

I need some help with my log files

Posted by goldman - 2008/02/26 01:45

I have no clue on what files I have to fix or delete can some one help me

Here are my log files

FreeFixer v0.27 log

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

Operating system: Windows XP Service Pack 2

Log dated 2008-02-25 20:43

Winlogon Notify (9 whitelisted)

!SABWinLogon - C:\Arquivos de programas\SuperAdBlocker.com\Super Ad Blocker\SABWINLO.DLL

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

Browser Helper Objects

{00000000-6C30-11D8-9363-000AE6309654}, SuperAdBlockerBHO Class, C:\Arquivos de programas\SuperAdBlocker.com\Super Ad Blocker\SABBHO.dll

{02478D38-C3F9-4EFB-9B51-7695ECA05670}, Yahoo! Toolbar Helper, C:\Arquivos de programas\Yahoo!\Companion\Installs\cpn\yt.dll

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

{25CEE8EC-5730-41bc-8B58-22DDC8AB8C20}, Winamp Toolbar BHO, C:\Arquivos de programas\Winamp Toolbar\winamptb.dll

{72853161-30C5-4D22-B7F9-0BBC1D38A37E}, Groove GFS Browser Helper, C:\ARQUIV~1\MICROS~2\Office12\GRA8E1~1.DLL

{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}, SSVHelper Class, C:\Arquivos de programas\Java\jre1.6.0_03\bin\ssv.dll

{AF69DE43-7D58-4638-B6FA-CE66B5AD205D}, Google Toolbar Notifier BHO, C:\Arquivos de programas\Google\GoogleToolbarNotifier2.1.1119.1736\swg.dll

{BDF3E430-B101-42AD-A544-FADC6B084872}, CNavExtBho Class, C:\Arquivos de programas\Norton SystemWorks\Norton AntiVirus\NavShExt.dll

Internet Explorer toolbars (2 whitelisted)

HKLM\...\Toolbar\{42CDD1BF-3FFB-4238-8AD1-7859DF00B1D6} - Norton AntiVirus - C:\Arquivos de programas\Norton SystemWorks\Norton AntiVirus\NavShExt.dll

HKLM\...\Toolbar\{EBF2BA02-9094-4c5a-858B-BB198F3D8DE2} - Winamp Toolbar - C:\Arquivos de programas\Winamp Toolbar\winamptb.dll

HKLM\...\Toolbar\{EF99BD32-C1FB-11D2-892F-0090271D4F88} - Barra de Ferramentas do Yahoo! com bloqueador de pop-up - C:\Arquivos de programas\Yahoo!\Companion\Installs\cpn\yt.dll

HKLM\...\Toolbar\{B4B3001E-0F56-4E51-8250-BDE11547EC55} - Super Ad Blocker Toolbar - C:\Arquivos de programas\SuperAdBlocker.com\Super Ad Blocker\sabtb.dll

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

HKCU\...\Toolbar\ShellBrowser\{AB455519-4E14-498B-A0A9-7DCEF42440FC} - - No file specified

HKCU\...\Toolbar\WebBrowser\{4E7BD74F-2B8D-469E-CCB0-B130EEDBE97C} - - No file specified

Basic Internet Explorer settings

HKCU\...\Main, Start Page = <http://br.msn.com/>

HKLM\...\Main, Default_Page_URL = <http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome>

HKLM\...\Main, Default_Search_URL = <http://www.google.com/ie>

Registry Startups (1 whitelisted)

HKLM\...\Run, InCD = C:\Arquivos de programas\Ahead\InCD\InCD.exe

Error getting translation table with 'VerQueryValue' for the file 'C:\Arquivos de programas\Ahead\InCD\InCD.exe'. System error message: Não foi possível encontrar o tipo de recurso especificado no arquivo de imagem.

HKLM\...\Run, LGODDFU = "C:\Arquivos de programas\lg_fwupdate\fwupdate.exe"

HKLM\...\Run, SoundMan = SOUNDMAN.EXE

HKLM\...\Run, ISUSPM Startup = "C:\Arquivos de programas\Arquivos comuns\InstallShield\UpdateService\isuspm.exe" - startup

HKLM\...\Run, ISUSScheduler = "C:\Arquivos de programas\Arquivos comuns\InstallShield\UpdateService\issch.exe" - start

HKLM\...\Run, NAV Agent = C:\ARQUIV~1\NORTON~1\NORTON~1\navapw32.exe
HKLM\...\Run, Adobe Photo Downloader = "C:\Arquivos de programas\Adobe\Photoshop Album Starter Edition\3.2\Apps\lapdproxy.exe"
HKLM\...\Run, Adobe Reader Speed Launcher = "C:\Arquivos de programas\Adobe\Reader 8.0\Reader\Reader_sl.exe"
HKLM\...\Run, GrooveMonitor = "C:\Arquivos de programas\Microsoft Office\Office12\GrooveMonitor.exe"
HKLM\...\Run, RemoteControl = "C:\Arquivos de programas\CyberLink\PowerDVD\PDVDServ.exe"
HKLM\...\Run, SunJavaUpdateSched = "C:\Arquivos de programas\Java\jre1.6.0_03\bin\jusched.exe"
HKLM\...\Run, ISTRay = "C:\Arquivos de programas\Spyware Doctor\pctsTray.exe"
HKLM\...\Run, 00PCTFW = "C:\Arquivos de programas\PC Tools Firewall Plus\FirewallGUI.exe" -s
HKLM\...\Run, combofix = C:\WINDOWS\system32\kmd.exe /c C:\ComboFix(2)\Combobatch.bat
HKCU\...\Run, MSMSGs = "C:\Arquivos de programas\Messenger\msmsgs.exe" /background
HKCU\...\Run, swg = C:\Arquivos de programas\Google\GoogleToolbarNotifier\GoogleToolbarNotifier.exe
Error getting translation table with 'VerQueryValue' for the file 'C:\Arquivos de programas\Google\GoogleToolbarNotifier\GoogleToolbarNotifier.exe'. System error message: Não foi possível encontrar o tipo de recurso especificado no arquivo de imagem.

HKCU\...\Run, SuperAdBlocker = C:\Arquivos de programas\SuperAdBlocker.com\Super Ad Blocker\SAdBlock.exe

Autostart shortcuts

Adobe Gamma Loader.exe.Ink, , C:\Arquivos de programas\Arquivos comuns\Adobe\Calibration\Adobe Gamma Loader.exe

Recorte de tela e Iniciador do OneNote 2007.Ink, Recorte de tela (Windows+S) e Iniciador (Windows+N) para Microsoft Office OneNote., C:\Arquivos de programas\Microsoft Office\Office12\ONENOTEM.EXE

Processes (15 whitelisted)

C:\Arquivos de programas\PC Tools Firewall Plus\FWService.exe
C:\Arquivos de programas\Ahead\InCD\InCDsrv.exe
C:\Arquivos de programas\SuperAdBlocker.com\Super Ad Blocker\SABSVc.EXE
C:\Arquivos de programas\Spyware Doctor\pctsAuxs.exe
C:\Arquivos de programas\Spyware Doctor\pctsSvc.exe
C:\ARQUIV~1\NORTON~1\SPEEDD~1\nopdb.exe
C:\WINDOWS\SOUNDMAN.EXE
C:\Arquivos de programas\Arquivos comuns\InstallShield\UpdateService\issch.exe
C:\Arquivos de programas\Adobe\Photoshop Album Starter Edition\3.2\Apps\lapdproxy.exe
C:\Arquivos de programas\CyberLink\PowerDVD\PDVDServ.exe
C:\Arquivos de programas\Spyware Doctor\pctsTray.exe
C:\Arquivos de programas\PC Tools Firewall Plus\FirewallGUI.exe
C:\Arquivos de programas\Messenger\msmsgs.exe
C:\Arquivos de programas\SuperAdBlocker.com\Super Ad Blocker\SAdBlock.exe
C:\Arquivos de programas\Mozilla Firefox\firefox.exe
C:\Arquivos de programas\FreeFixer\freefixer.exe

Application modules (59 whitelisted)

C:\Arquivos de programas\Spyware Doctor\smumhook.dll
C:\Arquivos de programas\SuperAdBlocker.com\Super Ad Blocker\sabmsghk.dll
C:\ARQUIV~1\MICROS~2\Office12\GRA8E1~1.DLL
C:\ARQUIV~1\MICROS~2\Office12\GrooveUtil.DLL
C:\ARQUIV~1\MICROS~2\Office12\GrooveNew.DLL
C:\Arquivos de programas\MSN Messenger\fssexhext.8.1.0178.00.dll
C:\ARQUIV~1\MICROS~2\Office12\GR99D3~1.DLL

Services (33 whitelisted)

InCDsrv, InCD Helper, c:\arquivos de programas\ahead\incd\incdsrv.exe
PCToolsFirewallPlus, PC Tools Firewall Plus, c:\arquivos de programas\pc tools firewall plus\fwservice.exe
SABSVc, Super Ad Blocker Service, c:\arquivos de programas\superadblocker.com\super ad blocker\sabsvc.exe
sdAuxService, PC Tools Auxiliary Service, c:\arquivos de programas\spyware doctor\pctsauxs.exe
sdCoreService, PC Tools Security Service, c:\arquivos de programas\spyware doctor\pctssvc.exe
Speed Disk service, Speed Disk service, c:\arquiv~1\norton~1\speedd~1\nopdb.exe

Drivers (26 whitelisted)

AvgAsCln, AVG Anti-Spyware Clean Driver, C:\WINDOWS\system32\drivers\avgascln.sys
IKSysFlt, System Filter Driver, C:\WINDOWS\system32\drivers\iksysflt.sys
IKSysSec, System Security Driver, C:\WINDOWS\system32\drivers\iksyssec.sys
InCDPass, InCDPass, C:\WINDOWS\system32\drivers\incdpass.sys
pctfw2, pctfw2, c:\windows\system32\drivers\pctfw2.sys

pctmp, PC Tools Firewall Memory Protection Driver, C:\WINDOWS\system32\drivers\pctmp.sys
pctssipc, PC Tools Security Suite IPC Driver, C:\WINDOWS\system32\drivers\pctssipc.sys
PxHelp20, PxHelp20, C:\WINDOWS\system32\drivers\pxhelp20.sys
SABDIFSV, SABDIFSV, c:\arquivos de programas\superadblocker.com\super ad blocker\sabdifsv.sys
SABKUTIL, SABKUTIL, c:\arquivos de programas\superadblocker.com\super ad blocker\sabkutil.sys
SYMTDI, SYMTDI, c:\windows\system32\drivers\symtdi.sys

=====

Re:I need some help with my log files

Posted by securitywonks - 2008/03/27 08:07

I donot find much suspicious files, at first you scan yourcomputer with Bitdefender Online Scan and Spybot (with latest updates)

=====

use BITDEFENDER with INTERNET EXPLORER:
<http://www.bitdefender.com/scan8/ie.html>

remove, what it says, it is an online antivirus

Install SPYBOT software, update definitions and then scan and remove what it says:

<http://projects.securitywonks.net/projects/details.php?file=2>

post the latest log after that,

all the best with your system

=====