; content:"126FB030-1E9E-4517-A254-
430616582C50"; nocase; content:"LoadXmlEmail"; nocase; classtype:web-application-attack; reference:url,www.milw0rm.com/exploits/6600; reference:url,doc.emergingthreats.net/2008607;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_Chilkat; sid:2008607; rev:9;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Chilkat Crypt ActiveX Component WriteFile Insecure Method"; flow:to_client,established; content:"335285B9-82E8-
4FDF-9EB1-1A3E60056904"; nocase; content:"WriteFile"; nocase; classtype:web-application-attack; reference:url,secunia.com/advisories/32513; reference:url,milw0rm.com/exploits/6963;
reference:url,doc.emergingthreats.net/2008814; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_Chilkat; sid:2008814; rev:8;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Chilkat Socket ACTIVEX Remote Arbitrary File Creation"; flow:to_client,established; content:"474FCCCD-1B89-4D34-
9E09-45807F23289C"; nocase; content:"SaveLastError"; nocase; classtype:web-application-attack; reference:bugtraq,32333; reference:url,milw0rm.com/exploits/7142;
reference:url,doc.emergingthreats.net/2008870; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_Chilkat; sid:2008870; rev:9;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Chilkat Socket Activex Remote Arbitrary File Overwrite 1"; flow:to_client,established; content:"3B598BD0-AF50-
48C6-B6A5-63261A48B054"; nocase; content:"SaveLastError"; nocase; classtype:web-application-attack; reference:bugtraq,32333; reference:url,milw0rm.com/exploits/7594;
reference:url,doc.emergingthreats.net/2009046; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_Chilkat; sid:2009046; rev:50;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Chinagames ActiveX Control CreateChinagames Method Buffer Overflow"; flow:to_client,established;
content:"75108829-202F-493C-86C5-1C182A485C4C"; nocase; content:"CreateChinagames"; nocase; classtype:web-application-attack; reference:bugtraq,34871;
reference:url,milw0rm.com/exploits/8758; reference:url,doc.emergingthreats.net/2009500; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_Chinagames;
sid:2009500; rev:7;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Ciansoft PDFBuilderX Control ActiveX Arbitrary File Overwrite"; flow:to_client,established; content:"00E7C7F8-
71E2-498A-AB28-A3D72FC74405"; nocase; content:"SaveToFile"; nocase; classtype:web-application-attack; reference:bugtraq,32333; reference:url,milw0rm.com/exploits/7794;
reference:url,doc.emergingthreats.net/2009064; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_Ciansoft; sid:2009064; rev:7;)

#by Akash Mahajan of Stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Citrix Presentation Server Client WFICA.OCX ActiveX Component Heap Buffer Overflow Exploit";
flow:established,to_client; content:"0x40000"; content:"SendChannelData"; nocase; content:"238F6F83-B8B4-11CF-8771-00A024541EE3"; nocase; classtype:web-application-attack;
reference:url,www.milw0rm.com/exploits/5106; reference:bugtraq,21458; reference:cve,CVE-2006-6334; reference:url,doc.emergingthreats.net/bin/view/Main/2007851;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/EXPLOIT/EXPLOIT_Citrix; sid:2007851; rev:8;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX ComponentOne VSFlexGrid ActiveX Control Archive Method Buffer Overflow Attempt"; flow:established,to_client;
content:"<OBJECT "; nocase; content:"classid"; nocase; distance:8; content:"C945E31A-102E-4A0D-8854-D599D7AE05FA"; nocase; distance:0; content:"Archive"; nocase; classtype:attempted-
user; reference:url,exploit-db.com/exploits/12673; reference:url,doc.emergingthreats.net/2011210; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_ComponentOne; sid:2011210; rev:6;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Consona Products SdcUser.TgConCtl ActiveX Control Buffer Overflow Attempt"; flow:established,to_client; content:"
<OBJECT "; nocase; content:"classid"; nocase; distance:0; content:"01113300-3E00-11D2-8470-0060089874ED"; nocase; distance:0; content:"RunCMD"; nocase; classtype:attempted-user;
reference:url,www.kb.cert.org/vuls/id/602801; reference:bugtraq,40006; reference:url,juniper.net/security/auto/vulnerabilities/vuln40006.html;
reference:url,doc.emergingthreats.net/2011212; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_Consona; sid:2011212; rev:5;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Consona Products SdcUser.TgConCtl ActiveX Control BOF Function Call"; flow:to_client,established;
content:"ActiveXObject"; nocase; content:"SdcUser.TgConCtl"; nocase; distance:0; content:"RunCMD"; nocase; classtype:attempted-user; reference:url,www.kb.cert.org/vuls/id/602801;
reference:bugtraq,40006; reference:url,juniper.net/security/auto/vulnerabilities/vuln40006.html; reference:url,doc.emergingthreats.net/2011213;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_Consona; sid:2011213; rev:3;)

#by evilghost and kevin ross
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT DX Studio Player Firefox Plug-in Command Injection Attempt"; flow:established,to_client; content:"dxstudio";
nocase; content:"shell.execute("; nocase; classtype:attempted-user; reference:cve,2009-2011; reference:url,doc.emergingthreats.net/2010841; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_DX_Studio; sid:2010841; rev:3;)

#by Chandon at Stillsecure
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Data Dynamics ActiveBar ActiveX Control (Actbar3.ocx 3.2) Multiple Insecure Methods"; flow:to_client,established;
content:"5407153D-022F-4CD2-88FF-465569BC5DB8"; nocase; pcrcr:"/.\.(ini|exe|dll|bat|com|cab|txt)/i", pcrcr:"/(Save|SaveLayoutChanges|SaveMenuUsageData)/i"; classtype:web-application-
attack; reference:bugtraq,24959; reference:cve,CVE-2007-3883; reference:url,www.exploit-db.com/exploits/5395; reference:url,doc.emergingthreats.net/2008127;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_Data_Dynamics; sid:2008127; rev:9;)

```

```
#by Akash Mahajan at stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV D-Link MPEG4 SHM (Audio) Control ActiveX Control Url Property Buffer Overflow Vulnerability";
flow:to_client,established; content:"A93B47FD-9BF6-4DA8-97FC-9270B9D64A6C"; nocase; content:"0x40000"; content:"Url"; nocase; classtype:web-application-attack; reference:bugtraq,28010;
reference:url,www.milw0rm.com/exploits/5193; reference:url,doc.emergingthreats.net/2007905; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Dlink;
sid:2007905; rev:47;)

#by Kevin Ross
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Possible EDraw Flowchart ActiveX Control OpenDocument Method Remote Code Execution Attempt";
flow:to_client,established; content:"F685AFD8-A5CC-410E-98E4-BAA1C559BA61"; nocase; content:"OpenDocument"; nocase; pcre:"/<OBJECT\s+[\^>]*classid\s*=\s*[\x22\x27]?
\s*clsid\s*\x3a\s*\x7b\s*\s*F685AFD8-A5CC-410E-98E4-BAA1C559BA61/si"; classtype:attempted-user; reference:url,doc.emergingthreats.net/2011055; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_EDraw; sid:2011055; rev:4;)

#by Kevin Ross
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Possible EMC Captiva PixTools Distributed Imaging ActiveX Control Vulnerable WriteToLog Method Arbitrary File
Creation/Overwrite Attempt"; flow:established,from_server; content:"00200338-3D33-4FFC-AC20-67AA234325F3"; nocase; content:"WriteToLog"; nocase; pcre:"/<OBJECT\s+[\^>]*classid\s*=\s*
[\x22\x27]? \s*clsid\s*\x3a\s*\x7b\s*\s*00200338-3D33-4FFC-AC20-67AA234325F3/si"; classtype:attempted-user; reference:url,www.securityfocus.com/bid/36566/info;
reference:url,www.shinnai.net/xplits/TXT_17zVhRhRsRE6qC6DAj52.html; reference:url,doc.emergingthreats.net/2010035; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB EMC; sid:2010035; rev:5;)

#by Kevin Ross
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Possible EMC Captiva PixTools Distributed Imaging ActiveX Control Vulnerable SetLogLevel/SetLogFile Method Arbitrary
File Creation/Overwrite Attempt"; flow:established,from_server; content:"00200338-3D33-4FFC-AC20-67AA234325F3"; nocase; content:"SetLog"; nocase; pcre:"/<OBJECT\s+
[\^>]*classid\s*=\s*[\x22\x27]? \s*clsid\s*\x3a\s*\x7b\s*\s*00200338-3D33-4FFC-AC20-67AA234325F3/si"; classtype:attempted-user; reference:url,www.securityfocus.com/bid/36566/info;
reference:url,www.shinnai.net/xplits/TXT_17zVhRhRsRE6qC6DAj52.html; reference:url,doc.emergingthreats.net/2010036; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB EMC; sid:2010036; rev:5;)

#by Wolvee
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV EMC Captiva PixTools ActiveX Arbitrary File Creation/Overwrite function call Attempt";
flow:to_client,established; content:"ActiveXObject"; nocase; content:"PDIControl.PDI.1"; nocase; distance:0; content:"WriteToLog"; distance:0; classtype:web-application-attack;
reference:url,www.securityfocus.com/bid/36566/info; reference:url,www.shinnai.net/xplits/TXT_17zVhRhRsRE6qC6DAj52.html; reference:url,doc.emergingthreats.net/2010154;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB EMC; sid:2010154; rev:4;)

#by Wolvee
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV EMC Captiva PixTools ActiveX Arbitrary File Creation/Overwrite function call Attempt";
flow:to_client,established; content:"ActiveXObject"; nocase; content:"PDIControl.PDI.1"; nocase; distance:0; content:"SetLog"; distance:0; classtype:web-application-attack;
reference:url,www.securityfocus.com/bid/36566/info; reference:url,www.shinnai.net/xplits/TXT_17zVhRhRsRE6qC6DAj52.html; reference:url,doc.emergingthreats.net/2010155;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB EMC; sid:2010155; rev:4;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV EasyMail Objects emmailstore.dll ActiveX Control Remote Buffer Overflow"; flow:to_client,established;
content:"588BE023-76A2-4F6D-8993-F7E588D79D98"; nocase; content:"0x400000"; nocase; content:"CreateStore"; nocase; classtype:web-application-attack; reference:bugtraq,32722;
reference:url,milw0rm.com/exploits/7402; reference:url,doc.emergingthreats.net/2008963; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_EasyMail;
sid:2008963; rev:9;)

#by Sujit Ghosal
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Quiksoft EasyMail imap connect() ActiveX stack overflow vulnerability"; flow:from_server,established; content:"
<script"; nocase; content:"unescape|28|"; nocase; content:"|2e|connect"; nocase; distance:0; content:"0CEA3FB1-7F88-4803-AA8E-AD021566955D"; nocase; distance:0; pcre:"/<OBJECT\s+
[\^>]*classid\s*=\s*[\x22\x27]? \s*clsid\s*\x3a\s*\x7b\s*\s*0CEA3FB1-7F88-4803-AA8E-AD021566955D/si"; classtype:attempted-user; reference:url,www.milw0rm.com/exploits/9704;
reference:url,www.securityfocus.com/bid/22583; reference:url,doc.emergingthreats.net/2009948; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_EasyMail;
sid:2009948; rev:8;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV EasyMail Quiksoft ActiveX Control Remote code execution clsid access attempt"; flow:to_client,established;
content:"0CEA3FB1-7F88-4803-AA8E-AD021566955D"; nocase; content:"LicenseKey"; nocase; pcre:"/<OBJECT\s+[\^>]*classid\s*=\s*[\x22\x27]? \s*clsid\s*\x3a\s*\x7b\s*\s*0CEA3FB1-7F88-4803-AA8E-
AD021566955D/si"; classtype:web-application-attack; reference:url,milw0rm.com/exploits/9684; reference:url,doc.emergingthreats.net/2010253; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_EasyMail; sid:2010253; rev:6;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV EasyMail Quiksoft ActiveX CreateStore method Remote code execution clsid access"; flow:established,to_client;
content:"18A76B9A-45C1-11D3-80DC-00C04F6892D0"; nocase; pcre:"/<OBJECT\s+[\^>]*classid\s*=\s*[\x22\x27]? \s*clsid\s*\x3a\s*\x7b\s*\s*18A76B9A-45C1-11D3-80DC-00C04F6892D0/si";
content:"CreateStore"; nocase; classtype:web-application-attack; reference:url,www.milw0rm.com/exploits/9685; reference:url,doc.emergingthreats.net/2010277;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_EasyMail; sid:2010277; rev:5;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV EasyMail ActiveX AddAttachment method Remote code execution clsid access attempt"; flow:established,to_client;
content:"68AC0D5F-0424-11D5-822F-00C04F68A8D9"; nocase; content:"AddAttachment"; nocase; pcre:"/<OBJECT\s+[\^>]*classid\s*=\s*[\x22\x27]? \s*clsid\s*\x3a\s*\x7b\s*\s*68AC0D5F-0424-11D5-
822F-00C04F68A8D9/si"; classtype:web-application-attack; reference:url,www.milw0rm.com/exploits/9705; reference:url,doc.emergingthreats.net/2010278;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_EasyMail; sid:2010278; rev:5;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Easy Grid ActiveX Multiple Arbitrary File Overwrite"; flow:to_client,established; content:"DD44C0EA-B2CF-31D1-
8D03-444553540000"; nocase; distance:0; content:"DoSaveFile"; nocase; classtype:web-application-attack; reference:bugtraq,33272; reference:url,doc.emergingthreats.net/2009102;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_EasyGrid; sid:2009102; rev:7;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Easy Grid ActiveX Multiple Arbitrary File Overwrite"; flow:to_client,established; content:"DD44C0EA-B2CF-31D1-
8D03-444553540000"; nocase; distance:0; content:"DoSaveFile"; nocase; classtype:web-application-attack; reference:bugtraq,33272; reference:url,doc.emergingthreats.net/2009063;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Easygrid; sid:2009063; rev:7;)

#by Jaime Blasco, updated by wolvee
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV eBay Enhanced Picture Services Control Clsid Access (1)"; flow:from_server,established; content:"4C39376E-FA9D-
4349-BACC-D305C1750EF3"; nocase; content:"PictureURLs"; nocase; pcre:"/<OBJECT\s+[\^>]*classid\s*=\s*[\x22\x27]? \s*clsid\s*\x3a\s*\x7b\s*\s*4C39376E-FA9D-4349-BACC-D305C1750EF3/si";
classtype:attempted-user; reference:url,www.kb.cert.org/vuls/id/983731; reference:url,www.microsoft.com/technet/security/advisory/969898.mspx;
reference:url,pages.ebay.com/securitycenter/activex/index.html; reference:url,doc.emergingthreats.net/2009402; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Ebay; sid:2009402; rev:8;)

#by Jaime Blasco, updated by wolvee
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV eBay Enhanced Picture Services Control Clsid Access (2)"; flow:from_server,established; content:"C3EB1670-84E0-
4EDA-B570-0B51AAE81679"; nocase; content:"PictureURLs"; nocase; pcre:"/<OBJECT\s+[\^>]*classid\s*=\s*[\x22\x27]? \s*clsid\s*\x3a\s*\x7b\s*\s*C3EB1670-84E0-4EDA-B570-0B51AAE81679/si";
classtype:attempted-user; reference:url,www.kb.cert.org/vuls/id/983731; reference:url,www.microsoft.com/technet/security/advisory/969898.mspx;
reference:url,pages.ebay.com/securitycenter/activex/index.html; reference:url,doc.emergingthreats.net/2009403; reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Ebay; sid:2009403; rev:8;)

#by mike cox
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT Possible HTTP 401 XSS Attempt (External Source)"; flow:from_server,established; content:"HTTP/1.1 401
Unauthorized[0d 0a]"; depth:27; nocase; content:"<script"; nocase; within:512; classtype:web-application-attack; reference:url,doc.emergingthreats.net/2010514;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Error_XSS; sid:2010514; rev:3;)

#by mike cox
#
```

```

alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT Possible HTTP 403 XSS Attempt (External Source)"; flow:from_server,established; content:"HTTP/1.1 403 Forbidden[00 0a]"; depth:24; nocase; content:"<script"; nocase; within:512; classtype:web-application-attack; reference:url,doc.emergingthreats.net/2010516; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Error_XSS; sid:2010516; rev:3;)

#by mike cox
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT Possible HTTP 404 XSS Attempt (External Source)"; flow:from_server,established; content:"HTTP/1.1 404 Not Found[00 0a]"; depth:24; nocase; content:"<script"; nocase; within:512; classtype:web-application-attack; reference:url,doc.emergingthreats.net/2010518; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Error_XSS; sid:2010518; rev:3;)

#by mike cox
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT Possible HTTP 405 XSS Attempt (External Source)"; flow:from_server,established; content:"HTTP/1.1 405 Method Not Allowed[00 0a]"; depth:33; nocase; content:"<script"; nocase; within:512; classtype:web-application-attack; reference:url,doc.emergingthreats.net/2010520; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Error_XSS; sid:2010520; rev:3;)

#by mike cox
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT Possible HTTP 406 XSS Attempt (External Source)"; flow:from_server,established; content:"HTTP/1.1 406 Not Acceptable[00 0a]"; depth:29; nocase; content:"<script"; nocase; within:512; classtype:web-application-attack; reference:url,doc.emergingthreats.net/2010522; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Error_XSS; sid:2010522; rev:3;)

#by mike cox
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT Possible HTTP 500 XSS Attempt (External Source)"; flow:from_server,established; content:"HTTP/1.1 500 Internal Server Error[00 0a]"; depth:36; nocase; content:"<script"; nocase; within:512; classtype:web-application-attack; reference:url,doc.emergingthreats.net/2010525; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Error_XSS; sid:2010525; rev:3;)

#by mike cox
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT Possible HTTP 503 XSS Attempt (External Source)"; flow:from_server,established; content:"HTTP/1.1 503 Service Unavailable[00 0a]"; depth:34; nocase; content:"<script"; nocase; within:512; classtype:web-application-attack; reference:url,doc.emergingthreats.net/2010527; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Error_XSS; sid:2010527; rev:3;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV EvansFTP EvansFTP.ocx Remote Buffer Overflow"; flow:to_client,established; content:"7E864D3E-3E6A-48F0-88AF-CEAE8322F9FD"; nocase; content:"RemoteAddress"; nocase; classtype:web-application-attack; reference:bugtraq,32814; reference:url,www.milw0rm.com/exploits/7460; reference:url,doc.emergingthreats.net/2008999; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_EvansFTP; sid:2008999; rev:7;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV FathFTP ActiveX DeleteFile Arbitrary File Deletion"; flow:to_client,established; content:"62A989CE-D39A-11D5-86F0-B9C370762176"; nocase; content:"DeleteFile"; nocase; classtype:web-application-attack; reference:bugtraq,33842; reference:url,xForce.iss.net/xforce/xfdb/48837; reference:url,doc.emergingthreats.net/2009184; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_FathFTP; sid:2009184; rev:7;)

#by stillsecure
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV FathFTP ActiveX Control GetFromURL Method Buffer Overflow Attempt"; flow:to_client,established; content:"<OBJECT "; nocase; content:"Classid"; nocase; distance:0; content:"62A989CE-D39A-11D5-86F0-B9C370762176"; nocase; distance:0; content:"GetFromURL"; nocase; classtype:web-application-attack; reference:url,exploit-db.com/exploits/14269; reference:url,doc.emergingthreats.net/2011251; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_FathFTP; sid:2011251; rev:6;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV FathFTP ActiveX Control RasIsConnected Method Buffer Overflow Attempt"; flow:to_client,established; flowbits:isset,etpro.clsid.detected; content:"<OBJECT "; nocase; content:"Classid"; nocase; distance:0; content:"62A989CE-D39A-11D5-86F0-B9C370762176"; nocase; distance:0; content:"RasIsConnected"; nocase; classtype:web-application-attack; reference:url,exploit-db.com/exploits/14269; reference:url,doc.emergingthreats.net/2011252; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_FathFTP; sid:2011252; rev:4;)

#by kevin ross
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT Mozilla Firefox Window.Open Document URI Spoofing Attempt"; flow:established,to_client; content:"window.open("; nocase; content:"setTimeout("; nocase; distance:0; content:"document.body.innerHTML"; nocase; distance:0; content:".stop"; nocase; distance:0; pcre:"/(window|w)\x2Estop/i"; classtype:misc-attack; reference:url,www.mozilla.org/security/announce/2010/mfsa2010-45.html; reference:url,bugzilla.mozilla.org/show_bug.cgi?id=556957; reference:cve,2010-1206; reference:url,doc.emergingthreats.net/2011240; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Firefox; sid:2011240; rev:4;)

#by stillsecure
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV FlexCell Grid ActiveX Multiple Arbitrary File Overwrite"; flow:to_client,established; content:"2A7D9CCE-211A-4654-9449-718F71ED9644"; nocase; pcre:"/(SaveFile|ExportToXML)/i"; classtype:web-application-attack; reference:url,www.milw0rm.com/exploits/7868; reference:bugtraq,33453; reference:url,doc.emergingthreats.net/2009120; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_FlexCell; sid:2009120; rev:8;)

#by kevin ross and joel esler
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT Foxit PDF Reader Buffer Overflow Attempt"; flow:established,to_client; content:"PDF-"; nocase; depth:300; content:"Launch"; nocase; distance:0; isdataat:600,relative; content:"|0A|"; within:600; content:"NewWindow true"; nocase; distance:600; classtype:attempted-user; reference:url,www.coresecurity.com/content/foxit-reader-vulnerabilities#ref.4; reference:cve,2009-0837; reference:url,doc.emergingthreats.net/2010876; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Foxit; sid:2010876; rev:3;)

#kevin ross
#
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT Possible Foxit PDF Reader Authentication Bypass Attempt"; flow:established,to_client; content:"PDF-"; nocase; depth:300; content:"Type/Action"; nocase; content:"Launch"; nocase; within:40; content:"NewWindow true"; nocase; distance:0; pcre:"/Type\x2FAction.+Launch.+x28\x2F[a-z]\x2F[a-z].+NewWindow\x20true/si"; classtype:attempted-user; reference:url,www.coresecurity.com/content/foxit-reader-vulnerabilities#ref.4; reference:cve,2009-0836; reference:url,doc.emergingthreats.net/2010878; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Foxit; sid:2010878; rev:2;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Foxit Reader ActiveX control OpenFile method Heap Overflow Attempt"; flow:established,to_client; content:"05563215-225C-45EB-BB34-AFA47217B1DE"; nocase; content:"OpenFile"; nocase; pcre:"/<OBJECT\s+[\^"]classid\s*=\s*[\x22\x27]?/s"clid\s*=\s*[\x3a\s*\x7b\s*05563215-225C-45EB-BB34-AFA47217B1DE/si"; classtype:attempted-user; reference:url,www.exploit-db.com/exploits/11196; reference:url,doc.emergingthreats.net/2010929; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Foxit; sid:2010929; rev:5;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Foxit Reader ActiveX OpenFile method Remote Code Execution Function Call"; flow:to_client,established; content:"ActiveXObject"; nocase; content:"FOXITREADEROCXlib.FoxitReaderOCX"; nocase; distance:0; content:"OpenFile "; nocase; classtype:attempted-user; reference:url,www.exploit-db.com/exploits/11196; reference:url,doc.emergingthreats.net/2010930; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Foxit; sid:2010930; rev:3;)

#by Akash Mahajan of Stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Gateway Weblaunch2.ocx ActiveX Control Insecure Method Exploit"; flow:to_client,established; content:"0x40000"; content:"DOWnLaunch"; content:"978B6657-DC7F-4489-9067-51FAB9D08857E"; nocase; classtype:web-application-attack; reference:url,www.milw0rm.com/exploits/4982; reference:bugtraq,27193; reference:url,doc.emergingthreats.net/2007852; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_Gateway; sid:2007852; rev:8;)

#by Stillsecure
#
##alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ACTIVEV GdPicture Pro ActiveX control SaveAsPDF Insecure Method"; flow:to_client,established; content:"E8512363-3581-42EF-A43D-990F7935CB8E"; nocase; content:"SaveAsPDF"; nocase; classtype:web-application-attack; reference:url,secunia.com/Advisories/31966; reference:url,milw0rm.com/exploits/6638; reference:url,doc.emergingthreats.net/2008613; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_GdPicture_Pro; sid:2008613; rev:8;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV GeoVision LiveAudio ActiveX Control Remote Code Execution"; flow:to_client,established; content:"814A3C52-B6F7-4AEA-A9BC-7849B9B0ECAB"; nocase; content:"GetAudioPlayingTime"; nocase; classtype:web-application-attack; reference:bugtraq,34115; reference:url,milw0rm.com/exploits/8206; reference:url,doc.emergingthreats.net/2009328; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_GeoVision; sid:2009328; rev:7;)

```



```
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Haihaisoft Universal Player ActiveX Control URL Property Buffer Overflow Function Call Attempt";
flow:to_client,established; content:"ActiveXObject"; nocase; content:"MYACTIVEX[2E|MyActiveXCtrl|2E|1"; nocase; distance:0; content:"URL"; nocase; classtype:attempted-user;
reference:url,www.shinnai.net/exploits/Zls16TIFuVPh1kPhMp.txt; reference:url,www.securityfocus.com/bid/37151/info; reference:url,doc.emergingthreats.net/2010374;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_HaiHaisoft; sid:2010374; rev:3;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Hummingbird Deployment Wizard 2008 ActiveX Insecure Methods"; flow:to_client,established; content:"7F9B30F1-5129-
4F5C-A76C-CE264AC7D10"; nocase; pcre:"/(Run|SetRegistryValueAsString|PerformUpdateAsync)/i"; classtype:web-application-attack; reference:url,secunia.com/Advisories/32337;
reference:url,doc.emergingthreats.net/2008678; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_Hummingbird; sid:2008678; rev:8;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Hyleos ChemView ActiveX Control SavesMolFile Method Buffer Overflow Attempt"; flow:established,to_client;
content:"C372350A-1D5A-44DC-A759-767FC553D96C"; nocase; content:"SaveasMolFile"; nocase; pcre:"/(<OBJECT\s+[>])*classid\s*=\s*[\x22\x27]?[s]*clsid\s*\x3a\s*\x7b?\s*\x22350A-1D5A-44DC-
A759-767FC553D96C/si"; classtype:attempted-user; reference:url,www.security-assessment.com/files/advisories/2010-02-11_ChemviewX_Activex.pdf; reference:url,secunia.com/advisories/38523;
reference:url,secunia.com/advisories/38523; reference:url,doc.emergingthreats.net/2010997; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_Hyleos;
sid:2010997; rev:5;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Hyleos ChemView ActiveX Control ReadMolFile Method Buffer Overflow Attempt"; flow:established,to_client;
content:"C372350A-1D5A-44DC-A759-767FC553D96C"; nocase; content:"ReadMolFile"; nocase; pcre:"/(<OBJECT\s+[>])*classid\s*=\s*[\x22\x27]?[s]*clsid\s*\x3a\s*\x7b?\s*\x22350A-1D5A-44DC-A759-
767FC553D96C/si"; classtype:attempted-user; reference:url,www.security-assessment.com/files/advisories/2010-02-11_ChemviewX_Activex.pdf; reference:url,secunia.com/advisories/38523;
reference:url,doc.emergingthreats.net/2010998; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_Hyleos; sid:2010998; rev:5;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Hyleos ChemView ActiveX Buffer Overflow Function Call"; flow:to_client,established; content:"ActiveXObject";
content:"HyleosChemView.HLChemView"; nocase; pcre:"/(ReadMolFile|SaveasMolFile)/i"; classtype:attempted-user; reference:url,www.security-
assessment.com/files/advisories/2010-02-11_ChemviewX_Activex.pdf; reference:url,secunia.com/advisories/38523; reference:url,doc.emergingthreats.net/2010999;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_Hyleos; sid:2010999; rev:3;)

#by Stillsecure (stillsecure.com)
#
##alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET ACTIVEV IAS Helper COH Component iashlpr.dll activex remote DOS"; flow:to_client,established; content:"68C0968C-0CE6-11D1-BAAE-
00C04FC2E200"; nocase; content:"PutProperty"; nocase; classtype:web-application-attack; reference:url,www.securityfocus.com/archive/1/archive/1/496695/100/0/threaded;
reference:cve,2008-2639; reference:url,securityreason.com/securityalert/4323; reference:url,doc.emergingthreats.net/2008618; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_IAS; sid:2008618; rev:8;)

#by stillsecure
#
#Updated references and revision numbers for Cisco, CVE and BID and changed message to something more informative
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV IBM Access Support ActiveX GetXMLValue Stack Overflow Attempt"; flow:from_server,established;
content:"ActiveXObject"; nocase; content:"IbmEgath.IbmEgathCtl.1"; distance:0; nocase; content:"GetXMLValue"; nocase; classtype:attempted-user;
reference:url,dev.metasploit.com/rdmine/projects/framework/repository/entry/modules/exploits/windows/browser/ibmegath_getxmlvalue.rb; reference:url,www.kb.cert.org/vuls/id/340420;
reference:url,tools.cisco.com/security/center/viewAlert.x?alertId=17871; reference:cve,2009-0215; reference:url,doc.emergingthreats.net/2010482;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_IBM; sid:2010482; rev:4;)

#by stillsecure
#
#Updated references and revision numbers for Cisco, CVE and BID and changed message to something more informative
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV IBM Access Support ActiveX GetXMLValue Stack Overflow Attempt"; flow:established,to_client; content:"74FFE28D-
2378-11D5-990C-006094235084"; nocase; content:"GetXMLValue"; nocase; pcre:"/(<OBJECT\s+[>])*classid\s*=\s*[\x22\x27]?[s]*clsid\s*\x3a\s*\x7b?\s*\x2274FE28D-2378-11D5-990C-006094235084/si";
classtype:attempted-user; reference:url,dev.metasploit.com/rdmine/projects/framework/repository/entry/modules/exploits/windows/browser/ibmegath_getxmlvalue.rb;
reference:url,www.kb.cert.org/vuls/id/340420; reference:url,tools.cisco.com/security/center/viewAlert.x?alertId=17871; reference:cve,2009-0215;
reference:url,doc.emergingthreats.net/2010483; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_IBM; sid:2010483; rev:6;)

#by Chandan at Stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Ibiz E-Banking Integrator V2 ActiveX Edition Insecure Method"; flow:to_client,established; content:"CLSID";
nocase; content:"24445430-F789-11CE-86F8-0020AFD8C60B"; distance:0; nocase; pcre:"/.*\.(in|exe|dll|bat|com|cab|txt)/i"; content:"WriteOFXDataFile"; nocase; classtype:web-application-
attack; reference:url,www.milw0rm.com/exploits/5416; reference:url,doc.emergingthreats.net/2008126; reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_Ibiz;
sid:2008126; rev:6;)

#Submitted 2006-09-18 by Christian Seifert, updated 2/5/07
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Microsoft Multimedia Controls - ActiveX control's spline function call CLSID"; flow:from_server,established;
content:"D7A7D7C3-D47F-11D0-89D3-00A0C90833E6"; nocase; content:".Spline|28|"; nocase; pcre:"/(<OBJECT\s+[>])*classid\s*=\s*[\x22\x27]?[s]*clsid\s*\x3a\s*\x7b?\s*\x22A7D7C3-D47F-11D0-89D3-
00A0C90833E6/si"; classtype:attempted-user; reference:url,www.osvdb.org/displayvuln.php?osvdb_id=28841; reference:cve,2006-4446; reference:url,doc.emergingthreats.net/2003102;
reference:url,www.emergingthreats.net/cgi-bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_IE_Vulnerabilities; sid:2003102; rev:11;)

#Submitted 2006-09-18 by Christian Seifert, updated 2/5/07
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Microsoft Multimedia Controls - ActiveX control's spline function call Object"; flow:from_server,established;
content:" DirectAnimation.PathControl"; content:".Spline|28|"; nocase; pcre:"/new[\r\n\s]*ActiveXObject[\r\n\s]*\([\r\n\s]*
(\x22DirectAnimation\.PathControl\x22|\x27DirectAnimation\.PathControl\x27)[\r\n\s]*\)\)\(w+)[\r\n\s]*=[\r\n\s]*
(\x22DirectAnimation\.PathControl\x22|\x27DirectAnimation\.PathControl\x27)[\r\n\s]*\x3b.new[\r\n\s]*ActiveXObject[\r\n\s]*\([\r\n\s]*1[\r\n\s]*\)\)/smi"; classtype:attempted-user;
reference:url, www.osvdb.org/displayvuln.php?osvdb_id=28841; reference:cve,2006-4446; reference:url,doc.emergingthreats.net/2003103; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_IE_Vulnerabilities; sid:2003103; rev:9;)

#Submitted 2006-09-18 by Christian Seifert, updated 2/5/07
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Microsoft Multimedia Controls - ActiveX control's KeyFrame function call CLSID"; flow:from_server,established;
flowbits:isset,etpro.clsid.detected; content:"D7A7D7C3-D47F-11D0-89D3-00A0C90833E6"; nocase; content:".KeyFrame|28|"; nocase; classtype:attempted-user;
reference:url,www.osvdb.org/displayvuln.php?osvdb_id=28842; reference:cve,2006-4777; reference:url,doc.emergingthreats.net/2003104; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_IE_Vulnerabilities; sid:2003104; rev:9;)

#Submitted 2006-09-18 by Christian Seifert, updated 2/5/07
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Microsoft Multimedia Controls - ActiveX control's KeyFrame function call Object"; flow:from_server,established;
content:"ActiveXObject"; nocase; content:"DirectAnimation.PathControl"; nocase; content:".KeyFrame|28|"; nocase; pcre:"/new[\r\n\s]*ActiveXObject[\r\n\s]*\([\r\n\s]*
(\x22DirectAnimation\.PathControl\x22|\x27DirectAnimation\.PathControl\x27)[\r\n\s]*\)\)\(w+)[\r\n\s]*=[\r\n\s]*
(\x22DirectAnimation\.PathControl\x22|\x27DirectAnimation\.PathControl\x27)[\r\n\s]*\x3b.new[\r\n\s]*ActiveXObject[\r\n\s]*\([\r\n\s]*1[\r\n\s]*\)\)/smi"; classtype:attempted-user;
reference:url,www.osvdb.org/displayvuln.php?osvdb_id=28842; reference:cve,2006-4777; reference:url,doc.emergingthreats.net/2003105; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_IE_Vulnerabilities; sid:2003105; rev:9;)

#Submitted 2006-11-01 by Frank Knobbe
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Microsoft WMIScriptUtils.WMIOObjectBroker object call CLSID"; flow:from_server,established; content:"7F587F63-
F06F-4331-8A26-339E03C0AE3D"; nocase; classtype:attempted-user; reference:url,www.securityfocus.com/bid/20843; reference:url,secunia.com/advisories/22603; reference:cve,2006-4704;
reference:url,www.microsoft.com/technet/security/bulletin/ms06-073.mspx; reference:url,doc.emergingthreats.net/2003158; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_IE_Vulnerabilities; sid:2003158; rev:10;)

#Submitted 2006-11-01 by Frank Knobbe
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Microsoft VsmIDE.DTE object call CLSID"; flow:from_server,established; content:"06723E09-F4C2-43c8-8358-
09FC01D80766"; nocase; classtype:attempted-user; reference:url,doc.emergingthreats.net/2003159; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_IE_Vulnerabilities; sid:2003159; rev:9;)

#Submitted 2006-11-01 by Frank Knobbe
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Microsoft DExplore.AppObj.8.0 object call CLSID"; flow:from_server,established; content:"639F725F-182D-4831-A9FD-
874847682010"; nocase; classtype:attempted-user; reference:url,doc.emergingthreats.net/2003160; reference:url,www.emergingthreats.net/cgi-
bin/cvswb.cgi/sigs/WEB_CLIENT/WEB_IE_Vulnerabilities; sid:2003160; rev:9;)

#Submitted 2006-11-01 by Frank Knobbe
#
```


[illegible]


```
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV COM Object Instantiation Memory Corruption Vulnerability (group 2)"; flow:established,from_server; pcre:"/01E04581-4EEE-11D0-BF9F-00AA005B4383|AF604EFE-8897-11D1-B944-00A0C90312E1|7849596A-48EA-486E-8937-A2A3009F31A9|FBE8BA05-BEEE-4442-804E-40906C4515E9|3050F391-98B5-11CF-BB82-00AA0080DCE0B|8EE42293-C315-11D0-806F-00A0C9A06E1F|246EB050-7F1C-11CE-BE57-00AA0051FE20|510A4910-7F1C-11CE-BE57-00AA0051FE20|6D36CE10-7F1C-11CE-BE57-00AA0051FE20|860D28D0-8BF4-11CE-BE59-00AA0051FE20|9478F640-7F1C-11CE-BE57-00AA0051FE20|80516FF0-7F1C-11CE-BE57-00AA0051FE20/i"; classtype:web-application-attack; reference:cve,2005-1990; reference:url,www.microsoft.com/technet/security/Bulletin/MS05-038.msp; reference:url,doc.emergingthreats.net/2002172; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS05-038; sid:2002172; rev:11;)
```

#disabling these all, they're old and very high load

```
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV COM Object Instantiation Memory Corruption Vulnerability (group 3)"; flow:established,from_server; pcre:"/EEED4C20-7F1B-11CE-BE57-00AA0051FE20|C786C04A-CBB5-11D0-BB4C-00C04FC2D8B0|858BD920-42A0-1069-A2E4-08002B30309D|E846F0A0-D367-11D1-8286-00A0C9231C29|B483AECB-DFD6-11D1-9DAA-00805F85CFE3|ECAB80BF-7F19-11D2-978E-0000F875E2A|46D066FA-9616-11D2-9342-0000F875AE17|67DC4C87-AA48-11D1-8F4F-00C04FB611C7|00022613-0000-0000-C000-000000000046|D2D588B5-D081-11D0-99E0-00C04FC2F8EC|5D08B586-343A-11D0-AD46-00C04FD8FDDF|CC7BF842-F175-11D1-A392-00E0291F3959|CC7BF843-F175-11D1-A392-00E0291F3959|3F8A6C33-E0FD-11D0-8A8C-00A0C9C02C5C/i"; classtype:web-application-attack; reference:cve,2005-1990; reference:url,www.microsoft.com/technet/security/Bulletin/MS05-038.msp; reference:url,doc.emergingthreats.net/2002173; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS05-038; sid:2002173; rev:13;)
```

#By Blake Harstein of Demarc

```
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Internet Explorer Vulnerable CLSID (Msdds.dll)"; flow:established,from_server; content:"EC444CB6-3E7E-4865-B1C3-00E72F39B3F"; nocase; classtype:web-application-attack; reference:url,www.frsirt.com/exploits/20050817.IE-Msddsdl1-0day.php; reference:url,doc.emergingthreats.net/2002308; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS05-038; sid:2002308; rev:48;)
```

#By Blake Hartstein

```
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV COM Object MS05-052 (group 1)"; flow:established,from_server; pcre:"/BC5F1E51-5110-11D1-AFF5-006097C9A284|F27CE930-4CA3-11D1-AFF2-006097C9A284|3BC4F3A7-652A-11D1-B4D0-00C04FC2D8B0|ECABAF2C-7F19-11D2-978E-0000F875E2A|283807B8-2C60-11D0-A31D-00AA00892C03|250770F3-6AF2-11CF-A915-008029E31FCD|D2404453-1F01-11D1-8E63-006097D2DF48|03CB9467-FD9D-42A8-82F9-8615B4223E6E|598EBA02-B49A-11D2-A1C1-00609778EA66|8FE7E181-BB96-11D2-A1C8-00609778EA66|4CFB5280-8008-4367-848F-5A13EBF27FD1|B3E0E785-BD78-4366-9560-87BDABE2723BE|208D06A3-E128-4755-9607-2E39EF84CF5C/i"; classtype:web-application-attack; reference:cve,2005-2127; reference:url,www.microsoft.com/technet/security/Bulletin/MS05-052.msp; reference:url,doc.emergingthreats.net/2002491; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS05-052; sid:2002491; rev:12;)
```

#By Blake Hartstein

```
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV COM Object MS05-052 (group 2)"; flow:established,from_server; pcre:"/4FAA8301-CE66-477C-9F58-F601039E9B78|6C8E0382-A879-4D2A-8EC3-1F2A43611BA8|F117831B-C052-11D1-B1C0-00C04FC2F3EF|3050F667-98B5-11CF-BB82-00AA0080DCE0B|1AA06BA1-0E88-11D1-8391-00C04FB07C09|F28D867A-DDB1-11D3-B8E8-00A0C901AE6B|6B7F1602-D44C-11D0-A7D9-AE3D17000000|7007ACCF-3202-11D1-AA02-00805F1270E|992CFFA0-F557-101A-88EC-00DD0B10CCC48|00020420-0000-0000-C000-000000000046|0006F02A-0000-0000-000000000046|ABBA0018-3075-11D6-88A4-008080200F88|CE292861-FC88-11D0-9E69-00C04FD7C15B/i"; classtype:web-application-attack; reference:cve,2005-2127; reference:url,www.microsoft.com/technet/security/Bulletin/MS05-052.msp; reference:url,doc.emergingthreats.net/2002492; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS05-052; sid:2002492; rev:12;)
```

#By Blake Hartstein

```
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV COM Object MS05-052 (group 3)"; flow:established,from_server; pcre:"/6E227101-F799-11CF-9227-00AA00A1EB95|7057E952-BD18-11D1-8919-00C04FC2C836|7007ACCF-3202-11D1-AA02-00805F1270E|4622AD11-FF23-11D0-8D34-00A0C90F2719|98CB4060-D3E7-42A1-8D85-949D34EBFE14|47C6C527-6204-4F91-849D-66E234DE0E01|35CECE8A3-28E6-11D2-8773-92E220524153|730F6C0C-2C86-11D2-8773-92E220524153|2C10A98F-D64F-4384-BD6E-DD0E1B8F2074C|6F9F3481-840D-4614-B09C-646288ECDE8|8E268FC1-AFD6-11CF-BFFC-00AA00C0FDC|F0975AFE-5C7F-11D2-8773-92E220524153/i"; classtype:web-application-attack; reference:cve,2005-2127; reference:url,www.microsoft.com/technet/security/Bulletin/MS05-052.msp; reference:url,doc.emergingthreats.net/2002493; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS05-052; sid:2002493; rev:81;)
```

#By Blake Hartstein

```
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV McIwindx ActiveX Control"; flow:from_server,established; content:"288F1523-FAC4-11CE-B16F-00AA0060D93D"; nocase; classtype:web-application-attack; reference:url,www.microsoft.com/technet/security/bulletin/ms05-054.msp; reference:url,doc.emergingthreats.net/2002724; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS05-054; sid:2002724; rev:11;)
```

#By Blake Hartstein

```
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV COM Object Instantiation Memory Corruption Vulnerability MS05-054"; flow:established,from_server; pcre:"/9006(2|0421|5)|1401(0000)|6F071|0000-0000-C000-0000000000046|6E2271(FB|09A-F)|F799-11CF-9227-00AA00A1EB95|ECAB(AFC0|B0AB)-7F19-11D2-978E-0000F875E2A|3050F4F5-98B5-11CF-BB82-00AA0080DCE0B|DF083D60-548F-101B-8E65-08002B2D0119|2D2E24C8-0CD5-458F-86EA-3E6FA22C8E64|51B4ABF3-748F-4E3B-A276-C828330E926A|E4979309-7A32-495E-BA92-78014AAD4961|62EC9F22-5E30-11D2-97A1-00C04FB6DD9A|B1DAED44-EE64-11D0-97FE-00C04FC308A4|D675E22B-CAE9-11D2-AF7B-00C04F99179F/i"; classtype:web-application-attack; reference:cve,2005-2831; reference:url,www.microsoft.com/technet/security/bulletin/ms05-054.msp; reference:url,doc.emergingthreats.net/2002725; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS05-054; sid:2002725; rev:13;)
```

#By Blake Hartstein from Demarc

```
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Danim.dll and Dxtmsft.dll COM Objects"; flow:established,from_server; pcre:"/42B07B28-2280-4937-B035-0293FB812781|542FB453-5003-11CF-92A2-00AA0088A733/i"; classtype:web-application-attack; reference:cve,2006-1186; reference:url,www.microsoft.com/technet/security/bulletin/ms06-013.msp; reference:url,doc.emergingthreats.net/2002861; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-013; sid:2002861; rev:11;)
```

#By Blake Hartstein at Demarc

```
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Wmm2fxa.dll COM Object Instantiation Memory Corruption CLSID 1 Access Attempt"; flow:established,to_client; content:"B4D0CDD9-2CC1-4081-982B-20D7030234EF"; nocase; pcre:"/<OBJECT\s+[^\s]*classid\s*=\s*[\\x22\\x27]?\\s*clsid\s*\\x3a\s*\\x7B?\\s*B4D0CDD9-2CC1-4081-982B-20D7030234EF/si"; classtype:attempted-user; reference:cve,2006-1303; reference:bugtraq,18328; reference:url,www.microsoft.com/technet/security/bulletin/ms06-021.msp; reference:url,doc.emergingthreats.net/2002971; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-021; sid:2002971; rev:4;)
```

#By Blake Hartstein at Demarc

```
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Wmm2fxa.dll COM Object Instantiation Memory Corruption CLSID 2 Access Attempt"; flow:established,to_client; content:"C63344D8-70D3-4032-9832-7A3CAD5091A5"; nocase; pcre:"/<OBJECT\s+[^\s]*classid\s*=\s*[\\x22\\x27]?\\s*clsid\s*\\x3a\s*\\x7B?\\s*C63344D8-70D3-4032-9832-7A3CAD5091A5/si"; classtype:attempted-user; reference:cve,2006-1303; reference:bugtraq,18328; reference:url,www.microsoft.com/technet/security/bulletin/ms06-021.msp; reference:url,doc.emergingthreats.net/2010263; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-021; sid:2010263; rev:5;)
```

#By Blake Hartstein at Demarc

```
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Wmm2fxa.dll COM Object Instantiation Memory Corruption CLSID 3 Access Attempt"; flow:established,to_client; content:"353359C1-39E1-491B-9951-464FD8AB071C"; nocase; pcre:"/<OBJECT\s+[^\s]*classid\s*=\s*[\\x22\\x27]?\\s*clsid\s*\\x3a\s*\\x7B?\\s*353359C1-39E1-491B-9951-464FD8AB071C/si"; classtype:attempted-user; reference:cve,2006-1303; reference:bugtraq,18328; reference:url,www.microsoft.com/technet/security/bulletin/ms06-021.msp; reference:url,doc.emergingthreats.net/2010264; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-021; sid:2010264; rev:5;)
```

#by shirkdog and Blake hartstein, split by kevin ross for performance

```
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV COM Object MS06-042 CLSID 1 Access Attempt"; flow:established,to_client; content:"5DFB2651-9668-11D0-B178-00C04FC2A0CA"; nocase; pcre:"/<OBJECT\s+[^\s]*classid\s*=\s*[\\x22\\x27]?\\s*clsid\s*\\x3a\s*\\x7B?\\s*5DFB2651-9668-11D0-B178-00C04FC2A0CA/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.msp; reference:url,doc.emergingthreats.net/2010292; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010292; rev:5;)
```

#by shirkdog and Blake hartstein, split by kevin ross for performance

```
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV COM Object MS06-042 CLSID 2 Access Attempt"; flow:established,to_client; content:"39A2C2A6-4778-11D2-98D8-204C4F4F5020"; nocase; pcre:"/<OBJECT\s+[^\s]*classid\s*=\s*[\\x22\\x27]?\\s*clsid\s*\\x3a\s*\\x7B?\\s*39A2C2A6-4778-11D2-98D8-204C4F4F5020/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.msp; reference:url,doc.emergingthreats.net/2010293; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010293; rev:5;)
```

#by shirkdog and Blake hartstein, split by kevin ross for performance

```
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV COM Object MS06-042 CLSID 3 Access Attempt"; flow:established,to_client; content:"3DA2AA3E-3D96-11D2-98D2-204C4F4F5020"; nocase; pcre:"/<OBJECT\s+[^\s]*classid\s*=\s*[\\x22\\x27]?\\s*clsid\s*\\x3a\s*\\x7B?\\s*3DA2AA3E-3D96-11D2-98D2-204C4F4F5020/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.msp; reference:url,doc.emergingthreats.net/2010294; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010294; rev:5;)
```

#by shirkdog and Blake hartstein, split by kevin ross for performance

```
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV COM Object MS06-042 CLSID 4 Access Attempt"; flow:established,to_client; content:"E8C31D11-6FD2-4659-AD75-155FA143F42B"; nocase; pcre:"/<OBJECT\s+[^\s]*classid\s*=\s*[\\x22\\x27]?\\s*clsid\s*\\x3a\s*\\x7B?\\s*E8C31D11-6FD2-4659-AD75-155FA143F42B/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.msp; reference:url,doc.emergingthreats.net/2010295; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010295; rev:5;)
```

#by shirkdog and Blake hartstein, split by kevin ross for performance

##alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg:"ET ACTIVEV COM Object MS06-042 CLSID 5 Access Attempt"; flow:established,to_client; content:"44C79591-D0DE-49C4-BA3C-A45A87003356"; nocase; pcre:"/<OBJECT\s+[>]*classid\s*=\s*[\x22\x27]?s*clsid\s*\x3a\s*\x7b?s*44C79591-D0DE-49C4-BA3C-A45A87003356/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.mspx; reference:url,doc.emergingthreats.net/2010296; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010296; rev:5;)

#by shirkdog and Blake hartstein, split by kevin ross for performance

##alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg:"ET ACTIVEV COM Object MS06-042 CLSID 6 Access Attempt"; flow:established,to_client; content:"1B544C24-FD0B-11CE-8C63-00AA0044B520"; nocase; pcre:"/<OBJECT\s+[>]*classid\s*=\s*[\x22\x27]?s*clsid\s*\x3a\s*\x7b?s*1B544C24-FD0B-11CE-8C63-00AA0044B520/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.mspx; reference:url,doc.emergingthreats.net/2010297; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010297; rev:5;)

#by shirkdog and Blake hartstein, split by kevin ross for performance

##alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg:"ET ACTIVEV COM Object MS06-042 CLSID 7 Access Attempt"; flow:established,to_client; content:"1CB1623E-BBEC-4E8D-B2DF-DC08C6F4627C/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.mspx; reference:url,doc.emergingthreats.net/2010298; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010298; rev:5;)

#by shirkdog and Blake hartstein, split by kevin ross for performance

##alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg:"ET ACTIVEV COM Object MS06-042 CLSID 8 Access Attempt"; flow:established,to_client; content:"2D20D48B-B47E-4FB7-83BD-E3C2EE250D26/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.mspx; reference:url,doc.emergingthreats.net/2010299; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010299; rev:5;)

#by shirkdog and Blake hartstein, split by kevin ross for performance

##alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg:"ET ACTIVEV COM Object MS06-042 CLSID 9 Access Attempt"; flow:established,to_client; content:"31087270-D348-432C-899E-2D2F38FF29A0/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.mspx; reference:url,doc.emergingthreats.net/2010300; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010300; rev:5;)

#by shirkdog and Blake hartstein, split by kevin ross for performance

##alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg:"ET ACTIVEV COM Object MS06-042 CLSID 10 Access Attempt"; flow:established,to_client; content:"41D28841-7692-4C83-AFD3-F60E845341AF/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.mspx; reference:url,doc.emergingthreats.net/2010301; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010301; rev:5;)

#by shirkdog and Blake hartstein, split by kevin ross for performance

##alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg:"ET ACTIVEV COM Object MS06-042 CLSID 11 Access Attempt"; flow:established,to_client; content:"2EA10031-0033-450E-8072-E27D9E768142/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.mspx; reference:url,doc.emergingthreats.net/2010302; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010302; rev:5;)

#by shirkdog and Blake hartstein, split by kevin ross for performance

##alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg:"ET ACTIVEV COM Object MS06-042 CLSID 12 Access Attempt"; flow:established,to_client; content:"4D4C9FEF-ED80-47EA-A3FA-3215FDBB33AB/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.mspx; reference:url,doc.emergingthreats.net/2010303; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010303; rev:5;)

#by shirkdog and Blake hartstein, split by kevin ross for performance

##alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg:"ET ACTIVEV COM Object MS06-042 CLSID 13 Access Attempt"; flow:established,to_client; content:"C0D076C5-E4C6-4561-8BF4-80D48DB819D7/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.mspx; reference:url,doc.emergingthreats.net/2010304; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010304; rev:5;)

#by shirkdog and Blake hartstein, split by kevin ross for performance

##alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg:"ET ACTIVEV COM Object MS06-042 CLSID 14 Access Attempt"; flow:established,to_client; content:"4F3E50BD-A9D7-4721-B0E1-00CB42A0A747/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.mspx; reference:url,doc.emergingthreats.net/2010305; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010305; rev:5;)

#by shirkdog and Blake hartstein, split by kevin ross for performance

##alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg:"ET ACTIVEV COM Object MS06-042 CLSID 15 Access Attempt"; flow:established,to_client; content:"586FB486-5560-4FF3-96DF-1118C96AF456/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.mspx; reference:url,doc.emergingthreats.net/2010306; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010306; rev:5;)

#by shirkdog and Blake hartstein, split by kevin ross for performance

##alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg:"ET ACTIVEV COM Object MS06-042 CLSID 16 Access Attempt"; flow:established,to_client; content:"5B4B05EB-1F63-446B-AAD1-E10A34D650E0/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.mspx; reference:url,doc.emergingthreats.net/2010307; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010307; rev:5;)

#by shirkdog and Blake hartstein, split by kevin ross for performance

##alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg:"ET ACTIVEV COM Object MS06-042 CLSID 17 Access Attempt"; flow:established,to_client; content:"679E132F-561B-42F8-846C-A70BDC62999/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.mspx; reference:url,doc.emergingthreats.net/2010308; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010308; rev:5;)

#by shirkdog and Blake hartstein, split by kevin ross for performance

##alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg:"ET ACTIVEV COM Object MS06-042 CLSID 18 Access Attempt"; flow:established,to_client; content:"6C68955E-F965-4249-8E18-F0977B1D2899/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.mspx; reference:url,doc.emergingthreats.net/2010309; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010309; rev:5;)

#by shirkdog and Blake hartstein, split by kevin ross for performance

##alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg:"ET ACTIVEV COM Object MS06-042 CLSID 19 Access Attempt"; flow:established,to_client; content:"7F1232EE-44D7-4494-AB8B-CC61810E21A5/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.mspx; reference:url,doc.emergingthreats.net/2010310; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010310; rev:5;)

#by shirkdog and Blake hartstein, split by kevin ross for performance

##alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg:"ET ACTIVEV COM Object MS06-042 CLSID 20 Access Attempt"; flow:established,to_client; content:"92883667-E95C-443D-AC96-4CACA278EB6E/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.mspx; reference:url,doc.emergingthreats.net/2010311; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010311; rev:5;)

#by shirkdog and Blake hartstein, split by kevin ross for performance
#

12/21/2022 11:15:53 AM

```
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX COM Object MS06-042 CLSID 38 Access Attempt"; flow:established,to_client; content:"A204529E-84E0-4550-A2E0-C2507C5C0D0"; nocase; pcre:"/<OBJECT\s+[>]*classid\s*=\s*[\x22\x27]\?s*clsid\s*\x3a\s*\x7B?\s*A204529E-84E0-4550-A2E0-C2507C5C0D0/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.msp; reference:url,doc.emergingthreats.net/2010329; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010329; rev:5;)

#by shirkdog and Blake hartstein, split by kevin ross for performance
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX COM Object MS06-042 CLSID 39 Access Attempt"; flow:established,to_client; content:"E673DCF2-C316-4c6f-AA96-4E4DC6DC291E"; nocase; pcre:"/<OBJECT\s+[>]*classid\s*=\s*[\x22\x27]\?s*clsid\s*\x3a\s*\x7B?\s\E673DCF2-C316-4c6f-AA96-4E4DC6DC291E/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.msp; reference:url,doc.emergingthreats.net/2010330; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010330; rev:5;)

#by shirkdog and Blake hartstein, split by kevin ross for performance
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX COM Object MS06-042 CLSID 40 Access Attempt"; flow:established,to_client; content:"D74CA70F-2236-4BA8-A297-4B2A28C2363C"; nocase; pcre:"/<OBJECT\s+[>]*classid\s*=\s*[\x22\x27]\?s*clsid\s*\x3a\s*\x7B?\s\D74CA70F-2236-4BA8-A297-4B2A28C2363C/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.msp; reference:url,doc.emergingthreats.net/2010331; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010331; rev:5;)

#by shirkdog and Blake hartstein, split by kevin ross for performance
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX COM Object MS06-042 CLSID 41 Access Attempt"; flow:established,to_client; content:"01002B17-5D93-4551-81E4-831FEF780A53"; nocase; pcre:"/<OBJECT\s+[>]*classid\s*=\s*[\x22\x27]\?s*clsid\s*\x3a\s*\x7B?\s\01002B17-5D93-4551-81E4-831FEF780A53/si"; classtype:attempted-user; reference:cve,2006-3638; reference:url,www.microsoft.com/technet/security/Bulletin/MS06-042.msp; reference:url,doc.emergingthreats.net/2010332; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2010332; rev:5;)

#by Jaime Blasco
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Communications Control Clsid Access"; flow:from_server,established; content:"648A5600-2C6E-101B-82B6-000000000014"; nocase; pcre:"/<OBJECT\s+[>]*classid\s*=\s*[\x22\x27]\?s*clsid\s*\x3a\s*\x7B?\s\648A5600-2C6E-101B-82B6-000000000014/si"; classtype:attempted-user; reference:url,www.microsoft.com/technet/security/advisory/969898.msp; reference:url,doc.emergingthreats.net/2009400; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS06-042; sid:2009400; rev:7;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft DebugDiag CrashHangExt.dll ActiveX Control Remote Denial of Service"; flow:to_client,established; content:"723D6F8-AD31-440F-BAF0-9E7A292A53DA"; nocase; content:"GetEntryPointForThread"; nocase; classtype:web-application-attack; reference:bugtraq,31996; reference:url,doc.emergingthreats.net/2008792; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MSDebugDiag; sid:2008792; rev:47;)

#by kevin ross
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT Possible Microsoft Internet Explorer mshtml.dll Timer ID Memory Pointer Information Disclosure Attempt"; flow:established,to_client; content:"setInterval("; nocase; content:"document.getElementById"; nocase; distance:0; content:".innerHTML"; nocase; distance:0; content:".toString("; nocase; within:60; classtype:attempted-user; reference:url,tools.cisco.com/security/center/viewAlert.x?alertId=20815; reference:url,reversemode.com/index.php?option=com_content&task=view&id=68&Itemid=1; reference:url,doc.emergingthreats.net/2011764; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MSIEmshtml; sid:2011764; rev:3;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Visual Basic Common AVI ActiveX Control File Parsing Buffer Overflow"; flow:to_client,established; content:"B09DE715-87C1-11D1-8BE3-0000F8754DA1"; nocase; content:"Open"; nocase; content:".avi"; nocase; distance:0; classtype:web-application-attack; reference:url,www.milw0rm.com/exploits/7431; reference:bugtraq,32613; reference:url,doc.emergingthreats.net/2008993; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MSVB_AVI; sid:2008993; rev:7;)

#by Veerendra at secpod
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft PicturePusher ActiveX Cross Site File Upload Attack"; flow:from_server,established; content:"507813C3-0B26-47AD-AB0C-D483C7A21FA7"; nocase; pcre:"/http\:\/\/.*?[\w]{4,}=1/i"; nocase; pcre:"/(PostURL|AddSeparator|AddString|Post)/i"; classtype:web-application-attack; reference:url,milw0rm.com/exploits/6699; reference:url,doc.emergingthreats.net/2008673; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS_Picturepusher; sid:2008673; rev:9;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Whale Intelligent App Gateway ActiveX Buffer Overflow Function call-1"; flow:from_server,established; content:"ActiveXObject"; nocase; content:"ComponentManager.Installer.1"; distance:0; nocase; content:"CheckForUpdates"; nocase; classtype:web-application-attack; reference:url,dev.metasploit.com/redmine/projects/framework/repository/entry/modules/exploits/windows/browser/mswhale_checkforupdates.rb; reference:url,www.kb.cert.org/vuls/id/789121; reference:url,doc.emergingthreats.net/210560; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS_Whale; sid:2010560; rev:3;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Whale Intelligent App Gateway ActiveX Buffer Overflow Function call-2"; flow:from_server,established; content:"ActiveXObject"; nocase; content:"ComponentManager.Installer.1"; distance:0; nocase; content:"UpdateComponents"; nocase; classtype:web-application-attack; reference:url,dev.metasploit.com/redmine/projects/framework/repository/entry/modules/exploits/windows/browser/mswhale_checkforupdates.rb; reference:url,www.kb.cert.org/vuls/id/789121; reference:url,doc.emergingthreats.net/2010561; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS_Whale; sid:2010561; rev:3;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Whale Intelligent Application Gateway ActiveX Buffer Overflow-1"; flow:established,to_client; content:"809563A9-805F-459B-87F2-BA842255C89A"; nocase; content:"CheckForUpdates"; nocase; pcre:"/<OBJECT\s+[>]*classid\s*=\s*[\x22\x27]\?s*clsid\s*\x3a\s*\x7B?\s\809563A9-805F-459B-87F2-BA842255C89A/si"; classtype:web-application-attack; reference:url,dev.metasploit.com/redmine/projects/framework/repository/entry/modules/exploits/windows/browser/mswhale_checkforupdates.rb; reference:url,www.kb.cert.org/vuls/id/789121; reference:url,doc.emergingthreats.net/2010562; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS_Whale; sid:2010562; rev:5;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Whale Intelligent Application Gateway ActiveX Buffer Overflow-2"; flow:established,to_client; content:"809563A9-805F-459B-87F2-BA842255C89A"; nocase; content:"UpdateComponents"; nocase; pcre:"/<OBJECT\s+[>]*classid\s*=\s*[\x22\x27]\?s*clsid\s*\x3a\s*\x7B?\s\809563A9-805F-459B-87F2-BA842255C89A/si"; classtype:web-application-attack; reference:url,dev.metasploit.com/redmine/projects/framework/repository/entry/modules/exploits/windows/browser/mswhale_checkforupdates.rb; reference:url,www.kb.cert.org/vuls/id/789121; reference:url,doc.emergingthreats.net/2010563; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS_Whale; sid:2010563; rev:5;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Windows Media Services nskey.dll ActiveX Control Possible Remote Buffer Overflow"; flow:to_client,established; content:"26462058-878C-11D1-807C-0000C040BCDB"; nocase; content:"CallHTMLHelp"; nocase; classtype:web-application-attack; reference:bugtraq,30814; reference:cve,2008-5232; reference:url,doc.emergingthreats.net/2008925; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS_Windows_Media_Services; sid:2008925; rev:7;)

#by Akash Mahajan of Stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Works 7 WkImgSrv.dll ActiveX Remote BOF Exploit"; flow:to_client,established; content:"0x40000"; content:"WksPictureInterface"; nocase; distance:0; content:"00E1D859-6EFD-4CE7-8C0A-2DA3BCAAD9C6"; nocase; distance:0; classtype:web-application-attack; reference:bugtraq,28820; reference:url,www.milw0rm.com/exploits/5460; reference:url,www.milw0rm.com/exploits/5530; reference:url,doc.emergingthreats.net/2008226; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS_Works; sid:2008226; rev:8;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft XML Core Services DTD Cross Domain Information Disclosure object"; flow:to_client,established; content:"Hsxml2.DOFDocument.3.0"; nocase; content:"loadXML"; distance:0; nocase; content:"parseError.srcText"; distance:0; nocase; classtype:web-application-attack; reference:bugtraq,32155; reference:url,milw0rm.com/exploits/7196; reference:url,doc.emergingthreats.net/2008886; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/WEB_CLIENT/WEB_MS_XML_Core; sid:2008886; rev:6;)

#by stillsecure
#
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft XML Core Services DTD Cross Domain Information Disclosure clsid"; flow:to_client,established; content:"f5078f32-c551-11d3-89b9-0000f8fe221"; nocase; content:"loadXML"; nocase; distance:0; content:"parseError.srcText"; nocase; distance:0; classtype:web-application-attack; reference:bugtraq,32155; reference:url,milw0rm.com/exploits/7196; reference:url,doc.emergingthreats.net/2008887; reference:url,www.emergingthreats.net/cgi-
```

```
bin/cvsweb.cgi/signs/WEB_CLIENT/WEB_MS_XML_Core; sid:2008887; rev:7;)
```

```
#
```

```
##alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX MM6 Technologies Barcode ActiveX Barcode.dll Multiple Arbitrary File Overwrite"; flow:to_client,established;  
content:"14D09688-CFA7-11D5-995A-005004CE563B"; nocase; pcre:"/(SaveAsBMP|SaveAsWMF)/i"; classtype:web-application-attack; reference:bugtraq,31979;  
reference:url,milw0rm.com/exploits/6871; reference:url,doc.emergingthreats.net/2008889; reference:url,www.emergingthr
```