



FIRSTLIGHT

SAMPLE SIGNATURE SET

As of August 1st 2007, the FirstLight signature set comprises over 10000 signatures that cover a broad range of both emerging and established threats.

Major areas covered by the FirstLight signature set include Client Side Attacks, Server Side Attacks, Exploit Components, Malware, Web Application Attacks, Protocols and Policy.

What follows is a sampling of signatures from each of the previously mentioned categories.

CLIENT SIDE ATTACKS

```
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET ANY ( msg:"EmbeddedQuickTime.FireFox.Command.Execution";
flow:to_client; content:"xml "; content:"quicktime"; content:"type=";
content:"application/x-quicktime-media-link"; distance:0; within:37; content:"embed ";
content:"qtnext="; content:"initWithPath"; reference:cve,; sid: 20040238; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET ANY ( msg:"NormalizeIDN.FireFox.Buffer.Overflow";
flow:to_client; content:"HTML"; nocase; content:"A HREF"; nocase; content:"http"; nocase;
content:"-----"; within:35; reference:cve,CVE-2005-2871; sid: 20040445;
rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET ANY (
msg:"GIF.File.Microsoft.InternetExplorer.Double.Free.B"; flow:to_client; content:"| 47 49 46 38
37 61 |"; content:"| 10 00 10 00 |"; distance:0; within:4; reference:cve,CVE-2003-1048; sid:
20040698; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET ANY (
msg:"mailto.URIHandler.AdobeAcrobat.Command.Execution"; flow:to_client; content:"| 25 50 44 46
|"; offset: 0; depth: 4; content:"obj"; nocase; content:"/URI(mailto: "; nocase; content:"| 25 |";
content:"| 3e 3e |"; reference:cve,; sid: 20040695; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET ANY ( msg:"SOAP.API.Mozilla.Integer.Overflow";
flow:to_client; content:"html"; nocase; content:"new Array"; nocase; content:"new
SOAPparameter"; nocase; reference:cve,CVE-2004-0722; sid: 20040696; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET ANY ( msg:"EMF.MicrosoftWindowsGraphicsRendering.MS04-
032.Buffer.Overflow"; flow:to_client; content:"| 01 00 00 00 40 00 00 00 00 00 00 00 00 00
00 20 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 4c 03 00 00 4c 03 00 00 20 45 4d 46 00 00 01
00 40 00 00 00 0b 00 00 00 0a 00 00 00 ff ff 00 00 |"; reference:cve,CAN-2004-0209; sid:
20040700; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET $HTTP_PORTS ( msg:"Internet Download Accelerator 5.2
Remote Buffer Overflow PoC"; flow:to_client; content:"clsid:2A646672-9C3A-4C28-9A7A-
1FB0F63F28B6"; nocase; content:".NotSafe"; distance:0; nocase; sid: 20039278; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET ANY (
msg:"VisualBasicActiveX.MicrosoftInternetExplorer.MS07-45.MemoryCorruption.C"; flow:to_client;
content:"8B21775E-717D-11CE-AB5B-D41203C10000"; sid: 20040004; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET ANY ( msg:"search.LinkedinToolbar.BufferOverflow";
flow:to_client; content:"0F2437D6-C4E4-42CA-A906-F506E09354B7"; nocase; content:".search";
distance:0; nocase; sid: 20039463; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET ANY (
msg:"HTTPDownloadFile.EDrawOfficeViewer.InsecureMethod"; flow:to_client; content:"6BA21C22-53A5-
463F-BBE8-5CF7FFA0132B"; content:".HttpDownloadFile"; sid: 20040028; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET ANY ( msg:"ListFiles.hpqutil.HP.ActiveX.Heap.Overflow";
flow:to_client; content:"F3F381A3-4795-41FF-8190-7AA2A8102F85"; nocase; content:".ListFiles";
nocase; reference:cve,; sid: 20040285; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET ANY ( msg:"SaveAsWMF.MW6QRCode.ActiveX.File.Overwrite";
flow:to_client; content:"3BB56637-651D-4D1D-AFA4-C0506F57EAF8"; nocase; content:".SaveAsWMF";
reference:cve,; sid: 20040322; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET ANY ( msg:"ActiveX.YahooMessenger.Buffer.Overflow";
flow:to_client; content:"64AA7031-C150-4118-8D31-FD273A2BB22C"; reference:cve,CVE-2007-4515;
sid: 20040177; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET ANY ( msg:"SaveAsBMP.MW6QRCode.ActiveX.File.Overwrite";
flow:to_client; content:"3BB56637-651D-4D1D-AFA4-C0506F57EAF8"; nocase; content:".SaveAsBMP";
nocase; reference:cve,; sid: 20040323; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET ANY ( msg:"src.AdobeReader.ActiveX.Buffer.Overflow";
flow:to_client; content:"CA8A9780-280D-11CF-A24D-444553540000"; nocase; content:".src";
distance:0; nocase; sid: 20038091; rev:1;)
```

SERVER SIDE ATTACKS

```
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET $HTTP_PORTS (
msg:"IPv6.URIParsing.Apache.2.Buffer.Overflow"; flow:to_server; content:"http://"; nocase;
content:"["; content:"HTTP"; reference:cve,CVE-2004-0786; sid: 20040732; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET 42 ( msg:"NameValidation.Windows.WINS.Buffer.Overflow";
flow:to_server; content:"| 00 00 78 00 |"; content:"| 05 37 1e f8 |"; content:"| 00 00 00 00
|"; content:"| 00 00 00 06 |"; dsiz: 52; reference:cve,CVE-2004-0567; sid: 20040701; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET 119 ( msg:"XPAT.NNTP.MicrosoftIIS.Buffer.Overflow";
flow:to_server; content:"XPAT"; nocase; content:"!| 0d 0a |"; within:300; reference:cve,CVE-
2004-0574; sid: 20040702; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET 9950 (
msg:"wsdel.SearchService.ColdFusionMX7.Buffer.Overflow"; flow:to_server; content:"wsdel";
nocase; content:"!| 0d 0a |"; within:300; reference:cve,; sid: 20040642; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET 6003 ( msg:"POST.Request.OracleOPMN.Format.String";
flow:to_server; content:"POST"; nocase; content:"%"; content:"%"; content:"HTTP"; nocase;
reference:cve,; sid: 20040633; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET 3050 (
msg:"isc_attach_database.FirebirdDatabase.Buffer.Overflow"; content:"| 00 00 00 13 00 00 00 00
00 00 42 f4 |"; offset:0; depth:14; reference:cve,; sid: 20040566; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET 3050 (
msg:"PWD_db_aliased.BorlandInterbase.Buffer.Overflow"; flow:to_server; content:"| 00 00 00 13 00
00 00 00 00 04 80 |"; offset:0; depth:14; reference:cve,; sid: 20040562; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET 21 ( msg:"NLST.SMBDirList.smbftpd.Format.String";
flow:to_server; content:"NLST"; nocase; content:"%"; content:"%"; content:"%";
content:"%"; reference:cve,; sid: 20040470; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET 9999 ( msg:"database.webdbm.MaxDB.StackOverflow";
flow:to_server; uricontent:"/webdbm"; nocase; content:"Database="; nocase; content:"!| 26 |";
within: 70; reference:cve,CVE-2006-4305; sid: 20040058; rev:1;)
Alert UDP $EXTERNAL_NET ANY -> $HOME_NET 407 (
msg:"HELLO.UDP.MotorolaTimbuktoPro.Buffer.Overflow"; content:"| 00 01 6b 00 00 b0 00 23 07 22 03
07 d6 69 6d 3b 27 a8 d0 f2 d6 69 6d 3b 27 a8 d0 f2 00 09 01 41 |"; content:"| 01 97 01 41 |";
distance:52; within:60; content:"| 01 02 00 04 b7 1d bf 42 00 00 00 00 7f 00 00 01 |";
distance:60; within:80; reference:cve,; sid: 20040407; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET 139 ( msg:"CanonicalizePathName.Win32.MS06-
40.StackOverflow"; content:"|ff|SMB|25 00 00 00 00|"; content:"|00 40|"; distance:0;
content:"|1f 00 00 00 00 00|"; distance:0; sid: 20031286;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET 21311 (
msg:"application.POST.DellOpenManage.Heap.Overflow"; content:"POST"; nocase;
content:"application="; nocase; content:"!|HTTP"; within:150; nocase; reference:cve,CVE-
2004-0331; sid: 20040067; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET 143 ( msg:"Search.IMAPD.Mercury.Stack.Overflow";
flow:to_server; content:"SEARCH ON"; nocase; content:"!| 0d 0a |"; within:300;
reference:cve,; sid: 20040333; rev:1;)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC CISCO VoIP DOS ATTEMPT";
flow:to_server,established; uricontent:"/StreamingStatistics"; reference:bugtraq,4794;
reference:cve,2002-0882; reference:nessus,11013; classtype:misc-attack; sid:1814; rev:8;)
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 445 (msg:"MS-SQL.xp_cmdshell.program.execution";
flow:to_server,established; content:"x|00|p|00|_|00|c|00|m|00|d|00|s|00|h|00|e|00|i|00|i|00|";
nocase; classtype:attempted-user; sid:1759; rev:5;)
```


MALWARE

```
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET ANY ( msg:"nginx.header.Storm.Worm.Attempt";
flow:to_client; content:"Server:"; content:"nginx/0.5.17"; reference:cve,; sid: 20040582;
rev:1;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 139 (msg: "Zotob.Infection.Attempt.Worm"; content: "| ff
|SMB"; content: "| 03 00 23 82 0c |W| 03 82 04 0a 00 90 |B| 90 |B| 90 |B| 81 c4 |T| f2 ff
ff fc e8 |F| 00 00 00 8b |E| 3c 8b 7c 05 |x| 01 ef 8b |O| 18 8b 5f | | 01 eb e3 |.I| 8b |4| 8b 01
ee |1| c0 99 ac 84 c0 |t| 07 c1 ca 0d 01 c2 eb f4 3b |T| 24 04 |u| e3 8b 5f 24 01 eb |f| 8b 0c
|K"; content: "echo get eraseme"; classtype:misc-activity; sid:20010384; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET 1434 ( msg:"Slammer Worm Propagation"; content:"|04|";
depth:1; content:"|81 F1 03 01 04 9B 81 F1 01|"; distance:0; content:"sock"; distance:0;
nocase; content:"send"; distance:0; nocase; sid: 20038627; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET 80 ( msg:"FP30REG.ELF.WORM"; content:"POST| 20|";
uricontent:"| 2f 5f |vti| 5f |bin| 2f 5f |vti| 5f |aut/fp30reg.dll"; uricontent:"| f1 99 c9 99
c9 9c 99 c9 |f,| aa 98 99 c9 99 c9 99 |q| f0 99 c9 99 c9 99 c9 fb b0 b8 83 c3 cb |f,| aa 98 99 c9
99 c9 |f,| be 98 99 c9 99 c9 |q| e3 99 c9 99 c9 99 c9 9b 9c c2 e7 |f,| be 98 99 c9 99 c9 |q| f2
99 c9 99 c9 99 c9 1a 1f 03 a4 14 04 b2 98 99 c9 99 c9 ca |q| c2 99 c9 99 c9 99 c9 bf 19 |5Qq| cb
99 c9 99 c9 99 c9 f9 3b 13 ef f9 29 |7| a1 9e ed 9a de |r| 60 5f 9e 99 c9 f8 |Z| d5 a9 99 c9 99
c9 99 c9 99 c9 99 c9 f5 ea fd b7 fd f5 f5 |"; distance:0; sid: 20013535;)
Alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg: "NIMDA.P7.WORM"; flow:to_server,
established; uricontent: "| 2f |winnt| 2f |system32| 2f |cmd.exe| 3f 2f |c| 2b |dir";
classtype:misc-activity; sid:20010208; rev: 1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET 2967:2968 ( msg:"SAVRT.SYMANTEC.EXPLOIT"; content:"| 01
10 0f 20 0a 00 00 00 02 18 00 01 00 00 00 00 00 24 00 14 b7 c9 d2 d9 3e |3| ef |4%| 1f |C| 00 02
02 5c 2f |"; depth:36; sid: 20030884;)
Alert tcp $EXTERNAL_NET any -> $HOME_NET !135 (msg: "SDBOT.P2.B.BACKDOOR"; flow:to_server,
established; content: "C| 00 24 00 5c 00 |1| 00 |2| 00 |3| 00 |4| 00 |5| 00 |6| 00 |1| 00 |1| 00
|1| 00 |1| 00 |1| 00 |1| 00 |1| 00 |1| 00 |1| 00 |1| 00 |1| 00 |1| 00 |1| 00 |1| 00 |1| 00 |.
| 00 |d| 00 |o| 00 |c"; classtype:misc-activity; sid:20010102; rev: 1;)
Alert tcp $EXTERNAL_NET any -> $HOME_NET 2745 (msg: "AGOBOT GET"; flow:to_server, established;
content: "ftp| 3a |//bla| 3a |bla"; content: "| 3a |21246/bot.exe| 00 |"; within: 20;
classtype:misc-activity; sid:20010012; rev: 1;)
Alert tcp $EXTERNAL_NET any -> $HOME_NET 4444 (msg: "TEEKIDS START"; flow:to_server, established;
content: "start teekids.exe| 0a |"; classtype:misc-activity; sid:20010013; rev: 1;)
Alert tcp $EXTERNAL_NET any -> $HOME_NET 2745 (msg: "BAGLE.GETBOT.WORM"; flow:to_server,
established; content:"ftp| 3a |//bla| 3a |bla| 40 |"; content:"/bot.exe| 00 |"; within: 36;
classtype:misc-activity; sid:20010100; rev:1;)
Alert tcp $EXTERNAL_NET any -> $HOME_NET 4444 (msg: "MSBLASTER GET"; flow:to_server, established;
content: "tftp | 2d |"; content: "GET msblast.exe| 0a |"; within: 20; classtype:misc-activity;
sid:20010005; rev: 1;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 2745 (msg:"BAGLE.ATTEMPTCONNECT.A2745.BACKDOOR";
flow:to_server,established; content:"C| ff ff ff |000| 01 0a 28 91 a1 2b e6 |`/2| 8f |`| 15 1a |
| 1a 00 |"; nocase; classtype:misc-activity; sid:20010064; rev:1;)
Alert tcp $EXTERNAL_NET any -> $HOME_NET 4444 (msg: "ENBIEI.START.A.WORM"; flow:to_server,
established; content: "start enbiei.exe | 0a |"; depth: 19; classtype:misc-activity;
sid:20010077; rev: 1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET 445 ( msg:"Sdranck.Y.Trojan"; content: "| 8a 00 00 02
|k| b3 9f |k| 60 8d |94| 1d |3| 0a 00 | | 00 00 00 |ciaraf.exe| 00 f0 ee 97 |y| 0c 18 cc c0 11
|Y| 95 0c 19 15 |k| 3b |j| b1 26 ab fb aa c1 9a ac 3b 05 cd ee |X| df de fe |o| e8 26 e4 be 81 9c
|H0| ca |e| a4 c3 |H"; sid: 20010618;)
```

WEB APPLICATION ATTACKS

```
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET $HTTP_PORTS (msg:"URL.SETUP.PHPMYADMIN.XSS.B";
uricontent:"| 2F |setup.php| 3F |"; uricontent:"<"; distance: 0; uricontent:"javascript:";
nocase; distance: 0; uricontent:">"; distance: 0; reference:cve,CVE-2007-5386 ; sid:20040660;
rev:1;)

Alert TCP $EXTERNAL_NET ANY -> $HOME_NET 7001 ( msg:"BEA.WEBLOGIC.ADMINCONSOLE.XSS";
uricontent:"console"; nocase; uricontent:"a"; nocase; uricontent: "script"; nocase;
reference:cve,2005-1747; sid: 20040127; rev:1;)

Alert TCP $EXTERNAL_NET ANY -> $HOME_NET $HTTP_PORTS
(msg:"RWSERVLET.DELIMITER.ORACLEREPORTS.XSS.C"; uricontent:"| 2F |rwservlet| 3F |";
uricontent:"delimiter| 3D |"; nocase; distance: 0; uricontent:"<"; distance: 0;
uricontent:"vbscript:"; nocase; distance: 0; uricontent:">"; distance: 0; sid:20039192; rev:1;)

Alert TCP $EXTERNAL_NET ANY -> $HOME_NET $HTTP_PORTS (msg:"SHOWENV.DEBUG.ORACLEREPORTS.XSS.B";
uricontent:"| 2F |showenv| 3F |"; uricontent:"debug| 3D |"; nocase; distance: 0; uricontent:"<";
distance: 0; uricontent:"javascript:"; nocase; distance: 0; uricontent:">"; distance: 0;
sid:20039185; rev:1;)

Alert TCP $EXTERNAL_NET ANY -> $HOME_NET $HTTP_PORTS
(msg:"SEARCH.Q.GOOGLE_CUSTOM_SEARCH_ENGINE.XSS.C"; uricontent:"| 2F |search.php| 3F |";
uricontent:"q| 3D |"; nocase; distance: 0; uricontent:"<"; distance: 0; uricontent:"vbscript:";
nocase; distance: 0; uricontent:">"; distance: 0; reference:cve,CVE-2007-3484; sid:20039080;
rev:1;)

Alert TCP $EXTERNAL_NET ANY -> $HOME_NET $HTTP_PORTS (msg:"PAM_LOGIN.CID.WEBMIN.XSS.B";
uricontent:"| 2F |pam_login.cgi| 3F |"; uricontent:"cid| 3D |"; nocase; distance: 0;
uricontent:"<"; distance: 0; uricontent:"javascript:"; nocase; distance: 0; uricontent:">";
distance: 0; reference:cve,CVE-2007-3156; sid:20038729; rev:1;)

Alert TCP $EXTERNAL_NET ANY -> $HOME_NET $HTTP_PORTS (msg:"ADMIN.TK.3COM_OFFICECONNECT.XSS.C";
uricontent:"| 2F |cgi-bin| 2F |admin| 3F |"; uricontent:"tk| 3D |"; nocase; distance: 0;
uricontent:"<"; distance: 0; uricontent:"vbscript:"; nocase; distance: 0; uricontent:">";
distance: 0; reference:cve,CVE-2006-3974; sid:20038739; rev:1;)

Alert TCP $EXTERNAL_NET ANY -> $HOME_NET $HTTP_PORTS (msg:"WGATE.SERVICE.SAP_ITS.XSS.B";
uricontent:"| 2F |scripts| 2F |wgate.dll| 3F |"; uricontent:"service| 3D |"; nocase; distance:
0; uricontent:"<"; distance: 0; uricontent:"javascript:"; nocase; distance: 0; uricontent:">";
distance: 0; reference:cve,CVE-2003-0749; sid:20025930; rev:1;)

Alert TCP $EXTERNAL_NET ANY -> $HOME_NET $HTTP_PORTS (msg:"POLLID.POLLWINDOW.JOOMLA.ASCII.SQL-
INJECTION"; uricontent:"| 2F |pollwindow.php| 3F |"; uricontent:"pollid| 3D |"; distance:0;
uricontent:"ascii(substring((SELECT"; nocase; distance: 0; uricontent:"FROM"; distance: 0;
reference:cve,CVE-; sid:20040413; rev:1;)

Alert TCP $EXTERNAL_NET ANY -> $HOME_NET $HTTP_PORTS (msg:"LANG.LOGON.CISCOCALLMANAGER.ASCII.SQL-
INJECTION"; uricontent:"| 2F |CCMUser| 2F |logon.asp| 3F |"; uricontent:"lang| 3D |"; distance:0;
uricontent:"ascii(substring((SELECT"; nocase; distance: 0; uricontent:"FROM"; distance: 0;
reference:cve,CVE-; sid:20040176; rev:1;)

Alert TCP $EXTERNAL_NET ANY -> $HOME_NET $HTTP_PORTS
(msg:"BB_FUNCTIONS.PATHTOFILES.MINIBB.PHP.INCLUSION"; uricontent:"| 2F |bb_functions.php| 3F |";
uricontent:"pathToFiles| 3D |"; distance:0; reference:cve,CVE-2006-5674; sid:20026062; rev:1;)

Alert TCP $EXTERNAL_NET ANY -> $HOME_NET $HTTP_PORTS (msg:"FN.VIEWER.WEBSHELL4.FILE.DISCLOSURE";
uricontent:"| 2F |viewer.php| 3F |"; uricontent:"fn| 3D |"; distance:0; reference:cve,CVE-;
sid:20040643; rev:1;)

Alert TCP $EXTERNAL_NET ANY -> $HOME_NET $HTTP_PORTS (msg:"LAST_MODULE.ADODB-PERF-
MODULE.INC.CMSMADESIMPLE.PHP.INJECTION"; uricontent:"| 2F |adodb-perf-module.inc.php| 3F |";
uricontent:"last_module| 3D |"; distance:0; reference:cve,CVE-; sid:20040375; rev:1;)

Alert TCP $EXTERNAL_NET ANY -> $HOME_NET $HTTP_PORTS (msg:"FILE.SHOW.HELPLINK.FILE.INCLUSION";
uricontent:"| 2F |show.php| 3F |"; uricontent:"file| 3D |"; distance:0; reference:cve,CVE-;
sid:20040355; rev:1;)

Alert TCP $EXTERNAL_NET ANY -> $HOME_NET $HTTP_PORTS
(msg:"PATH_TO_ROOT.LOGIN.FRONTACCOUNTING.FILE.INCLUSION"; uricontent:"| 2F |login.php| 3F |";
uricontent:"path_to_root| 3D |"; distance:0; reference:cve,CVE-; sid:20040405; rev:1;)

Alert TCP $EXTERNAL_NET ANY -> $HOME_NET $HTTP_PORTS
(msg:"OPENID_ROOT_PATH.BBSTORE.PHPBB.OPENIDMOD.FILE.INCLUSION"; uricontent:"| 2F |BBStore.php| 3F
|"; uricontent:"openid_root_path| 3D |"; distance:0; reference:cve,CVE-; sid:20040447; rev:1;)

Alert TCP $EXTERNAL_NET ANY -> $HOME_NET ANY (msg:"XML.xmlrpc.php.Injection"; content: "POST
/xmlrpc.php HTTP/1.1| 0a |"; content: "| 3c 3f |xml version| 3d 22 |1.0| 22 3f 3e 3c |methodCall|
3e 3c |methodName| 3e |test.method| 3c |/methodName| 3e 3c |params| 3e 3c |param| 3e 3c |value|
3e 3c |name| 3e3c 3f |xml version| 3d 22 |1.0| 22 3f 3e 3c |methodCall| 3e 3c |methodName| 3e
|test.method| 3c |/methodName| 3e 3c |params| 3e 3c |param| 3e 3c |value| 3e 3c |name| 3e|";
sid: 20010472; rev: 1; classtype: misc-activity; )

Alert TCP $EXTERNAL_NET ANY -> $HOME_NET $HTTP_PORTS (msg:"ID.TNEWS.BBPORTALS.ASCII.SQL-
INJECTION"; uricontent:"| 2F |tnews.php| 3F |"; uricontent:"id| 3D |"; distance:0;
uricontent:"ascii(substring((SELECT"; nocase; distance: 0; uricontent:"FROM"; distance: 0;
reference:cve,CVE-; sid:20040727; rev:1;)
```

PROTOCOLS & POLICY

```
Alert TCP $HOME_NET ANY -> $EXTERNAL_NET 1863 ( msg:"USR.Request.MSN.Messenger8.Policy";
flow:to_server; content:"USR"; nocase; reference:cve,; sid: 20040630; rev:1;)
Alert TCP $HOME_NET ANY -> $EXTERNAL_NET 1863 ( msg:"CVR.Request.MSN.Messenger8.Policy";
flow:to_server; content:"CVR"; nocase; reference:cve,; sid: 20040628; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET 8000 ( msg:"TCP.Logon.QQ.P2P.Policy"; content:"| 02 01
00 00 00 38 00 00 |"; offset: 0; depth: 12; content:"| 03 |"; reference:cve,; sid: 20040744;
rev:1;)
Alert TCP $HOME_NET ANY -> $EXTERNAL_NET 80 ( msg:"adtask.GETRequest.Xunlei.Thunder.P2P.Policy";
flow:to_server; content:"GET /bd/thunder5/show/adtask.xml HTTP/1.1"; nocase; content:"User-Agent:
InetURL/1.1"; nocase; reference:cve,; sid: 20040704; rev:1;)
Alert TCP $HOME_NET ANY -> $EXTERNAL_NET 3076 ( msg:"SYNC.Xunlei.P2P.Policy.A"; content:"| 02 00
02 00 01 00 00 00 1c 00 |"; offset:0; depth:10; content:"| 53 59 4e 43 |"; distance:4;
reference:cve,; sid: 20040705; rev:1;)
Alert TCP $HOME_NET ANY -> $EXTERNAL_NET ANY ( msg:"Connection.Attempt.Ares.P2P.Policy";
content:"| 03 00 5a 06 06 05 |"; offset:0; depth:6; reference:cve,; sid: 20040186; rev:1;)
Alert TCP $HOME_NET ANY -> $EXTERNAL_NET 80 ( msg:"GET.request.Ares.P2P.Policy"; content:"GET
/ares/home3.php?ver"; nocase; content:"Host: www.aresgalaxy.org"; nocase; reference:cve,; sid:
20040187; rev:1;)
Alert UDP $EXTERNAL_NET ANY -> $HOME_NET 7201 ( msg:"PPSTREAM.UDP.POLICY"; content:"|08 00 00
00|"; depth:4; reference:cve,; sid: 20040280; rev:1;)
Alert UDP $EXTERNAL_NET ANY -> $HOME_NET 8000 ( msg:"PPLIVE.PEER.POLICY"; content:"|e9 03 02 01
98|"; reference:cve,; sid: 20040278; rev:1;)
Alert TCP $HOME_NET ANY -> $EXTERNAL_NET 411 ( msg:"Command.DirectConnect.Protocol.Policy";
flow:to_server; content:"| 7c |"; reference:cve,; sid: 20040192; rev:1;)
Alert TCP $EXTERNAL_NET ANY <> $HOME_NET ANY ( msg:"Handshake.DirectConnect.Protocol.Policy.A";
content:"| 24 |MyNick"; nocase; content:"| 24 |Lock"; nocase; reference:cve,; sid:
20040194; rev:1;)
Alert TCP $HOME_NET ANY -> $EXTERNAL_NET ANY ( msg:"Login.Request.Skype.Policy"; flow:to_server;
content:"| 16 03 01 00 00 |"; reference:cve,; sid: 20040191; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET ANY ( msg:"Login.Response.Skype.Policy";
flow:to_client; content:"| 17 03 01 00 00 |"; reference:cve,; sid: 20040190; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET ANY ( msg:"WinMX.Request.policy"; flow:to_server;
content:"GET"; depth:3; nocase; content:"/mainbar/"; within:20; nocase;
content:"HTTP/1.1"; within:20; nocase; content:"Host: www.winmx.com"; distance:0; nocase;
sid: 20037970; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET 1024:65535 ( msg:"ICQ.IM.HANDSHAKE.GENERAL.POLICY";
content:"| 2a 01 |"; depth:2; content:"| 49 43 51 42 61 73 69 63 |"; distance:0; sid:
20037775; rev:1;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET 4000 ( msg:"EMULE.CONNECT.GENERIC.POLICY";
flow:to_server; content:"| e3 |"; depth:1; content:"| 03 01 00 11 3c 00 00 00 03 01 00 f9 |";
distance:0; sid: 20029113;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET ANY ( msg:"GNUTELLA.SERVERSIDE.SERVER.POLICY";
flow:to_client; content:"Server:| 20 |Gnutella"; nocase; sid: 20037352;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET 5190:5193 ( msg:"AIM.IM.GENERAL.HANDSHAKE.POLICY";
flow:to_server; content:"| 2a 02 |"; within:2; content:"| 41 4f 4c 20 49 6e 73 74 61 6e 74 20
4d 65 73 73 65 6e 67 65 72 2c |"; distance:0; sid: 20037766;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET ANY ( msg:"SOCKS.V5.DISCOVERY"; content: "| 05 01 02 |";
dsize: 3; sid: 20010557;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET ANY ( msg:"Google.IM.GENERAL.HANDSHAKE.POLICY";
flow:to_server; content:"| 48 6f 73 74 3a 20 6d 61 69 6c 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 0d 0a
|"; content:"| 0d 0a 43 6f 6f 6b 69 65 3a 20 67 6d 61 69 6c 63 68 61 74 |"; distance:0; sid:
20037768;)
Alert TCP $EXTERNAL_NET ANY -> $HOME_NET ANY ( msg:"MORPHEUS.GNUTELLA.REQUEST.POLICY";
flow:to_server; content:"GNUTELLA CONNECT"; depth:16; nocase; content:"X-Ultrapeer";
distance:0; nocase; sid: 20037300;)
```