

## Re: Possible virus freezing IE & slowing computer, help!

**Source:**

[http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help\\_and\\_support/2004-08/0496.html](http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help_and_support/2004-08/0496.html)

---

**From:** Jupiter Jones [MVP] ([jones\\_jupiter\\_at\\_hotnomail.com](mailto:jones_jupiter_at_hotnomail.com))

**Date:** 08/02/04

Date: Sun, 1 Aug 2004 21:32:01 -0600

Liz;

I meant to post the log to this forum where the experts are located:

<http://forum.aumha.org/viewforum.php?f=30&sid=980bbdbbcc32d4a506f49d43644d95f7>

--

Jupiter Jones [MVP]

<http://www3.telus.net/dandemar/>

"Liz" <liz@dolcezza.net> wrote in message

news:IkfPc.3019\$wz.1719@fedlread01...

> Yes, forgot to mention that and post the log, haha. Here it is, hope it

> helps:

>

> Logfile of HijackThis v1.98.1

> Scan saved at 2:08:25 PM, on 8/1/2004

> Platform: Windows XP SP1 (WinNT 5.01.2600)

> MSIE: Internet Explorer v6.00 SP1 (6.00.2800.1106)

>

> 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\svchost.exe

> C:\Program Files\TGTSoft\StyleXP\StyleXPService.exe

> C:\WINDOWS\system32\LEXBCES.EXE

> C:\WINDOWS\system32\spoolsv.exe

> C:\WINDOWS\system32\LEXPPS.EXE

> C:\PROGRA~1\AVG6\avgserve.exe

> C:\WINDOWS\System32\DRIVERS\CDANTSRV.EXE

> C:\WINDOWS\System32\cisvc.exe

> C:\Program Files\Compaq\Compaq Advisor\bin\compaq-rba.exe

> C:\WINDOWS\System32\nvsvc32.exe

> C:\WINDOWS\system32\pctspk.exe

> C:\WINDOWS\System32\tcpsvcs.exe

> C:\WINDOWS\System32\snmp.exe

> C:\WINDOWS\System32\svchost.exe

> C:\WINDOWS\system32\rundll32.exe

> C:\WINDOWS\Explorer.EXE

> C:\WINDOWS\System32\Smtray.exe

> C:\PROGRA~1\AVG6\avgcc32.exe

> C:\Program Files\Java\j2re1.4.2\_03\bin\jusched.exe

Re: Possible virus freezing IE & slowing computer, help!

microsoft.public.windowsxp.help\_and\_support: Re: Possible virus freezing IE & slowing computer, help!

```
> C:\Program Files\Common Files\Logitech\QCDriver3\LVCOMS.EXE
> C:\Program Files\Logitech\iTouch\iTouch.exe
> C:\PROGRA~1\Logitech\MOUSEW~1\SYSTEM\EM_EXEC.EXE
> C:\Program Files\Logitech\ImageStudio\LogiTray.exe
> C:\Program Files\Common Files\Real\Update_OB\realsched.exe
> C:\Program Files\TGTSoft\StyleXP\StyleXP.exe
> C:\PROGRA~1\AWS\WEATHE~1\Weather.exe
> C:\Program Files\Logitech\Desktop
> Messenger\8876480\Program\BackWeb-8876480.exe
> C:\Program Files\eBay\eBay Toolbar\4.3.0.9\ebaytbar.exe
> C:\Program Files\Common Files\Microsoft Shared\Works
Shared\wkcalrem.exe
> C:\WINDOWS\webshots.scr
> C:\WINDOWS\System32\cidaemon.exe
> C:\Program Files\Internet Explorer\iexplore.exe
> C:\WINDOWS\system32\winlogon.exe
> C:\Program Files\HijackThis.exe
>
> R1 - HKCU\Software\Microsoft\Internet Explorer\Main,SearchAssistant
= ,
> R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL
=
>
http://store.presario.net/scripts/redirectors/presario/storeredir2.dll?s=consumerfav&c=3c01&l=c=04
> R1 - HKLM\Software\Microsoft\Internet Explorer\Main,SearchAssistant
= ,
> R1 - HKCU\Software\Microsoft\Internet Explorer\Search,(Default) = ,
> R1 - HKLM\Software\Microsoft\Internet Explorer\Search,(Default) = ,
> R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Window Title =
Microsoft
> Internet Explorer provided by Compaq
> R1 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
> Settings,ProxyOverride =
dynhost.inetcam.com;register.inetcam.com;;localhost
> O3 - Toolbar: &Radio - {8E718888-423F-11D2-876E-00A0C9082467} -
> C:\WINDOWS\System32\msdxm.ocx
> O3 - Toolbar: eBay Toolbar -
{46AE04C0-BCFA-4728-90E7-00EB4A8B3863} -
> C:\Program Files\eBay\eBay Toolbar\4.3.0.9\EBayBand.dll
> O4 - HKLM\..\Run: [NvCplDaemon] RUNDLL32.EXE
> C:\WINDOWS\System32\NvCpl.dll,NvStartup
> O4 - HKLM\..\Run: [WCOLOREAL] "C:\Program
> Files\COMPAQ\Coloreal\coloreal.exe"
> O4 - HKLM\..\Run: [Smapp] Smtray.exe
> O4 - HKLM\..\Run: [Microsoft Works Portfolio] C:\Program
Files\Microsoft
> Works\WksSb.exe /AllUsers
> O4 - HKLM\..\Run: [srmclean] C:\Cpqs\Scom\srmclean.exe
> O4 - HKLM\..\Run: [AVG_CC] C:\PROGRA~1\AVG6\avgcc32.exe /STARTUP
> O4 - HKLM\..\Run: [QuickTime Task] "C:\Program
> Files\QuickTime\qttask.exe" -atboottime
> O4 - HKLM\..\Run: [SunJavaUpdateSched] C:\Program
> Files\Java\j2re1.4.2_03\bin\jusched.exe
> O4 - HKLM\..\Run: [LVCOMS] C:\Program Files\Common
> Files\Logitech\QCDriver3\LVCOMS.EXE
> O4 - HKLM\..\Run: [nwiz] nwiz.exe /install
> O4 - HKLM\..\Run: [zBrowser Launcher] C:\Program
> Files\Logitech\iTouch\iTouch.exe
> O4 - HKLM\..\Run: [EM_EXEC]
C:\PROGRA~1\Logitech\MOUSEW~1\SYSTEM\EM_EXEC.EXE
> O4 - HKLM\..\Run: [LogitechGalleryRepair] C:\Program
> Files\Logitech\ImageStudio\ISStart.exe
```

microsoft.public.windowsxp.help\_and\_support: Re: Possible virus freezing IE & slowing computer, help!

```
> 04 - HKLM\..\Run: [LogitechImageStudioTray] C:\Program
> Files\Logitech\ImageStudio\LogiTray.exe
> 04 - HKLM\..\Run: [TkBellExe] "C:\Program Files\Common
> Files\Real\Update_OB\realsched.exe" -osboot
> 04 - HKLM\..\Run: [geszfc] C:\WINDOWS\System32\geszfc.exe
> 04 - HKCU\..\Run: [STYLEXP] C:\Program
> Files\TGTSoft\StyleXP\StyleXP.exe -Hide
> 04 - HKCU\..\Run: [Weather] C:\PROGRA~1\AWS\WEATHE~1\Weather.exe 1
> 04 - HKCU\..\Run: [LDM] C:\Program Files\Logitech\Desktop
> Messenger\8876480\Program\BackWeb-8876480.exe
> 04 - Startup: Webshots.lnk = C:\Program Files\Webshots\Launcher.exe
> 04 - Global Startup: eBay Toolbar.LNK = C:\Program Files\EBay\EBay
> Toolbar\4.3.0.9\ebaytbar.exe
> 04 - Global Startup: Logitech Desktop Messenger.lnk = C:\Program
> Files\Logitech\Desktop Messenger\8876480\Program\LDMConf.exe
> 04 - Global Startup: Microsoft Works Calendar Reminders.lnk = ?
> 08 - Extra context menu item: &NeoTrace It! -
> C:\PROGRA~1\NEOTRA~1\NTXcontext.htm
> 09 - Extra button: (no name) -
{08B0E5C0-4FCB-11CF-AAA5-00401C608501} - (no
> file)
> 09 - Extra 'Tools' menuitem: Sun Java Console -
> {08B0E5C0-4FCB-11CF-AAA5-00401C608501} - (no file)
> 09 - Extra button: eBay Toolbar -
{92D7F210-7F20-11d3-8157-0090278B20DE} -
> C:\Program Files\EBay\EBay Toolbar\4.3.0.9\EBayBand.dll
> 09 - Extra 'Tools' menuitem: eBay Toolbar -
> {92D7F210-7F20-11d3-8157-0090278B20DE} - C:\Program Files\EBay\EBay
> Toolbar\4.3.0.9\EBayBand.dll
> 09 - Extra button: AIM - {AC9E2541-2814-11d5-BC6D-00B0D0A1DE45} -
C:\Program
> Files\AOL Instant Messenger\aim.exe
> 09 - Extra button: (no name) -
{CD67F990-D8E9-11d2-98FE-00C0F0318AFE} - (no
> file)
> 09 - Extra button: Yahoo! Messenger -
> {E5D12C4E-7B4F-11D3-B5C9-0050045C3C96} -
> C:\PROGRA~1\Yahoo!\MESSE~1\YPager.exe
> 09 - Extra 'Tools' menuitem: Yahoo! Messenger -
> {E5D12C4E-7B4F-11D3-B5C9-0050045C3C96} -
> C:\PROGRA~1\Yahoo!\MESSE~1\YPager.exe
> 09 - Extra button: Messenger -
{FB5F1910-F110-11d2-BB9E-00C04F795683} -
> C:\Program Files\Messenger\MSMSGSGS.EXE
> 09 - Extra 'Tools' menuitem: Windows Messenger -
> {FB5F1910-F110-11d2-BB9E-00C04F795683} - C:\Program
> Files\Messenger\MSMSGSGS.EXE
> 09 - Extra button: Support -
{150356B4-A312-4148-AFD0-E5CF7A1F3E2E} -
> C:\Program Files\Internet Explorer\SIGNUP\Presario.htm (HKCU)
> 09 - Extra button: NeoTrace It! -
{9885224C-1217-4c5f-83C2-00002E6CEF2B} -
> C:\PROGRA~1\NEOTRA~1\NTXtoolbar.htm (file missing) (HKCU)
> 09 - Extra button: WeatherBug -
{AF6CABAB-61F9-4f12-A198-B7D41EF1CB52} -
> C:\Program Files\AWS\WeatherBug\Weather.exe (HKCU)
> 010 - Unknown file in Winsock LSP: c:\windows\system32\lspak.dll
> 010 - Unknown file in Winsock LSP: c:\windows\system32\lspak.dll
> 010 - Unknown file in Winsock LSP: c:\windows\system32\lspak.dll
> 010 - Unknown file in Winsock LSP: c:\windows\system32\lspak.dll
> 010 - Unknown file in Winsock LSP: c:\windows\system32\lspak.dll
> 010 - Unknown file in Winsock LSP: c:\windows\system32\lspak.dll
```

microsoft.public.windowsxp.help\_and\_support: Re: Possible virus freezing IE & slowing computer, help!

```
> O10 - Unknown file in Winsock LSP: c:\windows\system32\lspak.dll
> O14 - IERESSET.INF:
>
START_PAGE_URL=http://store.presario.net/scripts/redirectors/presario/storer
> edir2.dll?s=consumerfav&c=3c01&lc=0409
> O16 - DPF: SwiftWebInstall Class -
> http://media.affinitymedia.com/offer/install/SwiftWebInstall.cab
> O16 - DPF: {16FD824B-8E7B-11D2-9855-00802962956C} (Specfile Control) -
> http://las.mlxchange.com/Control/Specfile.cab
> O16 - DPF: {284DAE3C-A691-11D3-AD58-00E0B8107A24} (SISCtrl Class) -
> http://las.mlxchange.com/Control/SISC.cab
> O16 - DPF: {2B96D5CC-C5B5-49A5-A69D-CC0A30F9028C} (MiniBugTransporterX Class) -
>
http://download.weatherbug.com/minibug/tricklers/AWS/MiniBugTransporter.cab?
> O16 - DPF: {2BC66F54-93A8-11D3-BEB6-00105AA9B6AE} (Symantec AntiVirus scanner) -
> http://security.symantec.com/sscv6/SharedContent/vc/bin/AvSniff.cab
> O16 - DPF: {4989312D-58CF-11D5-A7D7-00E02911103E} (Interealty MultiSelect) -
> http://las.mlxchange.com/Control/MultiSelectComboBox.cab
> O16 - DPF: {56336BCB-3D8A-11D6-A00B-0050DA18DE71} (RdxIE Class) -
> http://207.188.7.150/03c4392c2e4501428516/netzip/RdxIE601.cab
> O16 - DPF: {5D9E4B6D-CD17-4D85-99D4-6A52B394EC3B} (WSDownloader Control) -
> http://www.webshots.com/samplers/WSDownloader.ocx
> O16 - DPF: {62475759-9E84-458E-A1AB-5D2C442ADFDE} -
>
http://a1540.g.akamai.net/7/1540/52/20031216/qtinstall.info.apple.com/mickey/us/win/QuickTimeInst
> O16 - DPF: {644E432F-49D3-41A1-8DD5-E099162EEEC5} (Symantec RuFSI Utility Class) -
>
http://security.symantec.com/sscv6/SharedContent/common/bin/cabsa.cab
> O16 - DPF: {6FD482A3-7B57-438B-B040-52CAA30147EE} (MLXchange Client Utils) -
> http://las.mlxchange.com/Control/MLXClientUtils.cab
> O16 - DPF: {74D05D43-3236-11D4-BDCD-00C04F9A3B61} (HouseCall Control) -
>
http://a840.g.akamai.net/7/840/537/2004061001/housecall.trendmicro.com/housecall/xscan53.cab
> O16 - DPF: {78523E50-56EB-11D3-B739-CAA1986A452F} (LiteGridCtl Class) -
> http://las.mlxchange.com/Control/LiteGrid.cab
> O16 - DPF: {83AB6E4D-CDD7-11D3-B5E7-00104B9AFF6E} (GeacRevw Control) -
> http://las.mlxchange.com/Control/IRCSharc.cab
> O16 - DPF: {98264495-6376-443C-9340-2996038BD143} (VaCtrl Class) -
> http://198.247.172.30/plugin/h263ctrl.cab
> O16 - DPF: {EB387D2F-E27B-4D36-979E-847D1036C65D} (QDiagHUpdateObj Class) -
> http://h30043.www3.hp.com/hpdj/en/check/qdiagh.cab?316
> O16 - DPF: {EF791A6B-FC12-4C68-99EF-FB9E207A39E6} (McFreeScan Class) -
>
http://download.mcafee.com/molbin/iss-loc/vso/en-us/tools/mcfscan/2,0,0,4382/mcfscan.cab
> O16 - DPF: {F060A272-A18A-11D3-B75B-00E0B81077E8} (DropList Class) -
> http://las.mlxchange.com/Control/AspCustomCtrls.cab
```

microsoft.public.windowsxp.help\_and\_support: Re: Possible virus freezing IE & slowing computer, help!

> O16 - DPF: {F58E1CEF-A068-4C15-BA5E-587CAF3EE8C6} (MSN Chat Control 4.5) -  
> <http://chat.msn.com/bin/msnchat45.cab>  
>  
> "Jupiter Jones [MVP]" <jones\_jupiter@hotmail.com> wrote in message  
> news:OIt2RwBeEHA.4048@TK2MSFTNGP12.phx.gbl...  
> > Liz;  
> > Did you also run HijackThis?  
> > Post the log in the forum referenced on the link.  
> >  
> > --  
> > Jupiter Jones [MVP]  
> > <http://www3.telus.net/dandemar/>  
> >  
> >  
> > "Liz" <liz@dolcezza.net> wrote in message  
> > news:agePc.3012\$wz.2947@fedlread01...  
> > > I already have a firewall active due to my router. :(  
> > >  
> > > What I think this is is either spyware or a virus from a program  
> > > that I  
> > > accidently downloaded when I was viewing a fan site. It  
installed  
> > about 4  
> > > programs and even though I uninstalled them all,I'm still  
getting a  
> > > TON of  
> > > pop-ups. I did everything you said to do in your previous reply  
and  
> > > ran both  
> > > AdAware and SpyBot after updating both, but no luck.  
> > >  
> > > "Jupiter Jones [MVP]" <jones\_jupiter@hotmail.com> wrote in  
message  
> > > news:%231bYTKBeEHA.3420@TK2MSFTNGP12.phx.gbl...  
> > > > For Messenger Service ads:  
> > > > You need to install or enable a firewall:  
> > > > <http://support.microsoft.com/?kbid=330904>  
> > > >  
> > > >  
> > > >  
> > > >  
> > > > <http://www.microsoft.com/windowsxp/pro/using/howto/communicate/stopspam.asp>  
> > > > Disabling Messenger Service can be a good idea, but it does  
not  
> > > > solve  
> > > > the real problem.  
> > > > The ads are not the real problem, the ads are only a symptom.  
> > > > The real problem is open ports that allow unwanted traffic  
into  
> > > the  
> > > > computer.  
> > > > Disabling Messenger does nothing for the open ports.  
> > > > The firewall controls the traffic.  
> > > >  
> > > > Internet Connection Firewall will not work if you have AOL.  
> > > > AOL is not compatible with Windows XP Internet Connection  
Firewall  
> > > > (ICF)  
> > > > If you have AOL, you should contact AOL and/or get a 3rd party  
> > > > firewall:  
> > > > <http://www.zonelabs.com/store/content/home.jsp>

