

Re: Home Page

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help_and_support/2004-05/4634.html

From: Lawrence (*lawrencsystemsno spam_at_isp.com*)

Date: 05/11/04

Date: Tue, 11 May 2004 18:48:29 -0400

I believe if I were in your shoes, I would run spy-bot and check mark all the errors ad ware and spyware that it finds and remove ALL of them. .

"H" <anonymous@discussions.microsoft.com> wrote in message news:9C5AA420-9423-4BF2-8D3C-E2204FF9BDE9@microsoft.com...

> *Hi*

> *I have download hijack and done the scan. the warning given before deleting and to consult knowledgable folk.*

>

> *just Like to add before pasting the log is that my computer has a few problems all occurring at the same time.*

>

> *1) home page (riviera.cc changing to search-town .net*

> *2) on log in generic host process for win 32 services*

> *3) no sound*

> *4) can not get into media player*

> *5) trojan virus which has been detected and cleared by norton.*

>

> *I know if you delete certain things they can effect other so Im asking the experts.*

>

> *thanks.*

>

> *log*

>

>

> *Running processes:*

> *C:\WINDOWS\System32\smss.exe*

> *C:\WINDOWS\system32\winlogon.exe*

> *C:\WINDOWS\system32\services.exe*

> *C:\WINDOWS\system32\lsass.exe*

> *C:\WINDOWS\system32\svchost.exe*

> *C:\WINDOWS\system32\spoolsv.exe*

> *C:\Program Files\Norton AntiVirus\navapvc.exe*

> *C:\WINDOWS\System32\nvsvc32.exe*

> *C:\WINDOWS\System32\svchost.exe*

> *C:\WINDOWS\Explorer.EXE*

- > C:\Program Files\Alcatel\SpeedTouch USB\Dragdiag.exe
- > C:\PROGRA~1\NORTON~1\navapw32.exe
- > C:\Program Files\Hewlett-Packard\Digital Imaging\bin\hpobnz08.exe
- > C:\Program Files\Hewlett-Packard\Digital Imaging\bin\hpotdd01.exe
- > C:\Program Files\Hewlett-Packard\Digital Imaging\bin\hpoevm08.exe
- > C:\Program Files\Hewlett-Packard\Digital Imaging\Bin\hpoSTS08.exe
- > C:\WINDOWS\System32\svchost.exe
- > C:\Program Files\Internet Explorer\iexplore.exe
- > C:\Documents and Settings\Danny\Local Settings\Temp\Temporary Directory 2 for hijackthis.zip\HijackThis.exe
- >
- > R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar = <http://opti.riviera.cc> (obfuscated)
- > R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page = <http://opti.riviera.cc> (obfuscated)
- > R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page = <http://riviera.cc> (obfuscated)
- > R1 - HKCU\Software\Microsoft\Internet Explorer\Search,SearchAssistant = <http://opti.riviera.cc> (obfuscated)
- > R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Start Page = <http://riviera.cc> (obfuscated)
- > R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Bar = <http://opti.riviera.cc> (obfuscated)
- > R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Page = <http://opti.riviera.cc> (obfuscated)
- > R0 - HKLM\Software\Microsoft\Internet Explorer\Search,SearchAssistant = <http://opti.riviera.cc> (obfuscated)
- > R1 - HKCU\Software\Microsoft\Internet Explorer\Main,HomeOldSP = <http://riviera.cc> (obfuscated)
- > O2 - BHO: (no name) - {055D7684-71E2-48B7-8E13-29BCC5CA14F6} - C:\WINDOWS\system32\ckycic.dll
- > O2 - BHO: (no name) - {06849E9F-C8D7-4D59-B87D-784B7D6BE0B3} - C:\Program Files\Adobe\Acrobat 5.0\Reader\ActiveX\AcroIEHelper.ocx
- > O2 - BHO: (no name) - {53707962-6F74-2D53-2644-206D7942484F} - C:\PROGRA~1\SPYBOT~1.1\SDHelper.dll
- > O2 - BHO: NAV Helper - {BDF3E430-B101-42AD-A544-FADC6B084872} - C:\Program Files\Norton AntiVirus\NavShExt.dll
- > O2 - BHO: (no name) - {EBCDDA60-2A68-11D3-8A43-0060083CFB9C} - C:\WINDOWS\System32\nzdd.dll
- > O2 - BHO: (no name) - {EF99BD32-C1FB-11D2-892F-0090271D4F88} - (no file)
- > O3 - Toolbar: Norton AntiVirus - {42CDD1BF-3FFB-4238-8AD1-7859DF00B1D6} - C:\Program Files\Norton AntiVirus\NavShExt.dll
- > O3 - Toolbar: &Radio - {8E718888-423F-11D2-876E-00A0C9082467} - C:\WINDOWS\System32\msdxm.ocx
- > O4 - HKLM\..\Run: [WeatherOnTray] C:\Program Files\Hotbar\bin\4.4.5.0\WeatherOnTray.exe
- > O4 - HKLM\..\Run: [sys] regedit -s sysdll.reg
- > O4 - HKLM\..\Run: [StorageGuard] "C:\Program Files\VERITAS Software\Update Manager\sgtray.exe" /r
- > O4 - HKLM\..\Run: [SpeedTouch USB Diagnostics] "C:\Program Files\Alcatel\SpeedTouch USB\Dragdiag.exe" /icon

- > 04 – HKLM\..\Run: [PPMemCheck] "C:\Program Files\PestPatrol\PPMemCheck.exe"
- > 04 – HKLM\..\Run: [nwiz] nwiz.exe /install
- > 04 – HKLM\..\Run: [NvCplDaemon] RUNDLL32.EXE C:\WINDOWS\System32\NvCpl.dll,NvStartup
- > 04 – HKLM\..\Run: [NeroCheck] C:\WINDOWS\system32\NeroCheck.exe
- > 04 – HKLM\..\Run: [NAV Agent] C:\PROGRA~1\NORTON~1\navapw32.exe
- > 04 – HKLM\..\Run: [Microsoft Tray] A:\games.exe
- > 04 – Global Startup: Gator eWallet.lnk = C:\Program Files\Gator.com\OfferCompanion\Offers.exe
- > 04 – Global Startup: hp psc 2000 Series.lnk = C:\Program Files\Hewlett-Packard\Digital Imaging\bin\hpobnz08.exe
- > 04 – Global Startup: hpoddt01.exe.lnk = ?
- > 04 – Global Startup: RealDownload.lnk = C:\Program Files\Real\RealDownload\Realdownload.exe
- > 09 – Extra button: Real.com (HKLM)
- > 09 – Extra button: Messenger (HKLM)
- > 09 – Extra 'Tools' menuitem: Messenger (HKLM)
- > 09 – Extra button: Medion-UK (HKCU)
- > 012 – Plugin for .au: C:\Program Files\Internet Explorer\PLUGINS\npqtplugin.dll
- > 012 – Plugin for .mid: C:\Program Files\Internet Explorer\PLUGINS\npqtplugin.dll
- > 012 – Plugin for .mov: C:\Program Files\Internet Explorer\PLUGINS\npqtplugin.dll
- > 012 – Plugin for .pdf: C:\Program Files\Internet Explorer\PLUGINS\nppdf32.dll
- > 012 – Plugin for .spop: C:\Program Files\Internet Explorer\Plugins\NPDocBox.dll
- > 012 – Plugin for .wav: C:\Program Files\Internet Explorer\PLUGINS\npqtplugin.dll
- > 016 – DPF: ADVFN 4v4 – <http://www.advfn.com/p.php?pid=loadercab>
- > 016 – DPF: ADVFN US – http://usa.advfn.com/advfn_us8.cab
- > 016 – DPF: {0246ECA8-996F-11D1-BE2F-00A0C9037DFE} (TDServer Control) – <http://www.truedoc.com/activex/tdserver.cab>
- > 016 – DPF: {10A1B95D-5E35-4935-8BC3-D43E81E8105E} – <http://www.ultimxxx.net/exefiles/021941.exe>
- > 016 – DPF: {166B1BCA-3F9C-11CF-8075-444553540000} (Shockwave ActiveX Control) – <http://download.macromedia.com/pub/shockwave/cabs/director/sw.cab>
- > 016 – DPF: {19E28AFC-EAE3-4CE5-AC83-2407B42F57C9} (MSSecurityAdvisor Class) – <http://download.microsoft.com/download/0/5/c/05c905f4-dd30-427d-a3de-373c3e5552fc/msSecAdv.cab?10837840>
- > 016 – DPF: {1D4DB7D2-6EC9-47A3-BD87-1E41684E07BB} (Fun Web Products Installer Start) – <http://imgfarm.com/images/nocache/funwebproducts/SmileyCentralInitialSetup1.0.0.5.exe>
- > 016 – DPF: {6A5BC405-BF00-11D4-8F33-00B0D0659D9F} (IGIndexDealing.CTRL) – <http://www.igindex.co.uk/client/Dealer/progs/IGDealing.CAB>
- > 016 – DPF: {9F1C11AA-197B-4942-BA54-47A8489BB47F} (Update Class) – <http://v4.windowsupdate.microsoft.com/CAB/x86/unicode/iucl.CAB?37578.2270023148>
- > 016 – DPF: {A8658086-E6AC-4957-BC8E-7D54A7E8A78E} (SassCln Object) – <http://www.microsoft.com/security/controls/SassCln.CAB>

microsoft.public.windowsxp.help_and_support: Re: Home Page

- > O16 – DPF: {AB29A544–D6B4–4E36–A1F8–D3E34FC7B00A} (WTHoster Class) – <http://www.wildtangent.com/install/wdriver/ddc/shockwave/blackhawkstriker/wtinst.cab>
- > O16 – DPF: {C7932801–AF0C–11D6–8137–0050DA5F0293} (RdxIE Class) – <http://www.grokster.com/rdx/RdxIE.cab>
- > O16 – DPF: {CAFEEFAC–0014–0000–0001–ABCDEFFEDCBA} (Java Runtime Environment 1.4.0_01) –
- > O16 – DPF: {D27CDB6E–AE6D–11CF–96B8–444553540000} (Shockwave Flash Object) – <https://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab>
- > O16 – DPF: {EF99BD32–C1FB–11D2–892F–0090271D4F88} (YBIOCtrl Class) – <http://us.dll.yimg.com/download.yahoo.com/dl/toolbar/my/yiebio4023.cab>
- > O17 –
HKLM\System\CCS\Services\Tcpip\.\{430B6A21–FEB8–41F9–864D–932EFB4EFC9C}:
NameServer = 194.72.9.55 194.74.65.85
- >
- >