

# Aiutatemi non capisco nulla

Posted by foneit - 2009/02/16 00:16

FreeFixer v0.32 log

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

Operating system: Windows XP Service Pack 3

Log dated 2009-02-15 22:52

UserInits

C:\WINDOWS\system32\userinit.exe

Winlogon Notify

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

crypt32chain - C:\WINDOWS\system32\crypt32.dll

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

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

dimsntfy - C:\WINDOWS\System32\dimsntfy.dll

ScCertProp - C:\WINDOWS\system32\wlnotify.dll

Schedule - C:\WINDOWS\system32\wlnotify.dll

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

SensLogn - C:\WINDOWS\system32\WlNotify.dll

termsrv - C:\WINDOWS\system32\wlnotify.dll

wlballoon - C:\WINDOWS\system32\wlnotify.dll

TCP/IP settings

HKLM\..Interfaces\{C54EEF9C-C6CF-4214-94DC-7C85602F6C10}, NameServer = 91.188.0.5,91.188.0.35

Transport service providers

{FFE241A1-EE47-497C-8CE8-6A127E43CEA6} - C:\WINDOWS\system32\imon.dll

{5B3C504D-63BF-41DD-9B17-DF7AF8D58744} - C:\WINDOWS\system32\imon.dll

{6A12B9CF-9743-47B5-9ABE-28D71F751EF4} - C:\WINDOWS\system32\imon.dll

{07E80168-EDD5-4676-A142-B9414D1D9DA4} - C:\WINDOWS\system32\imon.dll

{828B43A3-43B7-4C80-88B3-30AE9B54E02E} - C:\WINDOWS\system32\imon.dll

{E70F1AA0-AB8B-11CF-8CA3-00805F48A192} - C:\WINDOWS\system32\mswsock.dll

{9D60A9E0-337A-11D0-BD88-0000C082E69A} - C:\WINDOWS\system32\rsvpsp.dll

{8D5F1830-C273-11CF-95C8-00805F48A192} - C:\WINDOWS\system32\mswsock.dll

{28A4D8DA-E908-4C6F-A926-A66CC7AD3224} - C:\WINDOWS\system32\imon.dll

Namespace service providers

{22059D40-7E9E-11CF-AE5A-00AA00A7112B} - C:\WINDOWS\System32\mswsock.dll

{3B2637EE-E580-11CF-A555-00C04FD8D4AC} - C:\WINDOWS\System32\winrnr.dll

{6642243A-3BA8-4AA6-BAA5-2E0BD71FDD83} - C:\WINDOWS\System32\mswsock.dll

Browser Helper Objects

{18DF081C-E8AD-4283-A596-FA578C2EBDC3}, Adobe PDF Link Helper, C:\Programmi\File

comuni\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll

{4f3ed5cd-0726-42a9-87f5-d13f3d2976ac}, Windows Live OneCare Family Safety Browser Helper Class,

C:\Programmi\Windows Live\Family Safety\fsbho.dll

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

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

Office\Office12\GrooveShellExtensions.dll

{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}, SSVHelper Class, C:\Programmi\Java\jre1.6.0\_07\bin\ssv.dll

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

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

comuni\Microsoft Shared\Windows Live\WindowsLiveLogin.dll

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

Toolbar\msntb.dll

{bf00e119-21a3-4fd1-b178-3b8537e75c92}, leMonitorBho Class, C:\Programmi\Megaupload\Mega

Manager\MegaIEMn.dll

Internet Explorer toolbars

HKLM\..Toolbar\{BDAD1DAD-C946-4A17-ADC1-64B5B4FF55D0} - Windows Live Toolbar - C:\Programmi\Windows

Live Toolbar\msntb.dll

HKCU\..Toolbar\WebBrowser\{01E04581-4EEE-11D0-BFE9-00AA005B4383} - &Indirizzo -

C:\WINDOWS\system32\browseui.dll  
HKCU\..\Toolbar\WebBrowser\{0E5CBF21-D15F-11D0-8301-00AA005B4383} - Co&Illegamenti -  
C:\WINDOWS\system32\SHELL32.dll  
HKCU\..\Toolbar\WebBrowser\{32099AAC-C132-4136-9E9A-4E364A424E17} - - No file specified

Basic Internet Explorer settings  
HKCU\..\Main, Start Page = http://www.google.it/

Registry Startups  
HKLM\..\Run, nod32kui = "C:\Programmi\Eset\nod32kui.exe" /WAITSERVICE  
HKLM\..\Run, TrojanScanner = C:\Programmi\Trojan Remover\Trjscan.exe /boot  
HKCU\..\Run, ctfmon.exe = C:\WINDOWS\system32\ctfmon.exe  
HKCU\..\Run, msnmsgr = "C:\Programmi\Windows Live\Messenger\msnmsgr.exe" /background  
HKCU\..\Run, Google Update = "C:\Documents and Settings\Michele\Impostazioni locali\Dati applicazioni\Google\Update\GoogleUpdate.exe" /c

Shared schedulers  
Precaricatore Browseui, {438755C2-A8BA-11D1-B96B-00A0C90312E1}, C:\WINDOWS\system32\browseui.dll  
Daemon di cache delle categorie di componenti, {8C7461EF-2B13-11d2-BE35-3078302C2030},  
C:\WINDOWS\system32\browseui.dll

Processes  
C:\WINDOWS\System32\smss.exe  
C:\WINDOWS\system32\csrss.exe  
C:\WINDOWS\system32\winlogon.exe  
C:\WINDOWS\system32\services.exe  
C:\WINDOWS\system32\lsass.exe  
C:\WINDOWS\system32\Ati2evxx.exe  
C:\WINDOWS\system32\svchost.exe  
C:\WINDOWS\system32\svchost.exe  
C:\WINDOWS\System32\svchost.exe  
C:\WINDOWS\system32\svchost.exe  
C:\WINDOWS\system32\svchost.exe  
C:\WINDOWS\system32\Ati2evxx.exe  
C:\WINDOWS\system32\spoolsv.exe  
C:\WINDOWS\Explorer.EXE  
C:\Programmi\Eset\nod32kui.exe  
C:\WINDOWS\system32\ctfmon.exe  
C:\Documents and Settings\Michele\Impostazioni locali\Dati applicazioni\Google\Update\GoogleUpdate.exe  
C:\Programmi\File comuni\Autodata Limited Shared\Service\ADCDCLicSvc.exe  
C:\WINDOWS\system32\CTsvcCDA.exe  
C:\Programmi\Windows Live\Family Safety\fsnssvc.exe  
C:\Programmi\Power Translator 12\LogoMedia TranslateDotNet Server.exe  
C:\Programmi\File comuni\Microsoft Shared\VS7DEBUG\mdm.exe  
C:\Programmi\Nero\Nero8\Nero BackItUp\NBService.exe  
C:\Programmi\Eset\nod32kui.exe  
C:\WINDOWS\system32\loctlsvc.exe  
C:\WINDOWS\system32\PSISvc.exe  
C:\Programmi\Alcohol Soft\Alcohol 120\StarWind\StarWindServiceAE.exe  
C:\WINDOWS\system32\svchost.exe  
C:\WINDOWS\system32\MsPMSPV.exe  
C:\WINDOWS\system32\SearchIndexer.exe  
C:\WINDOWS\System32\alg.exe  
C:\Programmi\Windows Live\Messenger\usnsvc.exe  
C:\Programmi\Internet Explorer\iexplore.exe  
C:\Programmi\File comuni\Microsoft Shared\Windows Live\WLLLoginProxy.exe  
C:\Programmi\Windows Live\Messenger\msnmsgr.exe  
C:\Documents and Settings\Michele\Dati applicazioni\Simply Super Software\Trojan Remover\cdg13E6.exe  
C:\Programmi\FreeFixer\freefixer.exe

Application modules (1 whitelisted)  
C:\WINDOWS\system32\ntdll.dll  
C:\WINDOWS\system32\kernel32.dll  
C:\WINDOWS\system32\VERSION.dll  
C:\WINDOWS\system32\sfc.dll

C:\WINDOWS\system32\sfc\_os.dll  
C:\WINDOWS\system32\USER32.dll  
C:\WINDOWS\system32\GDI32.dll  
C:\WINDOWS\system32\RPCRT4.dll  
C:\WINDOWS\system32\ADVAPI32.dll  
C:\WINDOWS\system32\Secur32.dll  
C:\WINDOWS\system32\WINTRUST.dll  
C:\WINDOWS\system32\CRYPT32.dll  
C:\WINDOWS\system32\MSASN1.dll  
C:\WINDOWS\system32\msvcrt.dll  
C:\WINDOWS\system32\IMAGEHLP.dll  
C:\WINDOWS\system32\ole32.dll  
C:\WINDOWS\system32\comdlg32.dll  
C:\WINDOWS\system32\COMCTL32.dll  
C:\WINDOWS\system32\SHELL32.dll  
C:\WINDOWS\system32\SHLWAPI.dll  
C:\WINDOWS\system32\WINSPOOL.DRV  
C:\WINDOWS\system32\oledlg.dll  
C:\WINDOWS\system32\OLEAUT32.dll  
C:\WINDOWS\system32\WS2\_32.dll  
C:\WINDOWS\system32\WS2HELP.dll  
C:\WINDOWS\system32\IMM32.DLL  
C:\WINDOWS\system32\uxtheme.dll  
C:\WINDOWS\system32\PSAPI.dll  
C:\WINDOWS\system32\MSCTF.dll  
C:\WINDOWS\system32\msctfime.ime  
C:\WINDOWS\system32\CLBCATQ.DLL  
C:\WINDOWS\system32\COMRes.dll  
C:\WINDOWS\system32\ieframe.dll  
C:\WINDOWS\system32\iertutil.dll  
C:\WINDOWS\system32\WININET.dll  
C:\WINDOWS\system32\Normaliz.dll  
C:\WINDOWS\system32\urlmon.dll  
C:\WINDOWS\system32\appHelp.dll  
C:\WINDOWS\system32\mshhtml.dll  
C:\WINDOWS\system32\msls31.dll  
C:\WINDOWS\system32\mlang.dll  
C:\WINDOWS\system32\msimtf.dll  
C:\WINDOWS\system32\mslbui.dll  
C:\WINDOWS\system32\mshtml.dll

#### Services

Ati HotKey Poller, , c:\windows\system32\ati2evxx.exe  
ATI Smart, ATI Smart, c:\windows\system32\ati2sgag.exe  
AudioSrv, Audio Windows, c:\windows\system32\svchost.exe  
Autodata Limited License Service, Autodata Limited License Service, c:\programmi\file comuni\autodata limited shared\service\adcdlicsv.exe  
Browser, Browser di computer, c:\windows\system32\svchost.exe  
Creative Service for CDROM Access, Creative Service for CDROM Access, c:\windows\system32\ctsvccda.exe  
CryptSvc, Servizi di crittografia, c:\windows\system32\svchost.exe  
DcomLaunch, Utilità di avvio processo server DCOM, c:\windows\system32\svchost.exe  
Dhcp, Client DHCP, c:\windows\system32\svchost.exe  
Dnscache, Client DNS, c:\windows\system32\svchost.exe  
Eventlog, Registro eventi, c:\windows\system32\services.exe  
fsssvc, Windows Live OneCare Family Safety, c:\programmi\windows live\family safety\fssvc.exe  
helpsvc, Guida in linea e supporto tecnico, c:\windows\system32\svchost.exe  
hpdj, hpdj, c:\docume~1\michele\impost~1\temp\hpdj.exe (file is missing)  
LanmanServer, Server, c:\windows\system32\svchost.exe  
lanmanworkstation, Workstation, c:\windows\system32\svchost.exe  
LEC TranslateDotNet Server, LEC TranslateDotNet Server, c:\programmi\power translator 12\logomedia translatedotnet server.exe  
LmHosts, Helper NetBIOS di TCP/IP, c:\windows\system32\svchost.exe  
MDM, Machine Debug Manager, c:\programmi\file comuni\microsoft shared\vs7debug\mdm.exe  
Nero BackItUp Scheduler 3, Nero BackItUp Scheduler 3, c:\programmi\nero\nero8\nero backup\nbservice.exe  
NOD32krn, NOD32 Kernel Service, c:\programmi\eset\nod32krn.exe

PLFlash DeviceControl Service, PLFlash DeviceControl Service, c:\windows\system32\ioctlsvc.exe  
PlugPlay, Plug and Play, c:\windows\system32\services.exe  
PolicyAgent, Servizi IPSEC, c:\windows\system32\lsass.exe  
ProtectedStorage, Archiviazione protetta, c:\windows\system32\lsass.exe  
ProtexisLicensing, ProtexisLicensing, c:\windows\system32\psiservice.exe  
RpcSs, RPC (Remote Procedure Call), c:\windows\system32\svchost.exe  
SamSs, Gestione account di protezione (SAM), c:\windows\system32\lsass.exe  
Schedule, Utilità di pianificazione, c:\windows\system32\svchost.exe  
seclogon, Accesso secondario, c:\windows\system32\svchost.exe  
SENS, Notifica eventi di sistema, c:\windows\system32\svchost.exe  
SharedAccess, Windows Firewall / Condivisione connessione Internet (ICS), c:\windows\system32\svchost.exe  
ShellHWDetection, Rilevamento hardware shell, c:\windows\system32\svchost.exe  
Spooler, Spooler di stampa, c:\windows\system32\spoolsv.exe  
srsservice, Servizio Ripristino configurazione di sistema, c:\windows\system32\svchost.exe  
StarWindServiceAE, StarWind AE Service, c:\programmi\alcohol soft\alcohol 120\starwind\starwindserviceae.exe  
stisvc, Acquisizione di immagini di Windows (WIA), c:\windows\system32\svchost.exe  
Themes, Temi, c:\windows\system32\svchost.exe  
TrkWks, Manutenzione collegamenti distribuiti client, c:\windows\system32\svchost.exe  
W32Time, Ora di Windows, c:\windows\system32\svchost.exe  
WebClient, WebClient, c:\windows\system32\svchost.exe  
winmgmt, Strumentazione gestione Windows, c:\windows\system32\svchost.exe  
WMDM PMSP Service, WMDM PMSP Service, c:\windows\system32\mspmmsp.exe  
wscsvc, Centro sicurezza PC, c:\windows\system32\svchost.exe  
WSearch, Windows Search, c:\windows\system32\searchindexer.exe  
wuauerv, Aggiornamenti automatici, c:\windows\system32\svchost.exe  
WZCSVC, Zero Configuration reti senza fili, c:\windows\system32\svchost.exe

#### Shell services

PostBootReminder, {7849596a-48ea-486e-8937-a2a3009f31a9}, C:\WINDOWS\system32\SHELL32.dll  
CDBurn, {fbeb8a05-beee-4442-804e-409d6c4515e9}, C:\WINDOWS\system32\SHELL32.dll  
WebCheck, {E6FB5E20-DE35-11CF-9C87-00AA005127ED}, C:\WINDOWS\system32\webcheck.dll  
SysTray, {35CEC8A3-2BE6-11D2-8773-92E220524153}, C:\WINDOWS\system32\stobject.dll  
WPDSHServiceObj, {AAA288BA-9A4C-45B0-95D7-94D524869DB5}, C:\WINDOWS\system32\WPDSHServiceObj.dll

#### Drivers

ACPI, Driver ACPI Microsoft, C:\WINDOWS\system32\drivers\acpi.sys  
AFD, AFD, C:\WINDOWS\system32\drivers\afd.sys  
agp440, Filtro bus Intel AGP, C:\WINDOWS\system32\drivers\agp440.sys  
AMON, AMON, C:\WINDOWS\system32\drivers\amon.sys  
atapi, Controller disco rigido IDE/ESDI standard, C:\WINDOWS\system32\drivers\atapi.sys  
BootScreen, , C:\WINDOWS\system32\drivers\vidstub.sys  
Cdrom, Driver del CD-ROM, C:\WINDOWS\system32\drivers\cdrom.sys  
Disk, Driver del disco, C:\WINDOWS\system32\drivers\disk.sys  
dk2drv, DK2 WindowsNT Driver, c:\windows\system32\drivers\dk2drv.sys  
ElbyCDIO, ElbyCDIO Driver, C:\WINDOWS\system32\drivers\elbycdio.sys  
FLE5WNNT, FLE-5 WindowsNT Driver, c:\windows\system32\drivers\fle5wnnt.sys  
FLSIface, FLSIface, c:\windows\system32\drivers\flsiface.sys  
FLSPAR, FLSPar, c:\windows\system32\drivers\flspar.sys  
FLSSER, FLSSer, c:\windows\system32\drivers\flsfer.sys  
FLSVCOM, FLSVCom, c:\windows\system32\drivers\flsvcom.sys  
fssfltr, FssFltr, C:\WINDOWS\system32\drivers\fssfltr.sys  
Ftdisk, Driver archiviazione volumi, C:\WINDOWS\system32\drivers\ftdisk.sys  
i8042prt, Driver di porta mouse PS/2 e tastiera i8042, C:\WINDOWS\system32\drivers\i8042prt.sys  
Imapi, Driver filtro masterizzazione CD, C:\WINDOWS\system32\drivers\imapi.sys  
IntelIde, , C:\WINDOWS\system32\drivers\intelide.sys  
intelppm, Driver processore Intel, C:\WINDOWS\system32\drivers\intelppm.sys  
IPSec, Driver IPSEC, C:\WINDOWS\system32\drivers\ipsec.sys  
isapnp, Driver bus PnP ISA/EISA, C:\WINDOWS\system32\drivers\isapnp.sys  
Kbdclass, Driver classe tastiera, C:\WINDOWS\system32\drivers\kbdclass.sys  
Mouclass, Driver classe mouse, C:\WINDOWS\system32\drivers\mouclass.sys  
NetBT, NetBios su Tcpip, C:\WINDOWS\system32\drivers\netbt.sys  
nod32drv, nod32drv, C:\WINDOWS\system32\drivers\nod32drv.sys  
ohci1394, Host controller VIA OHCI compatibile IEEE 1394, C:\WINDOWS\system32\drivers\ohci1394.sys  
PARLDR2K, ParLdr2k, c:\windows\system32\drivers\parldr2k.sys  
PCI, Driver bus PCI, C:\WINDOWS\system32\drivers\pci.sys

---

PCIIde, , C:\WINDOWS\system32\drivers\pciide.sys  
PfModNT, , c:\windows\system32\drivers\pfmodnt.sys  
RasAcD, Driver connessione automatica Accesso remoto, C:\WINDOWS\system32\drivers\rasacd.sys  
RDPCDD, , C:\WINDOWS\system32\drivers\rdpcdd.sys  
redbook, Driver filtro riproduzione CD-ROM audio digitale, C:\WINDOWS\system32\drivers\redbook.sys  
Serial, Driver della porta seriale, C:\WINDOWS\system32\drivers\serial.sys  
sptd, , C:\WINDOWS\system32\drivers\sptd.sys  
An error occurred when trying to open the file for reading.  
Filename: 'C:\WINDOWS\system32\drivers\sptd.sys'.  
Current Working Directory: 'C:\Programmi\FreeFixer'.  
System error message: Impossibile accedere al file. Il file è utilizzato da un altro processo. Error code: 32.  
C++ exception: ios\_base::failbit set  
Tcpip, Driver protocollo TCP/IP, C:\WINDOWS\system32\drivers\tcpip.sys  
TermDD, Driver della periferica terminale, C:\WINDOWS\system32\drivers\termdd.sys  
VgaSave, , C:\WINDOWS\system32\drivers\vga.sys  
wceusbsh, Driver host USB seriale Windows CE, C:\WINDOWS\system32\drivers\wceusbsh.sys  
WS2IFSL, Ambiente di supporto del provider del Servizio Non-IFS di Windows Socket 2.0,  
C:\WINDOWS\system32\drivers\ws2ifsl.sys

=====