

Fake yellow bar and web page redirecting

Posted by Cubster - 2007/12/09 20:51

Please help!!!

When I go on the internet I get a fake yellow bar stating "Warning: possible spyware or adware infection! Click here to scan your

computer for spyware and adware. . ." Also, my webpage redirects to the following website without me wanting it to: "http://directnameservice.com/r.php?sid=0&pn=&said=0&aid=0"

Below is my FreeFixer Log. Thanks in advance for all your help!!!

FreeFixer v0.25 log

http://www.freefixer.com/

Operating system: Windows XP Service Pack 2

Log dated 2007-12-09 11:29

Winlogon Notify (9 whitelisted)

!SASWinLogon - C:\Program Files\SUPERAntiSpyware\SASWINLO.dll

igfxcui - C:\WINDOWS\system32\igfxdev.dll

WgaLogon - C:\WINDOWS\system32\WgaLogon.dll

WRNotifier - C:\WINDOWS\system32\WRLogonNTF.dll

Browser Helper Objects

{02478D38-C3F9-4EFB-9B51-7695ECA05670}, Yahoo! Toolbar Helper, C:\Program Files\Yahoo!\Companion\Installs\cpn\yt.dll

{0579B4B1-0293-4d73-B02D-5EBB0BA0F0A2}, Ask Search Assistant BHO, C:\Program Files\AskSBar\SrchAsth\1.bin\A2SRCHAS.DLL

{06849E9F-C8D7-4D59-B87D-784B7D6BE0B3}, AcroIEHlprObj Class, C:\Program Files\Adobe\Acrobat 7.0\ActiveX\AcroIEHelper.dll

{5CA3D70E-1895-11CF-8E15-001234567890}, DriveLetterAccess, C:\WINDOWS\system32\dla\tfswshx.dll

{602ADB0E-4AFF-4217-8AA1-95DAC4DFA408}, , C:\Program Files\Common Files\Symantec Shared\coShared\Browser\2.0\colEPIg.dll

{6D53EC84-6AAE-4787-AEEE-F4628F01010C}, Symantec Intrusion Prevention, C:\PROGRA~1\COMMON~1\SYMANT~1\IDS\IPSBHO.dll

{AA58ED58-01DD-4d91-8333-CF10577473F7}, Google Toolbar Helper, c:\program files\google\googletoolbar1.dll

{CFF8726A-9262-441C-8163-C6371E9EDE47}, MSVPS System, C:\WINDOWS\advrepnok.dll

{F0D4B231-DA4B-4daf-81E4-DFEE4931A4AA}, Ask Toolbar BHO, C:\Program Files\AskSBar\bar\1.bin\ASKSBAR.DLL

Internet Explorer toolbars (2 whitelisted)

HKLM\...\Toolbar\{EF99BD32-C1FB-11D2-892F-0090271D4F88} - Yahoo! Toolbar - C:\Program Files\Yahoo!\Companion\Installs\cpn\yt.dll

HKLM\...\Toolbar\{16A0662E-AC21-4AD9-89E8-7495AC5ACE93} - The sdrmod - C:\WINDOWS\sdrmod.dll(file is missing)

HKLM\...\Toolbar\{2318C2B1-4965-11d4-9B18-009027A5CD4F} - &Google - c:\program files\google\googletoolbar1.dll

HKLM\...\Toolbar\{F0D4B239-DA4B-4daf-81E4-DFEE4931A4AA} - Ask Toolbar - C:\Program

Files\AskSBar\bar\1.bin\ASKSBAR.DLL

HKLM\...\Toolbar\{7FEBEFE3-6B19-4349-98D2-FFB09D4B49CA} - Show Norton Toolbar - C:\Program Files\Common Files\Symantec Shared\coShared\Browser\2.0\ColEPIg.dll

HKCU\...\Toolbar\ShellBrowser\{C4069E3A-68F1-403E-B40E-20066696354B} - - No file specified

HKCU\...\Toolbar\WebBrowser\{0B53EAC3-8D69-4B9E-9B19-A37C9A5676A7} - - No file specified

Basic Internet Explorer settings

HKCU\...\Main, Start Page = http://www.foxnews.com/

HKLM\...\Main, Start Page = http://www.dell4me.com/myway

HKLM\...\Main, Search Page = http://go.microsoft.com/fwlink/?LinkId=54896

HKLM\...\Main, Default_Page_URL = http://go.microsoft.com/fwlink/?LinkId=69157

HKLM\...\Main, Default_Search_URL = http://go.microsoft.com/fwlink/?LinkId=54896

Registry Startups (1 whitelisted)

HKLM\...\Run, SynTPEnh = "C:\Program Files\Synaptics\SynTP\SynTPEnh.exe"

HKLM\...\Run, igfxtray = C:\WINDOWS\system32\igfxtray.exe

HKLM\...\Run, igfxhkcmd = C:\WINDOWS\system32\hkcmd.exe

HKLM\...\Run, igfxpers = C:\WINDOWS\system32\igfxpers.exe

HKLM\...\Run, SunJavaUpdateSched = "C:\Program Files\Java\j2re1.4.2_03\bin\jusched.exe"
HKLM\...\Run, SigmateSysTrayApp = stsysra.exe
HKLM\...\Run, Dell Wireless Manager UI = C:\WINDOWS\system32\WLTRAY
HKLM\...\Run, Dell QuickSet = "C:\Program Files\Dell\QuickSet\quickset.exe"
HKLM\...\Run, DVDLauncher = "C:\Program Files\CyberLink\PowerDVD\DVDLauncher.exe"
HKLM\...\Run, MMTray = "C:\Program Files\Musicmatch\Musicmatch Jukebox\mm_tray.exe"
HKLM\...\Run, mmtask = "C:\Program Files\Musicmatch\Musicmatch Jukebox\mmtask.exe"
HKLM\...\Run, RealTray = "C:\Program Files\Real\RealPlayer\RealPlay.exe" SYSTEMBOOTHIDEPLAYER
HKLM\...\Run, dla = C:\WINDOWS\system32\dla\tfswctrl.exe
HKLM\...\Run, ISUSPM Startup = "C:\PROGRA~1\COMMON~1\INSTAL~1\UPDATE~1\ISUSPM.exe" -startup
HKLM\...\Run, ISUSScheduler = "C:\Program Files\Common Files\InstallShield\UpdateService\issch.exe" -start
HKLM\...\Run, DMXLauncher = "C:\Program Files\Dell\Media Experience\DMXLauncher.exe"
HKLM\...\Run, QuickTime Task = "C:\Program Files\QuickTime\qttask.exe" -atboottime
HKLM\...\Run, iTunesHelper = "C:\Program Files\iTunes\iTunesHelper.exe"
HKLM\...\Run, HP Software Update = "C:\Program Files\HP\HP Software Update\HPWuSchd2.exe"
HKLM\...\Run, HP Component Manager = "C:\Program Files\HP\hpcoretech\hpcmpmgr.exe"
HKLM\...\Run, Gearbox = "C:\Program Files\Gearbox Connection Kit\bin\confsvr.exe"
HKLM\...\Run, ccApp = "C:\Program Files\Common Files\Symantec Shared\ccApp.exe"
HKLM\...\Run, osCheck = "C:\Program Files\Norton Internet Security\osCheck.exe"
HKLM\...\Run, SpySweeper = C:\Program Files\Webroot\Spy Sweeper\SpySweeperUI.exe /startintray
HKLM\...\RunServices, Gearbox Deferal Check = "C:\Program Files\Gearbox Connection Kit\bin\gbdefer.exe"
HKCU\...\Run, ModemOnHold = "C:\Program Files\NetWaiting\netWaiting.exe"
HKCU\...\Run, MSMSGs = "C:\Program Files\Messenger\msmsgs.exe" /background
HKCU\...\Run, DellSupport = "C:\Program Files\DellSupport\DSAgnt.exe" /startup
HKCU\...\Run, SUPERAntiSpyware = C:\Program Files\SUPERAntiSpyware\SUPERAntiSpyware.exe

Autostart shortcuts

Adobe Reader Speed Launch.Ink, , C:\Program Files\Adobe\Acrobat 7.0\Reader\reader_sl.exe
America Online 9.0 Tray Icon.Ink, America Online 9.0 Tray Icon, C:\Program Files\America Online 9.0\altray.exe
Digital Line Detect.Ink, , C:\Program Files\Digital Line Detect\DLG.exe
HP Digital Imaging Monitor.Ink, , C:\Program Files\HP\Digital Imaging\bin\hpqtra08.exe
HP Image Zone Fast Start.Ink, , C:\Program Files\HP\Digital Imaging\bin\hpqthb08.exe
ImationFlashDetect.Ink, ImationFlashDetect Application, C:\Program Files\Imation\ImationFlashDetect.exe

Processes (18 whitelisted)

C:\Program Files\Common Files\Symantec Shared\ccSvcHst.exe
C:\Program Files\Common Files\Symantec Shared\CCPD-LC\symclscv.exe
C:\WINDOWS\System32\wltrysvc.exe
C:\WINDOWS\System32\bcmwltry.exe
C:\PROGRA~1\COMMON~1\AOL\ACS\AOLacsd.exe
C:\Program Files\Symantec\LiveUpdate\AluSchedulerSvc.exe
C:\Program Files\Dell\NICCONFIGSVC\NICCONFIGSVC.exe
C:\WINDOWS\system32\wdfmgr.exe
C:\Program Files\Webroot\Spy Sweeper\SpySweeper.exe
C:\Program Files\Synaptics\SynTP\SynTPEnh.exe
C:\WINDOWS\system32\hkcmd.exe
C:\WINDOWS\system32\igfxpers.exe
C:\Program Files\Java\j2re1.4.2_03\bin\jusched.exe
C:\WINDOWS\stsysra.exe
C:\WINDOWS\system32\WLTRAY.exe
C:\Program Files\Dell\QuickSet\quickset.exe
C:\Program Files\CyberLink\PowerDVD\DVDLauncher.exe
C:\Program Files\Musicmatch\Musicmatch Jukebox\mm_tray.exe
C:\Program Files\Musicmatch\Musicmatch Jukebox\mmtask.exe
C:\Program Files\Real\RealPlayer\RealPlay.exe
C:\WINDOWS\system32\dla\tfswctrl.exe
C:\Program Files\Common Files\InstallShield\UpdateService\issch.exe
C:\Program Files\Dell\Media Experience\DMXLauncher.exe
C:\Program Files\QuickTime\qttask.exe
C:\Program Files\iTunes\iTunesHelper.exe
C:\Program Files\HP\HP Software Update\HPWuSchd2.exe
C:\Program Files\HP\hpcoretech\hpcmpmgr.exe
C:\Program Files\Gearbox Connection Kit\bin\confsvr.exe
C:\WINDOWS\system32\igfxsvc.exe
C:\Program Files\Common Files\Symantec Shared\ccSvcHst.exe

C:\Program Files\iPod\bin\iPodService.exe
C:\Program Files\Webroot\Spy Sweeper\SpySweeperUI.exe
C:\Program Files\NetWaiting\netWaiting.exe
C:\Program Files\Gearbox Connection Kit\bin\gbConMon.exe
C:\Program Files\Gearbox Connection Kit\bin\gbTask.exe
C:\Program Files\DellSupport\DSAgnnt.exe
C:\Program Files\Digital Line Detect\DLG.exe
C:\Program Files\HP\Digital Imaging\bin\hpqtra08.exe
C:\Program Files\Imation\ImationFlashDetect.exe
C:\Program Files\HP\Digital Imaging\bin\hpqgalry.exe
C:\Program Files\Webroot\Spy Sweeper\SSU.EXE
C:\Program Files\SUPERAntiSpyware\SUPERAntiSpyware.exe
C:\Program Files\FreeFixer\freefixer.exe

Application modules (47 whitelisted)

C:\WINDOWS\system32\ieframe.dll
C:\WINDOWS\system32\iertutil.dll
C:\WINDOWS\system32\Normaliz.dll

Services (35 whitelisted)

AOL ACS, AOL Connectivity Service, c:\progra~1\common~1\ao\acs\ao\acs.exe
Automatic LiveUpdate Scheduler, Automatic LiveUpdate Scheduler, c:\program files\symantec\liveupdate\aluschedulervc.exe
ccEvtMgr, Symantec Event Manager, c:\program files\common files\symantec shared\ccsvchst.exe
ccSetMgr, Symantec Settings Manager, c:\program files\common files\symantec shared\ccsvchst.exe
CLTNetCnService, Symantec Lic NetConnect service, c:\program files\common files\symantec shared\ccsvchst.exe
LiveUpdate Notice, LiveUpdate Notice, c:\program files\common files\symantec shared\ccsvchst.exe
NICCONFIGSVC, NICCONFIGSVC, c:\program files\dell\nicconfigsvc\nicconfigsvc.exe
Symantec Core LC, Symantec Core LC, c:\program files\common files\symantec shared\ccpd-1c\symlcsvc.exe
UMWdf, Windows User Mode Driver Framework, c:\windows\system32\wdfmgr.exe
WebrootSpySweeperService, Webroot Spy Sweeper Engine, c:\program files\webroot\spy sweeper\spysweeper.exe
wltrysvc, Dell Wireless WLAN Tray Service, c:\windows\system32\wltrysvc.exe

Drivers (26 whitelisted)

AegisP, AEGIS Protocol (IEEE 802.1x) v3.2.0.3, C:\WINDOWS\system32\drivers\aeagisp.sys
APPDRV, APPDRV, C:\WINDOWS\system32\drivers\appdrv.sys
CO_Mon, CO_Mon, c:\windows\system32\drivers\co_mon.sys
drvmcdb, , C:\WINDOWS\system32\drivers\drvmcdb.sys
dsunidrv, DellSupport UniDriver, C:\WINDOWS\system32\drivers\dsunidrv.sys
eeCtrl, Symantec Eraser Control driver, c:\program files\common files\symantec shared\engine\eectrl.sys
mdmxsdk, , C:\WINDOWS\system32\drivers\mdmxsdk.sys
PxHelp20, PxHelp20, C:\WINDOWS\system32\drivers\pxhelp20.sys
SASDIFSV, SASDIFSV, c:\program files\superantispyware\sasdifsv.sys
SASKUTIL, SASKUTIL, c:\program files\superantispyware\saskutil.sys
Secdrv, Secdrv, C:\WINDOWS\system32\drivers\secdrv.sys
SPBBCDrv, SPBBCDrv, c:\program files\common files\symantec shared\spbbc\spbbcdrv.sys
SRTSPX, SRTSPX, C:\WINDOWS\system32\drivers\srtsp.sys
SSFS0BB9, Spy Sweeper File System Filer Driver: 0BB9, C:\WINDOWS\system32\drivers\ssfs0bb9.sys
SSHRMD, Spy Sweeper Hookrack MiniDriver, C:\WINDOWS\system32\drivers\sshrmd.sys
SSIDRV, Spy Sweeper Interdiction Driver, C:\WINDOWS\system32\drivers\ssidrv.sys
symlcbdr, symlcbdr, c:\windows\system32\drivers\symlcbdr.sys
SYMTDI, SYMTDI, C:\WINDOWS\system32\drivers\symtdi.sys

=====
Re:Fake yellow bar and web page redirecting

Posted by freefixer - 2007/12/10 01:05

Hello Cubster

The following Browser Helper Object looks suspicious:

{CFF8726A-9262-441C-8163-C6371E9EDE47}, MSVPS System, C:\WINDOWS\advreprok.dll

Please scan it at <http://virusscan.jotti.org/>. If the file is detected as malware, please remove it using FreeFixer, restart your computer, scan your computer again and post a new FreeFixer log.

Please let us know if this fixed the issue with the fake yellow bar and the redirect.

Re:Fake yellow bar and web page redirecting

Posted by Cubster - 2007/12/11 00:19

Thanks for all your help. I removed the file and so far so good. My browser would usually redirect after about 10 seconds. I have now had it up for about 10 minutes and it has not redirected nor have I seen the annoying yellow bar.

Thanks again for all your help.

Below is my new Freefixer log.

FreeFixer v0.25 log
<http://www.freefixer.com/>
Operating system: Windows XP Service Pack 2
Log dated 2007-12-10 15:11

Winlogon Notify (9 whitelisted)
!SASWinLogon - C:\Program Files\SUPERAntiSpyware\SASWINLO.dll
WgaLogon - C:\WINDOWS\system32\WgaLogon.dll
WRNotifier - C:\WINDOWS\system32\WRLogonNTF.dll

Browser Helper Objects
{02478D38-C3F9-4EFB-9B51-7695ECA05670}, Yahoo! Toolbar Helper, C:\Program Files\Yahoo!\Companion\Installs\cpn\yt.dll
{0579B4B1-0293-4d73-B02D-5EBB0BA0F0A2}, Ask Search Assistant BHO, C:\Program Files\AskSBar\SrchAstt\1.bin\A2SRCHAS.DLL
{06849E9F-C8D7-4D59-B87D-784B7D6BE0B3}, AcroIEHlprObj Class, C:\Program Files\Adobe\Acrobat 7.0\ActiveX\AcroIEHelper.dll
{5CA3D70E-1895-11CF-8E15-001234567890}, DriveLetterAccess, C:\WINDOWS\system32\dla\tfswshx.dll
{602ADB0E-4AFF-4217-8AA1-95DAC4DFA408}, , C:\Program Files\Common Files\Symantec Shared\coShared\Browser\2.0\colEPIg.dll
{6D53EC84-6AAE-4787-AEEE-F4628F01010C}, Symantec Intrusion Prevention, C:\PROGRA~1\COMMON~1\SYMANT~1\IDS\IPSBHO.dll
{AA58ED58-01DD-4d91-8333-CF10577473F7}, Google Toolbar Helper, c:\program files\google\googletoolbar1.dll
{F0D4B231-DA4B-4daf-81E4-DFEE4931A4AA}, Ask Toolbar BHO, C:\Program Files\AskSBar\bar\1.bin\ASKSBAR.DLL

Internet Explorer toolbars (2 whitelisted)
HKLM\..\Toolbar\{EF99BD32-C1FB-11D2-892F-0090271D4F88} - Yahoo! Toolbar - C:\Program Files\Yahoo!\Companion\Installs\cpn\yt.dll
HKLM\..\Toolbar\{16A0662E-AC21-4AD9-89E8-7495AC5ACE93} - The sdrmod - C:\WINDOWS\sdrmod.dll(file is missing)
HKLM\..\Toolbar\{2318C2B1-4965-11d4-9B18-009027A5CD4F} - &Google - c:\program files\google\googletoolbar1.dll
HKLM\..\Toolbar\{F0D4B239-DA4B-4daf-81E4-DFEE4931A4AA} - Ask Toolbar - C:\Program Files\AskSBar\bar\1.bin\ASKSBAR.DLL
HKLM\..\Toolbar\{7FEBEFE3-6B19-4349-98D2-FFB09D4B49CA} - Show Norton Toolbar - C:\Program Files\Common Files\Symantec Shared\coShared\Browser\2.0\ColEPIg.dll
HKCU\..\Toolbar\ShellBrowser\{C4069E3A-68F1-403E-B40E-20066696354B} - - No file specified
HKCU\..\Toolbar\WebBrowser\{0B53EAC3-8D69-4B9E-9B19-A37C9A5676A7} - - No file specified

Basic Internet Explorer settings
HKCU\..\Main, Start Page = <http://www.foxnews.com/>
HKLM\..\Main, Start Page = <http://www.dell4me.com/myway>
HKLM\..\Main, Search Page = <http://go.microsoft.com/fwlink/?LinkId=54896>
HKLM\..\Main, Default_Page_URL = <http://go.microsoft.com/fwlink/?LinkId=69157>
HKLM\..\Main, Default_Search_URL = <http://go.microsoft.com/fwlink/?LinkId=54896>

Registry Startups (1 whitelisted)
HKLM\..\Run, SynTPEnh = "C:\Program Files\Synaptics\SynTP\SynTPEnh.exe"

HKLM\...\Run, igfxtray = C:\WINDOWS\system32\igfxtray.exe
HKLM\...\Run, igfxhkcmd = C:\WINDOWS\system32\hkcmd.exe
HKLM\...\Run, igfxpers = C:\WINDOWS\system32\igfxpers.exe
HKLM\...\Run, SunJavaUpdateSched = "C:\Program Files\Java\j2re1.4.2_03\bin\jusched.exe"
HKLM\...\Run, Sigmate!SysTrayApp = stsysra.exe
HKLM\...\Run, Dell Wireless Manager UI = C:\WINDOWS\system32\WLTRAY
HKLM\...\Run, Dell QuickSet = "C:\Program Files\Dell\QuickSet\quickset.exe"
HKLM\...\Run, DVDLauncher = "C:\Program Files\CyberLink\PowerDVD\DVDLauncher.exe"
HKLM\...\Run, MMTray = "C:\Program Files\Musicmatch\Musicmatch Jukebox\mm_tray.exe"
HKLM\...\Run, mmtask = "C:\Program Files\Musicmatch\Musicmatch Jukebox\mmtask.exe"
HKLM\...\Run, RealTray = "C:\Program Files\Real\RealPlayer\RealPlay.exe" SYSTEMBOOTHIDEPLAYER
HKLM\...\Run, dla = C:\WINDOWS\system32\dla\tfswctrl.exe
HKLM\...\Run, ISUSPM Startup = "C:\PROGRA~1\COMMON~1\INSTAL~1\UPDATE~1\ISUSPM.exe" -startup
HKLM\...\Run, ISUSScheduler = "C:\Program Files\Common Files\InstallShield\UpdateService\issch.exe" -start
HKLM\...\Run, DMXLauncher = "C:\Program Files\Dell\Media Experience\DMXLauncher.exe"
HKLM\...\Run, QuickTime Task = "C:\Program Files\QuickTime\qttask.exe" -atboottime
HKLM\...\Run, iTunesHelper = "C:\Program Files\iTunes\iTunesHelper.exe"
HKLM\...\Run, HP Software Update = "C:\Program Files\HP\HP Software Update\HPWuSchd2.exe"
HKLM\...\Run, HP Component Manager = "C:\Program Files\HP\hpcoretech\hpcmpmgr.exe"
HKLM\...\Run, Gearbox = "C:\Program Files\Gearbox Connection Kit\bin\confsvr.exe"
HKLM\...\Run, ccApp = "C:\Program Files\Common Files\Symantec Shared\ccApp.exe"
HKLM\...\Run, osCheck = "C:\Program Files\Norton Internet Security\osCheck.exe"
HKLM\...\Run, SpyHunter Security Suite = "C:\Program Files\Enigma Software Group\SpyHunter\SpyHunter3.exe"
HKLM\...\Run, SpySweeper = "C:\Program Files\Webroot\Spy Sweeper\SpySweeperUI.exe" /startinray
HKLM\...\Run, Services, Gearbox Deferal Check = "C:\Program Files\Gearbox Connection Kit\bin\gbdefer.exe"
HKCU\...\Run, ModemOnHold = "C:\Program Files\NetWaiting\netWaiting.exe"
HKCU\...\Run, MSMSGs = "C:\Program Files\Messenger\msmsgs.exe" /background
HKCU\...\Run, DellSupport = "C:\Program Files\DellSupport\DSAgnnt.exe" /startup
HKCU\...\Run, SUPERAntiSpyware = "C:\Program Files\SUPERAntiSpyware\SUPERAntiSpyware.exe"

Autostart shortcuts

Adobe Reader Speed Launch.Ink, , C:\Program Files\Adobe\Acrobat 7.0\Reader\reader_sl.exe
America Online 9.0 Tray Icon.Ink, America Online 9.0 Tray Icon, C:\Program Files\America Online 9.0\ao!tray.exe
Digital Line Detect.Ink, , C:\Program Files\Digital Line Detect\DLG.exe
HP Digital Imaging Monitor.Ink, , C:\Program Files\HP\Digital Imaging\bin\hpqtra08.exe
HP Image Zone Fast Start.Ink, , C:\Program Files\HP\Digital Imaging\bin\hpqthb08.exe
ImationFlashDetect.Ink, ImationFlashDetect Application, C:\Program Files\Imation\ImationFlashDetect.exe

Processes (18 whitelisted)

C:\Program Files\Common Files\Symantec Shared\ccSvcHst.exe
C:\Program Files\Common Files\Symantec Shared\CCPD-LC\symclscvc.exe
C:\WINDOWS\System32\wltrysvc.exe
C:\WINDOWS\System32\bcmwltry.exe
C:\PROGRA~1\COMMON~1\AOL\ACS\AOLacsd.exe
C:\Program Files\Symantec\LiveUpdate\AluSchedulerSvc.exe
C:\Program Files\Dell\NICCONFIGSVC\NICCONFIGSVC.exe
C:\WINDOWS\system32\wdfmgr.exe
C:\Program Files\Webroot\Spy Sweeper\SpySweeper.exe
C:\Program Files\Synaptics\SynTP\SynTPEnh.exe
C:\WINDOWS\system32\hkcmd.exe
C:\WINDOWS\system32\igfxpers.exe
C:\Program Files\Java\j2re1.4.2_03\bin\jusched.exe
C:\WINDOWS\stsysra.exe
C:\WINDOWS\system32\WLTRAY.exe
C:\WINDOWS\system32\igfxsrv.exe
C:\Program Files\Dell\QuickSet\quickset.exe
C:\Program Files\CyberLink\PowerDVD\DVDLauncher.exe
C:\Program Files\Musicmatch\Musicmatch Jukebox\mm_tray.exe
C:\Program Files\Musicmatch\Musicmatch Jukebox\mmtask.exe
C:\Program Files\Real\RealPlayer\RealPlay.exe
C:\WINDOWS\system32\dla\tfswctrl.exe
C:\Program Files\Common Files\InstallShield\UpdateService\issch.exe
C:\Program Files\Dell\Media Experience\DMXLauncher.exe
C:\Program Files\QuickTime\qttask.exe
C:\Program Files\iTunes\iTunesHelper.exe

C:\Program Files\HP\HP Software Update\HPWuSchd2.exe
C:\Program Files\HP\hpcoretech\hpcmpmgr.exe
C:\Program Files\Gearbox Connection Kit\bin\confsvr.exe
C:\Program Files\Common Files\Symantec Shared\ccSvcHst.exe
C:\Program Files\Enigma Software Group\SpyHunter\SpyHunter3.exe
C:\Program Files\Webroot\Spy Sweeper\SpySweeperUI.exe
C:\Program Files\NetWaiting\netWaiting.exe
C:\Program Files\DellSupport\DSAgent.exe
C:\Program Files\SUPERAntiSpyware\SUPERAntiSpyware.exe
C:\Program Files\iPod\bin\iPodService.exe
C:\Program Files\Gearbox Connection Kit\bin\gbConMon.exe
C:\Program Files\Digital Line Detect\DLG.exe
C:\Program Files\Gearbox Connection Kit\bin\gbTask.exe
C:\Program Files\HP\Digital Imaging\bin\hpqtra08.exe
C:\Program Files\Imation\ImationFlashDetect.exe
C:\Program Files\HP\Digital Imaging\bin\hpqgalry.exe
C:\Program Files\FreeFixer\freefixer.exe

Application modules (47 whitelisted)

C:\Program Files\Enigma Software Group\SpyHunter\SpyHunterMonitor.dll
C:\WINDOWS\system32\ieframe.dll
C:\WINDOWS\system32\iertutil.dll
C:\WINDOWS\system32\Normaliz.dll

Services (35 whitelisted)

AOL ACS, AOL Connectivity Service, c:\progra~1\common~1\ao\acs\ao\acs.exe
Automatic LiveUpdate Scheduler, Automatic LiveUpdate Scheduler, c:\program files\symantec\liveupdate\aluschedulervc.exe
ccEvtMgr, Symantec Event Manager, c:\program files\common files\symantec shared\ccsvchst.exe
ccSetMgr, Symantec Settings Manager, c:\program files\common files\symantec shared\ccsvchst.exe
CLTNetCnService, Symantec Lic NetConnect service, c:\program files\common files\symantec shared\ccsvchst.exe
LiveUpdate Notice, LiveUpdate Notice, c:\program files\common files\symantec shared\ccsvchst.exe
NICCONFIGSVC, NICCONFIGSVC, c:\program files\dell\nicconfigsvc\nicconfigsvc.exe
Symantec Core LC, Symantec Core LC, c:\program files\common files\symantec shared\ccpd-1c\symlcsvc.exe
UMWdf, Windows User Mode Driver Framework, c:\windows\system32\wdfmgr.exe
WebrootSpySweeperService, Webroot Spy Sweeper Engine, c:\program files\webroot\spy sweeper\spysweeper.exe
wltrysvc, Dell Wireless WLAN Tray Service, c:\windows\system32\wltrysvc.exe

Drivers (26 whitelisted)

AegisP, AEGIS Protocol (IEEE 802.1x) v3.2.0.3, C:\WINDOWS\system32\drivers\aegisp.sys
APPDRV, APPDRV, C:\WINDOWS\system32\drivers\appdrv.sys
CO_Mon, CO_Mon, c:\windows\system32\drivers\co_mon.sys
drvmcdb, , C:\WINDOWS\system32\drivers\drvmcdb.sys
dsunidrv, DellSupport UniDriver, C:\WINDOWS\system32\drivers\dsunidrv.sys
eeCtrl, Symantec Eraser Control driver, c:\program files\common files\symantec shared\engine\eectrl.sys
mdmxsdk, , C:\WINDOWS\system32\drivers\mdmxsdk.sys
PxHelp20, PxHelp20, C:\WINDOWS\system32\drivers\pxhelp20.sys
SASDIFSV, SASDIFSV, c:\program files\superantispyware\sasdifsv.sys
SASKUTIL, SASKUTIL, c:\program files\superantispyware\saskutil.sys
Secdrv, Secdrv, C:\WINDOWS\system32\drivers\secdrv.sys
SPBBCDrv, SPBBCDrv, c:\program files\common files\symantec shared\spbbc\spbbcdrv.sys
SRTSPX, SRTSPX, C:\WINDOWS\system32\drivers\srtsp.sys
SSFS0BB9, Spy Sweeper File System Filer Driver: 0BB9, C:\WINDOWS\system32\drivers\ssfs0bb9.sys
SSHAMD, Spy Sweeper Hookrack MiniDriver, C:\WINDOWS\system32\drivers\sshcmd.sys
SSIDRV, Spy Sweeper Interdiction Driver, C:\WINDOWS\system32\drivers\ssidrv.sys
symlcbdr, symlcbdr, c:\windows\system32\drivers\symlcbdr.sys
SYMTDI, SYMTDI, C:\WINDOWS\system32\drivers\symtdi.sys

=====