

can someone help me please?

Posted by monchichi - 2008/06/30 18:53

Hello,

I have no idea what I have to do with these files (fix or delete...):(

Please help me!

Here's my logfile:

FreeFixer v0.27 log

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

Operating system: Windows XP Service Pack 2

Log dated 2008-06-28 13:53

Winlogon Notify (9 whitelisted)

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

Browser Helper Objects

{06849E9F-C8D7-4D59-B87D-784B7D6BE0B3}, Adobe PDF Reader, C:\Program Files\Common

Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll

{0A94B111-4504-4e26-AB05-E61E474AA38B}, Ask Search Assistant BHO, C:\Program

Files\AskPBar\SrchAsth\1.bin\A9SRCHAS.DLL

{53707962-6F74-2D53-2644-206D7942484F}, Spybot-S&D IE Protection, C:\PROGRA~1\SPYBOT~1\SDHelper.dll

{5CA3D70E-1895-11CF-8E15-001234567890}, DriveLetterAccess, C:\WINDOWS\System32\DLA\DLASHX_W.DLL

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

{BDBD1DAD-C946-4A17-ADC1-64B5B4FF55D0}, Windows Live Toolbar Helper, C:\Program Files\Windows Live

Toolbar\msntb.dll

{F4D76F01-7896-458a-890F-E1F05C46069F}, , No file specified

Internet Explorer toolbars (1 whitelisted)

HKLM\..\Toolbar\{BDAD1DAD-C946-4A17-ADC1-64B5B4FF55D0} - Windows Live Toolbar - C:\Program Files\Windows Live Toolbar\msntb.dll

HKLM\..\Toolbar\{F4D76F09-7896-458a-890F-E1F05C46069F} - - No file specified

HKCU\..\Toolbar\WebBrowser\{855F3B16-6D32-4FE6-8A56-BBB695989046} - - No file specified

HKCU\..\Toolbar\WebBrowser\{47833539-D0C5-4125-9FA8-0819E2EAAC93} - - No file specified

Basic Internet Explorer settings

HKCU\..\Main, Start Page = <http://start.icq.com/>

HKLM\..\Main, Start Page = <http://go.microsoft.com/fwlink/?LinkId=69157>

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>

HKLM\..\Search, SearchAssistant =

Registry Startups (1 whitelisted)

HKLM\..\Run, C-Media Mixer = Mixer.exe /startup

HKLM\..\Run, DLA = C:\WINDOWS\System32\DLA\DLACTRLW.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, avgnt = "C:\Program Files\AntiVir PersonalEdition Classic\avgnt.exe" /min

HKLM\..\Run, SunJavaUpdateSched = "C:\Program Files\Java\jre1.6.0_05\bin\jusched.exe"

HKLM\..\Run, Adobe Reader Speed Launcher = "C:\Program Files\Adobe\Reader 8.0\Reader\Reader_sl.exe"

HKLM\..\Run, ISTRay = "C:\Program Files\Spyware Doctor\pctsTray.exe"

HKLM\..\RunOnce, Spybot - Search & Destroy = "C:\Program Files\Spybot - Search & Destroy\SpybotSD.exe" /autocheck

HKCU\..\Run, prtcegx = c:\documents and settings\verena\local settings\application data\prtcegx.exe prtcegx

HKCU\..\Run, SpybotSD TeaTimer = C:\Program Files\Spybot - Search & Destroy\TeaTimer.exe

Autostart shortcuts

Microsoft Office.Ink, Microsoft Office Autostart, C:\Program Files\Microsoft Office\Office\OSA9.EXE

Processes (16 whitelisted)

C:\Program Files\AntiVir PersonalEdition Classic\avguard.exe
C:\Program Files\a-squared Anti-Dialer\a2service.exe
C:\Program Files\AntiVir PersonalEdition Classic\sched.exe
C:\WINDOWS\system32\bgsvcgen.exe
C:\Program Files\Spyware Doctor\pctsAuxs.exe
C:\Program Files\Spyware Doctor\pctsSvc.exe
C:\Program Files\Spyware Doctor\pctsTray.exe
C:\Program Files\AntiVir PersonalEdition Classic\avgnt.exe
C:\WINDOWS\Mixer.exe
C:\WINDOWS\System32\DLA\DLACTRLW.EXE
C:\Program Files\Common Files\InstallShield\UpdateService\issch.exe
C:\Program Files\Java\jre1.6.0_05\bin\jusched.exe
C:\documents and settings\verena\local settings\application data\prtcegx.exe
C:\Program Files\Spybot - Search & Destroy\TeaTimer.exe
C:\Program Files\Adobe\Reader 8.0\Reader\AcroRd32.exe
C:\Program Files\FreeFixer\freefixer.exe

Application modules (47 whitelisted)

C:\Program Files\Spyware Doctor\smumhook.dll
C:\Program Files\Spyware Doctor\klg.dat
C:\WINDOWS\system32\ieframe.dll
C:\WINDOWS\system32\iertutil.dll
C:\WINDOWS\system32\Normaliz.dll

Services (36 whitelisted)

a2AntiDialer, a-squared Anti-Dialer Service, c:\program files\a-squared anti-dialer\a2service.exe
AntiVirScheduler, AntiVir PersonalEdition Classic Planer, c:\program files\antivir personaledition classic\sched.exe
AntiVirService, AntiVir PersonalEdition Classic Guard, c:\program files\antivir personaledition classic\avguard.exe
bgsvcgen, B's Recorder GOLD Library General Service, c:\windows\system32\bgsvcgen.exe
sdAuxService, PC Tools Auxiliary Service, c:\program files\spyware doctor\pctsauxs.exe
sdCoreService, PC Tools Security Service, c:\program files\spyware doctor\pctssvc.exe

Drivers (27 whitelisted)

avgio, avgio, c:\program files\antivir personaledition classic\avgio.sys
avipbb, avipbb, C:\WINDOWS\system32\drivers\avipbb.sys
DRVMCDB, , C:\WINDOWS\system32\drivers\drvmcdb.sys
IKSysFlt, System Filter Driver, C:\WINDOWS\system32\drivers\iksysflt.sys
IKSysSec, System Security Driver, C:\WINDOWS\system32\drivers\iksyssec.sys
PxHelp20, PxHelp20, C:\WINDOWS\system32\drivers\pxhelp20.sys

Thank you very much!
Monchichi :-)

=====

Re:can someone help me please?

Posted by securitywonks - 2008/07/08 05:21

Dear Monchichi

sorry for delayed reply

I didnt find any much bad things in the log,

please explain your problem further,

thank you

SecurityWonks

=====