

freefixer log

Posted by pelle - 2009/02/03 17:07

FreeFixer v0.31 log

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

Operating system: Windows XP Service Pack 2

Log dated 2009-02-03 15:55

Suspicious file names

C:\WINDOWS\clspack.exe

C:\WINDOWS\extrac32.exe

Winlogon Notify (9 whitelisted)

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

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

Browser Helper Objects

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

{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}, Java(tm) Plug-In SSV Helper, C:\Programmi\Java\jre6\bin\ssv.dll

{DBC80044-A445-435b-BC74-9C25C1C588A9}, Java(tm) Plug-In 2 SSV Helper, C:\Programmi\Java\jre6\bin\jp2ssv.dll

{E7E6F031-17CE-4C07-BC86-EABFE594F69C}, JQSIStartDetectorImpl Class,

C:\Programmi\Java\jre6\lib\deploy\jqs\ie\jqs_plugin.dll

Internet Explorer toolbars (2 whitelisted)

HKLM\..\Toolbar\{5CBE3B7C-1E47-477e-A7DD-396DB0476E29} - Acer eDataSecurity Management -

C:\WINDOWS\system32\eDStoolbar.dll

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

Basic Internet Explorer settings

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

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

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

Registry Startups (6 whitelisted)

HKLM\..\Run, preload = C:\Windows\RUNXMLPL.exe

HKLM\..\Run, SynTPEnh = C:\Programmi\Synaptics\SynTP\SynTPEnh.exe

HKLM\..\Run, RTHDCPL = RTHDCPL.EXE

HKLM\..\Run, AzMixerSel = C:\Programmi\Realtek\InstallShield\AzMixerSel.exe

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

HKLM\..\Run, NvCplDaemon = RUNDLL32.EXE C:\WINDOWS\system32\NvCpl.dll,NvStartup

HKLM\..\Run, NvMediaCenter = RUNDLL32.EXE C:\WINDOWS\system32\NvMcTray.dll,NvTaskbarInit

HKLM\..\Run, eDataSecurity Loader = C:\Acer\Empowering Technology\eDataSecurity\eDSloader.exe 0

HKLM\..\Run, ePower_DMC = C:\Acer\Empowering Technology\ePower\ePower_DMC.exe

HKLM\..\Run, Boot = C:\Acer\Empowering Technology\ePower\Boot.exe

HKLM\..\Run, Acer ePresentation HPD = C:\Acer\Empowering Technology\ePresentation\ePresentation.exe

HKLM\..\Run, eRecoveryService = C:\Acer\Empowering Technology\eRecovery\ERAgent.exe

HKLM\..\Run, LVCOMSX = C:\WINDOWS\system32\LVCOMSX.EXE

HKLM\..\Run, LogitechCameraService(E) = C:\WINDOWS\system32\EIICtrl.exe /automation

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

HKLM\..\Run, avast! = C:\PROGRA~1\ALWILS~1\Avast4\ashDisp.exe

HKLM\..\Run, Wbutton = "C:\Programmi\Launch Manager\Wbutton.exe"

HKLM\..\Run, LMgrOSD = "C:\Programmi\Launch Manager\OSDCtrl.exe"

HKLM\..\Run, LManager = "C:\Programmi\Launch Manager\HotkeyApp.exe"

HKLM\..\Run, LaunchAp = "C:\Programmi\Launch Manager\LaunchAp.exe"

HKLM\..\Run, CtrlVol = "C:\Programmi\Launch Manager\CtrlVol.exe"

HKLM\..\Run, TKBellExe = "C:\Programmi\File comuni\Real\Update_OB\realsched.exe" -osboot

HKLM\..\Run, nwiz = nwiz.exe /install

HKLM\..\Run, EPSON Stylus DX4000 Series = C:\WINDOWS\System32\spool\DRIVERS\W32X86\3\E_FATIBEE.EXE /FU "C:\WINDOWS\TEMP\E_S45.tmp" /EF "HKLM"

HKLM\..\Run, SunJavaUpdateSched = "C:\Programmi\Java\jre6\bin\jusched.exe"

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

HKCU\..\Run, H/PC Connection Agent = "C:\Programmi\Microsoft ActiveSync\wcescomm.exe"

Autostart shortcuts

Acer Empowering Technology.Ink, , C:\Acer\Empowering Technology\Acer.Empowering.Framework.Launcher.exe

Processes (28 whitelisted)

C:\Programmi\Intel\Wireless\Bin\EvtEng.exe
C:\Programmi\Intel\Wireless\Bin\S24EvMon.exe
C:\Programmi\Alwil Software\Avast4\aswUpdSv.exe
C:\Programmi\Alwil Software\Avast4\ashServ.exe
C:\Programmi\Synaptics\SynTP\SynTPEnh.exe
C:\WINDOWS\RTHDCPL.EXE
C:\WINDOWS\AGRSMMMSG.exe
C:\Acer\Empowering Technology\eDataSecurity\eDSloader.exe
C:\Acer\Empowering Technology\ePower\ePower_DMC.exe
C:\Acer\Empowering Technology\epresentation\epresentation.exe
C:\Acer\Empowering Technology\erecovery\erecovery\RAgent.exe
C:\WINDOWS\system32\LVCOMSX.EXE
C:\WINDOWS\system32\EIkCtrl.exe
C:\PROGRA~1\ALWILS~1\Avast4\ashDisp.exe
C:\Programmi\Launch Manager\Wbutton.exe
C:\Programmi\Launch Manager\OSDCtrl.exe
C:\Programmi\Launch Manager\HotkeyApp.exe
C:\Programmi\Launch Manager\LaunchAp.exe
C:\Programmi\File comuni\Real\Update_OB\realsched.exe
C:\Programmi\Java\jre6\bin\jusched.exe
C:\Programmi\Microsoft ActiveSync\wcescomm.exe
C:\PROGRA~1\MICROS~4\rapimgr.exe
C:\Acer\Empowering Technology\Acer.Empowering.Framework.Launcher.exe
c:\programmi\file comuni\logitech\lvmvfm\LVPrsSrv.exe
C:\Acer\Empowering Technology\epPerformance\MemCheck.exe
C:\WINDOWS\ehome\ehRecvr.exe
C:\Programmi\Java\jre6\bin\jqs.exe
c:\Programmi\Microsoft SQL Server\MSSQL.1\MSSQL\Binn\sqlservr.exe
C:\WINDOWS\system32\nvsvc32.exe
C:\Programmi\Intel\Wireless\Bin\RegSrv.exe
c:\Programmi\Microsoft SQL Server\90\Shared\sqlwriter.exe
C:\Programmi\File comuni\VMware\VMware Virtual Image Editing\vmount2.exe
C:\WINDOWS\system32\vmnat.exe
C:\WINDOWS\ehome\mcrdsvc.exe
C:\WINDOWS\system32\vmnetdhcp.exe
C:\Programmi\Alwil Software\Avast4\ashMaiSv.exe
C:\Programmi\Alwil Software\Avast4\ashWebSv.exe
C:\WINDOWS\system32\igfxsrvc.exe
C:\Programmi\Mozilla Firefox\firefox.exe
C:\Programmi\FreeFixer\freefixer.exe
C:\WINDOWS\system32\mdm.exe

Application modules (57 whitelisted)

C:\Programmi\File comuni\Logitech\LVMVFM\LVPrclnj.dll
C:\WINDOWS\system32\MSNCHATHOOK.DLL
C:\WINDOWS\system32\sysenv.dll
C:\WINDOWS\system32\CryptoAPI.dll
C:\WINDOWS\system32\MSVCR71.dll
C:\WINDOWS\system32\MFC71U.DLL
C:\WINDOWS\system32\MSVCP71.dll
C:\WINDOWS\system32\MFC71ITA.DLL
C:\WINDOWS\system32\nview.dll
C:\WINDOWS\system32\NVWRSIT.DLL
C:\WINDOWS\system32\ieframe.dll
C:\WINDOWS\system32\iertutil.dll
C:\WINDOWS\system32\Normaliz.dll
C:\Programmi\File comuni\Microsoft Shared\VS7Debug\pdm.dll
C:\Programmi\File comuni\Microsoft Shared\VS7Debug\msdbg2.dll
C:\WINDOWS\system32\nvwddi.dll
C:\Acer\Empowering Technology\ePower\SysHook.dll

Services (44 whitelisted)

AcerMemUsageCheckService, Memory Check Service, c:\acer\empowering technology\performance\memcheck.exe
aswUpdSv, avast! iAVS4 Control Service, c:\programmi\alwil software\avast4\aswupdsv.exe
avast! Antivirus, avast! Antivirus, c:\programmi\alwil software\avast4\ashserv.exe
ehRecvr, Media Center Receiver Service, c:\windows\ehome\ehrecvr.exe
EvtEng, Intel(R) PROSet/Wireless Event Log, c:\programmi\intel\wireless\bin\evteng.exe
JavaQuickStarterService, Java Quick Starter, c:\programmi\java\jre6\bin\jqs.exe
LVPrsSrv, Logitech Process Monitor, c:\programmi\file comuni\logitech\lvmvfm\lvprcsv.exe
McrdSvc, Media Center Extender Service, c:\windows\ehome\mcrdsvc.exe
MSSQL\$SQLEXPRESS, SQL Server (SQLEXPRESS), c:\programmi\microsoft sql server\mssql.1\mssql\bin\sqlservr.exe
NVSvc, NVIDIA Display Driver Service, c:\windows\system32\nvsvc32.exe
RegSvc, Intel(R) PROSet/Wireless Registry Service, c:\programmi\intel\wireless\bin\regsvc.exe
S24EventMonitor, Intel(R) PROSet/Wireless Service, c:\programmi\intel\wireless\bin\s24evmon.exe
SQLWriter, SQL Server VSS Writer, c:\programmi\microsoft sql server\90\shared\sqlwriter.exe
VMnetDHCP, VMware DHCP Service, c:\windows\system32\vmnetdhcp.exe
vmount2, VMware Virtual Mount Manager Extended, c:\programmi\file comuni\vmware\vmware virtual image editing\vmount2.exe
VMware NAT Service, VMware NAT Service, c:\windows\system32\vmnat.exe

Shell services (4 whitelisted)

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

Drivers (74 whitelisted)

AegisP, AEGIS Protocol (IEEE 802.1x) v3.4.9.0, C:\WINDOWS\system32\drivers\aeagisp.sys
EpmPsd, Acer EPM Power Scheme Driver, c:\windows\system32\drivers\epm-psd.sys
EpmShd, Acer EPM System Hardware Driver, c:\windows\system32\drivers\epm-shd.sys
GiveIO, GiveIO Port Access, C:\WINDOWS\system32\drivers\giveio.sys
hcmon, VMware hcmon, c:\windows\system32\drivers\hcmon.sys
int15, int15, c:\windows\system32\drivers\int15.sys
PxHelp20, PxHelp20, C:\WINDOWS\system32\drivers\pxhelp20.sys
s24trans, Trasporto WLAN, C:\WINDOWS\system32\drivers\s24trans.sys
tvicport, tvicport, c:\windows\system32\drivers\tvicport.sys
VMnetBridge, VMware Bridge Protocol, C:\WINDOWS\system32\drivers\vmnetbridge.sys
VMnetuserif, VMware Network Application Interface, c:\windows\system32\drivers\vmnetuserif.sys
vmx86, VMware vmx86, c:\windows\system32\drivers\vmx86.sys
VPCAppSv, Virtual PC Application Services, C:\WINDOWS\system32\drivers\vpccappsv.sys
vstor2, Vstor2 Virtual Storage Driver, c:\programmi\file comuni\vmware\vmware virtual image editing\vstor2.sys
Wbutton, , C:\WINDOWS\system32\drivers\wbutton.sys (file is missing)
WudfPf, Windows Driver Foundation - User-mode Driver Framework Platform Driver, C:\WINDOWS\system32\drivers\wudfpf.sys
zntport, zntport, c:\windows\system32\drivers\zntport.sys

=====

Re:freefixer log

Posted by securitywonks - 2009/02/04 18:05

Dear Pelle

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

=====