

log

Posted by haletto - 2009/02/05 18:55

FreeFixer v0.31 log

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

Operating system: Windows XP Service Pack 3

Log dated 2009-02-05 17:49

Winlogon Notify (10 whitelisted)

!SASWinLogon - C:\Programmi\SUPERAntiSpyware\SASWINLO.dll

Namespace service providers (3 whitelisted)

{B600E6E9-553B-4A19-8696-335E5C896153} - C:\Programmi\Bonjour\mdnsNSP.dll (file is missing)

Browser Helper Objects

{06849E9F-C8D7-4D59-B87D-784B7D6BE0B3}, AcroIEHlprObj Class, C:\Programmi\Adobe\Acrobat

6.0\Acrobat\ActiveX\AcroIEHelper.dll

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

{5C255C8A-E604-49b4-9D64-90988571CECB}, , No file specified

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

{72853161-30C5-4D22-B7F9-0BBC1D38A37E}, Groove GFS Browser Helper, C:\Programmi\Microsoft Office\Office12\GrooveShellExtensions.dll

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

{9030D464-4C02-4ABF-8ECC-5164760863C6}, Guida per l'accesso a Windows Live, C:\Programmi\File comuni\Microsoft Shared\Windows Live\WindowsLiveLogin.dll

{AE7CD045-E861-484f-8273-0445EE161910}, AcroIEToolbarHelper Class, C:\Programmi\Adobe\Acrobat 6.0\Acrobat\AcroIEFavClient.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}, JQSIEStartDetectorImpl Class,

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

Internet Explorer toolbars (2 whitelisted)

HKLM\..\Toolbar\{47833539-D0C5-4125-9FA8-0819E2EAAC93} - Adobe PDF - C:\Programmi\Adobe\Acrobat 6.0\Acrobat\AcroIEFavClient.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://it.msn.com>

Registry Startups (1 whitelisted)

HKLM\.\Run, ATIPTA = C:\Programmi\ATI Technologies\ATI Control Panel\atiptaxx.exe

HKLM\.\Run, Apoint = C:\Programmi\Apoint2K\Apoint.exe

HKLM\.\Run, PadTouch = "C:\Programmi\TOSHIBA\PadTouch\PadExe.exe

HKLM\.\Run, AGRSMMSG = AGRSMMSG.exe

HKLM\.\Run, CeEPOWER = C:\Programmi\TOSHIBA\Power Management\CePMTTray.exe

HKLM\.\Run, = (file is missing)

HKLM\.\Run, CeEKEY = C:\Programmi\TOSHIBA\E-KEY\CeEKey.exe

HKLM\.\Run, EzButton = C:\Programmi\EzButton\EzButton.EXE

HKLM\.\Run, TPNF = C:\Programmi\TOSHIBA\TouchPad\TPTray.exe

HKLM\.\Run, ZoomingHook = c:\WINDOWS\System32\ZoomingHook.exe

HKLM\.\Run, SmoothView = C:\Programmi\TOSHIBA\TOSHIBA Zooming Utility\SmoothView.exe

HKLM\.\Run, NDSTray.exe = NDSTray.exe (file is missing)

HKLM\.\Run, dla = C:\WINDOWS\system32\dla\lftswctrl.exe

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

HKLM\.\Run, MOD = C:\Programmi\Microangelo\muamgr.exe

HKLM\.\Run, NeroFilterCheck = C:\WINDOWS\system32\NeroCheck.exe

HKLM\.\Run, PCSuiteTrayApplication = C:\PROGRA~1\Nokia\NOKIAP~1\LAUNCH~1.EXE -startup

HKLM\.\Run, GrooveMonitor = "C:\Programmi\Microsoft Office\Office12\GrooveMonitor.exe"

HKLM\.\Run, 9xadiras = 9xadiras.exe (file is missing)

HKLM\.\Run, 2kadiras = 2kadiras.exe (file is missing)

HKLM\.\Run, adiras = adiras.exe (file is missing)

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

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

HKLM\...\Run, SunJavaUpdateSched = "C:\Programmi\Java\jre6\bin\jusched.exe"
HKLM\...\Run, avast! = C:\PROGRA~1\Avast4\ashDisp.exe
HKCU\...\Run, TOSCDSPD = C:\Programmi\TOSHIBA\TOSCDSPD\toscdspd.exe
HKCU\...\Run, Sonic RecordNow! = (file is missing)
HKCU\...\Run, NBJ = "C:\Programmi\Nero\Nero BackItUp\NBJ.exe"
HKCU\...\Run, kxva = C:\WINDOWS\system32\kxvo.exe (file is missing)
HKCU\...\Run, SpybotSD TeaTimer = C:\Programmi\Spybot S&D\TeaTimer.exe
HKCU\...\Run, wsyocic = "c:\documents and settings\alex\impostazioni locali\dati applicazioni\wsyocic.exe" wsyocic

Autostart shortcuts

Acrobat Assistant.lnk, ACROBA~1|Acrobat Assistant, C:\Programmi\Adobe\Acrobat 6.0\Distillr\acrotray.exe
Adobe Gamma Loader.lnk, , C:\Programmi\File comuni\Adobe\Calibration\Adobe Gamma Loader.exe
DSLMON.lnk, , C:\Programmi\ADSL\StarModem ADSL USB MODEM\dslmon.exe
RAMASST.lnk, , C:\WINDOWS\system32\RAMASST.exe
Tasto di scelta rapida per l'avvio di AutoCAD.lnk, Accelera la procedura di avvio di AutoCAD inserendo i dati nella memoria cache del disco, C:\Programmi\File comuni\Autodesk Shared\acstart16.exe
PowerReg SchedulerV2.exe, , C:\Documents and Settings\Alex\Menu Avvio\Programmi\Esecuzione automatica\PowerReg SchedulerV2.exe
Ritaglio schermata e avvio di OneNote 2007.lnk, Collegamento per ritaglio di schermata (Windows+S) e avvio (Windows+N) per Microsoft Office OneNote., C:\Programmi\Microsoft Office\Office12\ONENOTEM.EXE

Processes (16 whitelisted)

C:\WINDOWS\system32\Ati2evxx.exe
C:\Programmi\Avast4\aswUpdSv.exe
C:\Programmi\Avast4\ashServ.exe
C:\Programmi\TOSHIBA\Power Management\CeEPwrSvc.exe
C:\Programmi\TOSHIBA\ConfigFree\CFSvcs.exe
C:\WINDOWS\system32\DVRAMSV.exe
C:\Programmi\Java\jre6\bin\jqs.exe
C:\Programmi\File comuni\Microsoft Shared\VS7Debug\mdm.exe
C:\Programmi\Avast4\ashMaiSv.exe
C:\Programmi\Avast4\ashWebSv.exe
C:\Programmi\ATI Technologies\ATI Control Panel\atiptaxx.exe
C:\Programmi\Apoin2K\Apoin.exe
C:\Programmi\TOSHIBA\PadTouch\PadExe.exe
C:\WINDOWS\AGRSMMMSG.exe
C:\Programmi\TOSHIBA\Power Management\CePMTTray.exe
C:\Programmi\TOSHIBA\E-KEY\CeEKey.exe
C:\Programmi\EzButton\EzButton.EXE
C:\Programmi\TOSHIBA\TouchPad\TPTray.exe
C:\WINDOWS\System32\ZoomingHook.exe
C:\Programmi\TOSHIBA\TOSHIBA Zooming Utility\SmoothView.exe
C:\Programmi\TOSHIBA\ConfigFree\NDSTray.exe
C:\WINDOWS\system32\dla\lftswctrl.exe
C:\Programmi\File comuni\Real\Update_OB\realsched.exe
C:\PROGRA~1\Nokia\NOKIAP~1\LAUNCH~1.EXE
C:\Programmi\Microsoft Office\Office12\GrooveMonitor.exe
C:\Programmi\iTunes\iTunesHelper.exe
C:\Programmi\Java\jre6\bin\jusched.exe
C:\PROGRA~1\Avast4\ashDisp.exe
C:\Programmi\TOSHIBA\TOSCDSPD\toscdspd.exe
C:\Programmi\Spybot S&D\TeaTimer.exe
C:\documents and settings\alex\impostazioni locali\dati applicazioni\wsyocic.exe
C:\Programmi\Apoin2K\Apntex.exe
C:\Programmi\File comuni\PCSuite\Services\ServiceLayer.exe
C:\Programmi\Adobe\Acrobat 6.0\Distillr\acrotray.exe
C:\Programmi\ADSL\StarModem ADSL USB MODEM\dslmon.exe
C:\WINDOWS\system32\RAMASST.exe
C:\Programmi\iPod\bin\iPodService.exe
C:\WINDOWS\system32\WISPTIS.EXE
C:\Programmi\Windows Live\Mail\wlmail.exe
C:\Programmi\Windows Live\Contacts\wlcomm.exe
C:\Programmi\Mozilla Firefox\firefox.exe
C:\Programmi\FreeFixer\freefixer.exe

Application modules (48 whitelisted)

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\1040\mdmui.dll
C:\Programmi\File comuni\Microsoft Shared\VS7DEBUG\MSDBG2.DLL

Services (36 whitelisted)

aswUpdSv, avast! iAVS4 Control Service, c:\programmi\avast4\aswupdsv.exe
Ati HotKey Poller, , c:\windows\system32\ati2evxx.exe
avast! Antivirus, avast! Antivirus, c:\programmi\avast4\ashserv.exe
CeEPwrSvc, CeEPwrSvc, c:\programmi\toshiba\power management\ceepwrsvc.exe
CFSvcs, ConfigFree Service, c:\programmi\toshiba\configfree\cfsvcs.exe
DVD-RAM_Service, DVD-RAM_Service, c:\windows\system32\dvdramsv.exe
JavaQuickStarterService, Java Quick Starter, c:\programmi\java\jre6\bin\jqs.exe
MDM, Machine Debug Manager, c:\programmi\file comuni\microsoft shared\vs7debug\mdm.exe

Drivers (29 whitelisted)

ADILoader, General Purpose USB Driver (adldr.sys), C:\WINDOWS\system32\drivers\adldr.sys
drvmcdb, , C:\WINDOWS\system32\drivers\drvmcdb.sys
Netdevio, TOSHIBA Network Device Usermode I/O Protocol, C:\WINDOWS\system32\drivers\netdevio.sys
PxHelp20, PxHelp20, C:\WINDOWS\system32\drivers\pxhelp20.sys
SASDIFSV, SASDIFSV, c:\programmi\superantispyware\sasdifsv.sys
SASKUTIL, SASKUTIL, c:\programmi\superantispyware\saskutil.sys
SvcEKIOMngr, SvcEKIOMngr, C:\WINDOWS\system32\drivers\lekiomngr.sys
SvcEPECioctl, SvcEPECioctl, C:\WINDOWS\system32\drivers\ecioctl.sys
SvcEPIOMngr, SvcEPIOMngr, C:\WINDOWS\system32\drivers\epiomngr.sys
SvcSSIOMngr, SvcSSIOMngr, C:\WINDOWS\system32\drivers\ssiomngr.sys
SvcTPIOMngr, SvcTPIOMngr, C:\WINDOWS\system32\drivers\tpiomngr.sys

=====