

FF Log--Thanks

Posted by Beamer - 2009/02/02 21:20

FreeFixer v0.31 log

<http://www.freefixer.com/>

Operating system: Windows XP Service Pack 3

Log dated 2009-02-02 12:51

Suspicious file names

C:\WINDOWS\setup.exe

Winlogon Notify (10 whitelisted)

AtiExtEvent - C:\WINDOWS\system32\Ati2evxx.dll

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

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

Applnit_DLLs

C:\PROGRA~1\Google\GOOGLE~2\GOEC62~1.DLL -

Namespace service providers (3 whitelisted)

{B600E6E9-553B-4A19-8696-335E5C896153} - C:\Program Files\Bonjour\mdnsNSP.dll

Browser Helper Objects

{06849E9F-C8D7-4D59-B87D-784B7D6BE0B3}, Adobe PDF Reader Link Helper, C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll

{14998b0b-2671-4adb-a005-dde2fb18eb35}, Dictionary.com BHO, mscoree.dll(file is missing)

{3049C3E9-B461-4BC5-8870-4C09146192CA}, RealPlayer Download and Record Plugin for Internet Explorer, C:\Program Files\Real\RealPlayer\rpbrowserrecordplugin.dll

{602ADB0E-4AFF-4217-8AA1-95DAC4DFA408}, , C:\Program Files\Common Files\Symantec Shared\coShared\Browser\2.5\colIEPIg.dll

{6D53EC84-6AAE-4787-AEEE-F4628F01010C}, Symantec Intrusion Prevention,

C:\PROGRA~1\COMMON~1\SYMANT~1\IDS\IPSBHO.dll

{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}, SSVHelper Class, C:\Program Files\Java\jre1.6.0_05\bin\ssv.dll

{AA58ED58-01DD-4d91-8333-CF10577473F7}, Google Toolbar Helper, C:\Program Files\Google\Google Toolbar\GoogleToolbar.dll

{AF69DE43-7D58-4638-B6FA-CE66B5AD205D}, Google Toolbar Notifier BHO, C:\Program Files\Google\GoogleToolbarNotifier\5.0.926.3450\swg.dll

{C84D72FE-E17D-4195-BB24-76C02E2E7C4E}, Google Dictionary Compression sdch, C:\Program Files\Google\Google Toolbar\Component\fastsearch_219B3E1547538286.dll

Internet Explorer toolbars (2 whitelisted)

HKLM\...\Toolbar\{bf2aa568-0085-423c-ba01-69b6705a9a96} - Dictionary.com - mscoree.dll(file is missing)

HKLM\...\Toolbar\{7FEBEFE3-6B19-4349-98D2-FFB09D4B49CA} - Show Norton Toolbar - C:\Program Files\Common Files\Symantec Shared\coShared\Browser\2.5\ColIEPIg.dll

HKLM\...\Toolbar\{2318C2B1-4965-11d4-9B18-009027A5CD4F} - &Google Toolbar - C:\Program Files\Google\Google Toolbar\GoogleToolbar.dll

HKCU\...\Toolbar\ShellBrowser\{42CDD1BF-3FFB-4238-8AD1-7859DF00B1D6} - - No file specified

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

Basic Internet Explorer settings

HKCU\...\Main, Start Page = <http://www.google.com/>

HKCU\...\Main, Search Page = <http://www.google.com>

HKLM\...\Search, SearchAssistant = <http://www.google.com/ie>

Registry Startups (3 whitelisted)

HKLM\...\Run, AGRSMMSG = AGRSMMSG.exe

HKLM\...\Run, ATIPTA = "C:\Program Files\ATI Technologies\ATI Control Panel\atiptaxx.exe"

HKLM\...\Run, High Definition Audio Property Page Shortcut = HDAudPropShortcut.exe

HKLM\...\Run, CreateCD_Reminder = "C:\WINDOWS\Sonysys\VAIO Recovery\reminder.exe"

HKLM\...\Run, SoundMan = SOUNDMAN.EXE

HKLM\...\Run, AlcWzrd = ALCWZRD.EXE

HKLM\...\Run, Alcmtr = ALCMTR.EXE

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

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

HKLM\...\Run, VAIO Recovery = "C:\WINDOWS\Sonysys\VAIO Recovery\PartSeal.exe"
HKLM\...\Run, VAIO Update 3 = "C:\Program Files\Sony\VAIO Update 3\VAIOUpdt.exe" /Stationary
HKLM\...\Run, VMConsole.exe = "C:\Program Files\Sony\VAIO Media Integrated Server\Platform\VMConsole.exe"
/windowmin
HKLM\...\Run, SunJavaUpdateSched = "C:\Program Files\Java\jre1.6.0_05\bin\jusched.exe"
HKLM\...\Run, Google Desktop Search = "C:\Program Files\Google\Google Desktop Search\GoogleDesktop.exe" /startup
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, AppleSyncNotifier = C:\Program Files\Common Files\Apple\Mobile Device
Support\bin\AppleSyncNotifier.exe
HKLM\...\Run, Adobe Reader Speed Launcher = "C:\Program Files\Adobe\Reader 8.0\Reader\Reader_sl.exe"
HKLM\...\Run, QuickTime Task = "C:\Program Files\QuickTime\qttask.exe" -atboottime
HKLM\...\Run, iTunesHelper = "C:\Program Files\iTunes\iTunesHelper.exe"
HKLM\...\Run, TkBellExe = "C:\Program Files\Common Files\Real\Update_OB\realsched.exe" -osboot
HKCU\...\Run, MSMSGs = "C:\Program Files\Messenger\msmsgs.exe" /background
HKCU\...\Run, swg = C:\Program Files\Google\GoogleToolbarNotifier\GoogleToolbarNotifier.exe

Autostart shortcuts

Adobe Gamma Loader.Ink, , C:\Program Files\Common Files\Adobe\Calibration\Adobe Gamma Loader.exe
Amazon Unbox.Ink, , C:\Program Files\Amazon\Amazon Unbox Video\ADV\WindowsClientSystemTray.exe
hp psc 1000 series.Ink, , C:\Program Files\Hewlett-Packard\Digital Imaging\bin\hpohmr08.exe
hpoddt01.exe.Ink, , C:\Program Files\Hewlett-Packard\Digital Imaging\bin\hpoddt01.exe
Microsoft Office Fast Start.Ink, , C:\MSOffice\Office\FASTBOOT.EXE
Service Manager.Ink, , C:\Program Files\Microsoft SQL Server\80\Tools\Binn\sqlmangr.exe
Adobe Gamma.Ink, , C:\Program Files\Common Files\Adobe\Calibration\Adobe Gamma Loader.exe

Processes (20 whitelisted)

C:\Program Files\Common Files\Symantec Shared\ccSvcHst.exe
C:\Program Files\Adobe\Photoshop Elements 3.0\PhotoshopElementsFileAgent.exe
C:\Program Files\Amazon\Amazon Unbox Video\ADV\WindowsClientService.exe
C:\Program Files\Common Files\Apple\Mobile Device Support\bin\AppleMobileDeviceService.exe
C:\Program Files\Symantec\LiveUpdate\AluSchedulerSvc.exe
C:\Program Files\Bonjour\mDNSResponder.exe
C:\WINDOWS\ehome\ehRecvr.exe
C:\Program Files\Microsoft SQL Server\MSSQL\$VAIO_VEDB\Binn\sqlservr.exe
C:\Program Files\Adobe\Photoshop Elements 3.0\PhotoshopElementsDeviceConnect.exe
C:\Program Files\Sony\Sony TV Tuner Library\SMceMan.exe
C:\Program Files\Sony\VAIO Media Integrated Server\VMISrv.exe
C:\Program Files\Common Files\Sony Shared\VAIO Entertainment Platform\VCSW\VCSW.exe
C:\Program Files\Webroot\Washer\WasherSvc.exe
C:\WINDOWS\ehome\mcrdsvc.exe
C:\Program Files\Common Files\Sony Shared\VAIO Entertainment Platform\VzCdb\VzCdbSvc.exe
C:\Program Files\Sony\VAIO Media Integrated Server\Platform\SV_Httpd.exe
C:\Program Files\Common Files\Sony Shared\VAIO Entertainment Platform\VzCdb\VzFw.exe
C:\Program Files\Sony\VAIO Media Integrated Server\Platform\UPnPFramework.exe
C:\Program Files\Sony\Sony TV Tuner Library\RM_SV.exe
C:\Program Files\Common Files\Sony Shared\VAIO Entertainment
Platform\VzCs\VzHardwareResourceManager\VzHardwareResourceManager.exe
C:\Program Files\iPod\bin\iPodService.exe
C:\PROGRA~1\COMMON~1\SYMANT~1\CCPD-LC\symIcSvc.exe
C:\Program Files\Common Files\Symantec Shared\VAScanner\comHost.exe
C:\Program Files\Google\GoogleToolbarNotifier\GoogleToolbarNotifier.exe
C:\Program Files\FreeFixer\freefixer.exe

Application modules (53 whitelisted)

C:\WINDOWS\system32\ieframe.dll
C:\WINDOWS\system32\iertutil.dll
C:\WINDOWS\system32\Normaliz.dll
C:\Program Files\Internet Explorer\ieproxy.dll

Services (37 whitelisted)

AdobeActiveFileMonitor, Adobe Active File Monitor, c:\program files\adobe\photoshop elements
3.0\photoshopelementsfileagent.exe
ADVService, Amazon Unbox Video Service, c:\program files\amazon\amazon unbox video\advwindowsclientservice.exe
Apple Mobile Device, Apple Mobile Device, c:\program files\common files\apple\mobile device

support\bin\applemobiledeviceservice.exe
Ati HotKey Poller, , c:\windows\system32\ati2evxx.exe
Automatic LiveUpdate Scheduler, Automatic LiveUpdate Scheduler, c:\program files\symantec\liveupdate\aluschedulersvc.exe
Bonjour Service, Bonjour Service, c:\program files\bonjour\mdnsresponder.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
ehRecvr, Media Center Receiver Service, c:\windows\ehome\ehrecvr.exe
LiveUpdate Notice, LiveUpdate Notice, c:\program files\common files\symantec shared\ccsvchst.exe
McrdSvc, Media Center Extender Service, c:\windows\ehome\mcrdsvc.exe
MSSQL\$VAIO_VEDB, MSSQL\$VAIO_VEDB, c:\program files\microsoft sql server\mssql\$vaio_vedb\binn\sqlservr.exe
PhotoshopElementsDeviceConnect, Photoshop Elements Device Connect, c:\program files\adobe\photoshop elements 3.0\photoshopelementsdeviceconnect.exe
Sony TVTA Manager, Sony TVTA Manager, c:\program files\sony\sony tv tuner library\smceman.exe
VAIOMediaPlatform-IntegratedServer-AppServer, VAIO Media Integrated Server, c:\program files\sony\vaio media integrated server\vmisrv.exe
VAIOMediaPlatform-IntegratedServer-HTTP, VAIO Media Integrated Server (HTTP), c:\program files\sony\vaio media integrated server\platform\sv_httpd.exe
VAIOMediaPlatform-IntegratedServer-UPnP, VAIO Media Integrated Server (UPnP), c:\program files\sony\vaio media integrated server\platform\upnpframework.exe
VzCdbSvc, VAIO Entertainment Database Service, c:\program files\common files\sony shared\vaio entertainment platform\vzcdb\vzcdbsvc.exe
VzFw, VAIO Entertainment File Import Service, c:\program files\common files\sony shared\vaio entertainment platform\vzcdb\vzfw.exe
wwEngineSvc, Window Washer Engine, c:\program files\webroot\washer\washersvc.exe

Shell services (4 whitelisted)

WPDSHServiceObj, {AAA288BA-9A4C-45B0-95D7-94D524869DB5}, C:\WINDOWS\system32\WPDSHServiceObj.dll

Drivers (27 whitelisted)

CO_Mon, CO_Mon, c:\windows\system32\drivers\co_mon.sys
DgiVecp, Team MFP Comm Driver, C:\WINDOWS\system32\drivers\dgivecp.sys
DMICall, Sony DMI Call service, C:\WINDOWS\system32\drivers\dmicall.sys
eeCtrl, Symantec Eraser Control driver, c:\program files\common files\symantec shared\engine\eectrl.sys
PxHelp20, PxHelp20, C:\WINDOWS\system32\drivers\pxhelp20.sys
SPBBCDrv, SPBBCDrv, c:\program files\common files\symantec shared\spbbc\spbbcdrv.sys
SRTSPX, SRTSPX, C:\WINDOWS\system32\drivers\srtspk.sys
SYMTDI, SYMTDI, C:\WINDOWS\system32\drivers\symtdi.sys

Re:FF Log--Thanks

Posted by securitywonks - 2009/02/04 18:01

Dear Beamer

my apologies for delay in response,

coming to log,

download Spybot Search & Destroy:

<http://projects.securitywonks.net/projects/details.php?file=2>

download MalwareBytes's Anti-Malware:

<http://projects.securitywonks.net/projects/details.php?file=158>

install the above two applications, update the definitions and scan your computer with them and fix what they suggest.

come back with fresh log after that,

All the Best with your computer :)

Re:FF Log--Thanks

Posted by Beamer - 2009/02/05 21:26

Thanks, but still foiled. Downloaded and installed both Spybot And MalWarebytes; cannot update either and so Spybot won't scan. MalWarebytes did a scan, but with 1-14-09 version. Don't want to send you another log until I've updated the programs. Tried to update Spybot manually from safer-networking site, but cannot access because (presumed) hijack bug blocks my access. Advice?

=====

Re:FF Log--Thanks

Posted by securitywonks - 2009/02/06 03:00

what you can basically do when installing SPYBOT is to uncheck "DOWNLOAD UPDATES IMMEDIATELY" option in the third screen of installation wizard (if I remember correct).

then, software gets installed normally and you can click SEARCH FOR UPDATES button and download updates.

are you not able to access spybot.info site?

open

```
C:\WINDOWS\system32\drivers\etc\HOSTS
```

delete everything except this:

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 102.54.94.97 rhino.acme.com # source server
# 38.25.63.10 x.acme.com # x client host

127.0.0.1 localhost
```

doing this way, you can attempt to visit websites of security programs. Actually, if there were any malicious entries related to security websites in HOSTS file, it will get identified in freefixer. Anyhow, as you said, you have issues in the computer which donot enable to access the security websites, try this manual way.

SAVE HOSTS file back normally and close the HOSTS file.

NOTE: HOSTS file DONOT have any extension, please ensure that.

let us know, if there is any progress, otherwise, I will host SPYBOT Definitions if required,

you can download MANUAL UPDATES for Malwarebytes.org from here

<http://www.gt500.org/malwarebytes/database.jsp>

it's advisable to try another antivirus scanner in your computer

Avast Home Edition (if this is a home computer):
<http://www.avast.com/eng/download-avast-home.html>

or

COMODO AntiVirus:
<http://antivirus.comodo.com/>

I donot observe a FIREWALL in your computer,

try COMODO Internet Security if you like (it have antivirus and firewall both)

tell how things progress

All the Best with your computer:)

=====