

# freefixer log -- is anyone still checking these?

Posted by katemarie1197 - 2009/02/02 09:24

I don't even know what's what...

FreeFixer v0.30 log

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

Operating system: Windows XP Service Pack 2

Log dated 2009-02-02 00:16

Hidden processes

pid: 2240, fbabj220320.exe, C:\Documents and Settings\Owner.YOUR-XB2X7J77GN\Application Data\Google\fbabj220320.exe

Winlogon Notify (9 whitelisted)

crypt - crypts.dll (file is missing)

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

TCP/IP settings

HKLM\...\Interfaces\{B9E0C825-4E5A-4F53-AB2C-747272C1CC83}, NameServer = 205.171.3.65,205.171.2.65

Namespace service providers (3 whitelisted)

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

Browser Helper Objects

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

{2E65A557-173C-4DE9-860B-28FC5CACA542}, Setup.Setup1,

C:\DOCUME~1\ALLUSE~1\APPLIC~1\Setup\Setup.dll (file is missing)

{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\_07\bin\ssv.dll

{7E853D72-626A-48EC-A868-BA8D5E23E045}, , No file specified

{9030D464-4C02-4ABF-8ECC-5164760863C6}, Windows Live Sign-in Helper, C:\Program Files\Common Files\Microsoft Shared\Windows Live\WindowsLiveLogin.dll

Internet Explorer toolbars (2 whitelisted)

HKLM\...\Toolbar\{12EE7A5E-0674-42f9-A76B-000000004D00} - - No file specified

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

HKCU\...\Toolbar\WebBrowser\{EF99BD32-C1FB-11D2-892F-0090271D4F88} - - No file specified

HKCU\...\Toolbar\WebBrowser\{2318C2B1-4965-11D4-9B18-009027A5CD4F} - - No file specified

Basic Internet Explorer settings

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

HKLM\...\Main, Start Page = [http://securityresponse.symantec.com/avcenter/fix\\_homepage/](http://securityresponse.symantec.com/avcenter/fix_homepage/)

Registry Startups

HKLM\...\Run, hpsysdrv = c:\windows\system\hpsysdrv.exe

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

HKLM\...\Run, Recguard = C:\WINDOWS\SMINST\RECGUARD.EXE

HKLM\...\Run, PS2 = C:\WINDOWS\system32\ps2.exe

HKLM\...\Run, Ohuxo = C:\Program Files\Pijrxb\Stub.exe (file is missing)

HKLM\...\Run, TkBellExe = "C:\Program Files\Common Files\Real\Update\_OB\realsched.exe" -osboot

HKLM\...\Run, SunJavaUpdateSched = "C:\Program Files\Java\jre1.6.0\_07\bin\jusched.exe"

HKLM\...\Run, FLMOFFICE4DMOUSE = C:\Program Files\Labtec\Desktop\V5.1\moffice.exe

HKLM\...\Run, OFFICEKB = C:\Program Files\Labtec\Desktop\V5.1\kbdap32a.exe

HKLM\...\Run, ccApp = "C:\Program Files\Common Files\Symantec Shared\ccApp.exe"

HKLM\...\Run, osCheck = "C:\Program Files\Norton AntiVirus\osCheck.exe"

HKLM\...\Run, AlcxMonitor = ALCXMNTR.EXE

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

HKLM\...\Run, HP Software Update = C:\Program Files\HP\HP Software Update\HPWuSchd2.exe

HKLM\...\Run, Lexmark 1200 Series = "C:\Program Files\Lexmark 1200 Series\lxczbmgr.exe"

HKLM\...\Run, QuickTime Task = "C:\Program Files\QuickTime\QTTask.exe" -atboottime

HKLM\...\Run, iTunesHelper = "C:\Program Files\iTunes\iTunesHelper.exe"

HKCU\.\Run, RecordNow! = (file is missing)  
HKCU\.\Run, e02mRhd2U = iucrdr.exe (file is missing)  
HKCU\.\Run, MoneyAgent = "C:\Program Files\Microsoft Money\System\mnyexpr.exe" (file is missing)  
HKCU\.\Run, BgMonitor\_{79662E04-7C6C-4d9f-84C7-88D8A56B10AA} = "C:\Program Files\Common Files\Ahead\Lib\NMBgMonitor.exe" (file is missing)  
HKCU\.\Run, Aim6 = "C:\Program Files\AIM6\aim6.exe" /d locale=en-US ee://aol/imApp  
HKCU\.\Run, SVCHOST.EXE = C:\WINDOWS\system32\drivers\svchost.exe

#### Autostart shortcuts

Adobe Reader Speed Launch.Ink, , C:\Program Files\Adobe\Acrobat 7.0\Reader\reader\_sl.exe  
Sonic CinePlayer Quick Launch.Ink, , C:\Program Files\Common Files\Sonic Shared\CineTray.exe

#### Processes (13 whitelisted)

C:\Program Files\Common Files\Symantec Shared\ccSvcHst.exe  
C:\WINDOWS\system32\LEXBCES.EXE  
C:\WINDOWS\system32\LEXPPS.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\System32\wdfmgr.exe  
C:\Program Files\Viewpoint\Common\ViewpointService.exe  
C:\windows\system\hpsysdrv.exe  
C:\WINDOWS\system32\hkcmd.exe  
C:\WINDOWS\system32\ps2.exe  
C:\Program Files\Common Files\Real\Update\_OB\realsched.exe  
C:\Program Files\Java\jre1.6.0\_07\bin\jusched.exe  
C:\Program Files\Labtec\Desktop\V5.1\moffice.exe  
C:\Program Files\Labtec\Desktop\V5.1\kbdap32a.exe  
C:\Program Files\Common Files\Symantec Shared\ccSvcHst.exe  
C:\Program Files\Labtec\Desktop\V5.1\MOUSE32A.EXE  
C:\WINDOWS\ALCXMNTR.EXE  
C:\WINDOWS\system32\igfxtray.exe  
C:\Program Files\HP\HP Software Update\HPWuSchd2.exe  
C:\Program Files\Viewpoint\Viewpoint Manager\ViewMgr.exe  
C:\Program Files\iTunes\iTunesHelper.exe  
C:\WINDOWS\system32\drivers\svchost.exe  
C:\Program Files\iPod\bin\iPodService.exe  
C:\Program Files\Crazy Browser\Crazy Browser.exe  
C:\Program Files\Mozilla Firefox\firefox.exe  
C:\Program Files\FreeFixer\freefixer.exe

#### Application modules (55 whitelisted)

C:\Documents and Settings\Owner.YOUR-XB2X7J77GN\Application Data\Google\ptnmsn64.dll  
C:\Program Files\Labtec\Desktop\V5.1\MOUDL32A.DLL

#### Services (32 whitelisted)

Apple Mobile Device, Apple Mobile Device, c:\program files\common files\apple\mobile device support\bin\applemobiledeviceservice.exe  
Automatic LiveUpdate Scheduler, Automatic LiveUpdate Scheduler, c:\program files\symantec\liveupdate\aluschedulervc.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  
LexBceS, LexBce Server, c:\windows\system32\lexbces.exe  
LiveUpdate Notice, LiveUpdate Notice, c:\program files\common files\symantec shared\ccsvchst.exe  
UMWdf, Windows User Mode Driver Framework, c:\windows\system32\wdfmgr.exe  
Viewpoint Manager Service, Viewpoint Manager Service, c:\program files\viewpoint\common\viewpointservice.exe

#### Drivers (27 whitelisted)

eeCtrl, Symantec Eraser Control driver, c:\program files\common files\symantec shared\engine\eectrl.sys  
fasttx2k, , C:\WINDOWS\system32\drivers\fasttx2k.sys  
nv\_agp, NVIDIA nForce AGP Bus Filter, C:\WINDOWS\system32\drivers\nv\_agp.sys  
PxHelp20, , C:\WINDOWS\system32\drivers\pxhelp20.sys  
SISAGP, SiS AGP Filter, C:\WINDOWS\system32\drivers\sisagp.sys

---

SiSkp, , C:\WINDOWS\system32\drivers\srvkp.sys  
SPBBCDrv, SPBBCDrv, c:\program files\common files\symantec shared\spbbc\spbbcdrv.sys  
SRTSPX, SRTSPX, C:\WINDOWS\system32\drivers\srtspk.sys  
SYMTEI, SYMTEI, C:\WINDOWS\system32\drivers\symtei.sys  
viaagp1, VIA AGP Filter, C:\WINDOWS\system32\drivers\viaagp1.sys

=====

## Re:freefixer log -- is anyone still checking these?

Posted by securitywonks - 2009/02/04 17:49

---

Dear Kate

my apologies for delayed response.

This situation continues for some more days and once the planned changes in website is completed, it will get fully active and our response with be more prompt,

coming to your log,

Delete this file: C:\Documents and Settings\Owner.YOUR-XB2X7J77GN\Application Data\Google\fbabj220320.exe

then, fix the following entry using FreeFixer:

pid: 2240, fbabj220320.exe, C:\Documents and Settings\Owner.YOUR-XB2X7J77GN\Application Data\Google\fbabj220320.exe

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

=====