

microsoft.public.security.virus: Re: possible spyware problem, please help!

Re: possible spyware problem, please help!

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-08/0962.html>

From: Chuck (*none_at_example.net*)

Date: 08/18/04

Date: 18 Aug 2004 16:47:18 -0500

On 18 Aug 2004 11:40:04 -0700, *email_address_deleted* (Ben) wrote:

>I recently purchased a used IBM a21m laptop. It was working great up
>until last night when Windows began running incredibly slow. I'd try
>to open a program and it would take an incredibly long time for the
>window to open. Also, some of the programs would automatically close
>shortly after opening them and programs would freeze up and stop
>responding. I was downloading prior to this occurrence, so does this
>sound like a spyware problem? What should I use to remedy it? I've
>tried running Adaware without much help.

>

>I also received a pop-up message box with "Messenger Service" in title
>bar. I've heard this is related to spyware.

>

>Thanks for you help.

Ben,

This particular pop-up is NOT a spyware problem. But it does demonstrate that your computer is unprotected. With proper protection, you should not be seeing the "Messenger Service" pop-ups.

Messenger Service of Windows

<<http://support.microsoft.com/default.aspx?scid=KB:en-us:168893>>

Messenger Service Window That Contains an Internet Advertisement
Appears

<<http://support.microsoft.com/?id=330904>>

Stopping Advertisements with Messenger Service Titles

<<http://www.microsoft.com/windowsxp/pro/using/howto/communicate/stospam.asp>>

If you're using AOL, you'll either need to find a 3rd party firewall that is compatible with AOL, or switch to a real ISP that is compatible with the real Internet. This is because AOL is an on-line content provider that ignores international networking standards in favor of its own proprietary products, and has deliberately made its connection software incompatible with both WinXP's built-in firewall and WinXP's Internet Connection Sharing feature. AOL's

Re: possible spyware problem, please help!

microsoft.public.security.virus: Re: possible spyware problem, please help!

proprietary connection applet is deliberately designed to preclude your setting/adjusting any of its properties, to include enabling/disabling WinXP's ICF and ICS.

Whichever firewall you decide upon, be sure to ensure UDP ports 135, 137, and 138 and TCP ports 135, 139, and 445 are all blocked. You may also disable Inbound NetBIOS (NetBIOS over TCP/IP). You'll have to follow the instructions from firewall's manufacturer for the specific steps.

You can test your firewall at:

Gibson Research <<http://grc.com/default.htm>> (ShieldsUp!)
SecurityMetrics <<http://www.securitymetrics.com/portscan.adp>>
Sygate Security Scan <<http://www.sygatetech.com/>>
Symantec Security Check <http://security.symantec.com/ssc/vr_main.asp>

Be especially wary of people who advise you to do nothing more than disable the messenger service. Disabling the messenger service, by itself, is a "head in the sand" approach to computer security. The real problem is not the messenger service pop-ups; they're actually providing a useful, if annoying, service by acting as a security alert.

WRT the slowing down of your computer, and closing / freezing by various programs, this sounds very much like a spyware / virus problem.

How current is your virus protection? Try one or more of these free online virus scans, which should complement your current protection:

<<http://www.bitdefender.com/scan/license.php>>
<<http://www.pandasoftware.com/activescan>>
<<http://www.ravantivirus.com/scan/>>
<<http://security.symantec.com/ssc/home.asp>>
<http://housecall.trendmicro.com/housecall/start_corp.asp>

Now check for, and learn to defend against, additional problems.

Start by downloading each of the following additional free tools:
CWShredder <<http://www.majorgeeks.com/download4086.html>>
CoolWWWSearch.SmartSearch (v1/v2) MiniRemoval
<<http://www.majorgeeks.com/download4113.html>>
HijackThis <<http://www.majorgeeks.com/download.php?det=3155>>
LSP-Fix and WinsockLSPFix <<http://www.cexx.org/lspfix.htm>>
Spybot S&D <<http://www.safer-networking.org/index.php?page=download>>
Stinger <<http://us.mcafee.com/virusInfo/default.asp?id=stinger>>

Create a separate folder for HijackThis, such as C:\HijackThis – copy the downloaded file there. AdAware and Spybot S&D have install routines – run them. The other downloaded programs can be copied into, and run from, any convenient folder.

First, run Stinger. Have it remove any problems found.

Re: possible spyware problem, please help!

microsoft.public.security.virus: Re: possible spyware problem, please help!

Next, close all Internet Explorer and Outlook windows, and run CoolWWWSearch.SmartSearchMiniRemoval, then CWShredder. Have the latter fix all problems found.

Next, run AdAware. First update it ("Check for updates now"), configure for full scan (<<http://www.lavahelp.com/howto/fullscan/>>), then scan ("Start" – "Use custom scanning options" – "Next"). When scanning finishes, select everything, and hit Next again.

Next, run Spybot S&D. First update it ("Search for updates"), then run a scan ("Check for problems"). Trust Spybot, and delete everything ("Fix Problems") that is displayed in Red.

Then, run HijackThis ("Scan"). Do NOT make any changes immediately. Save the HJT Log.

<<http://forums.spywareinfo.com/index.php?showtopic=227>>

Finally, have your HJT log interpreted by experts at one or more of the following security forums (and post a link to your forum posts, here):

Aumha: <<http://forum.aumha.org/index.php>>

Net-Integration: <<http://forums.net-integration.net/>>

Spyware Info: <<http://forums.spywareinfo.com/>>

Spyware Warrior: <<http://spywarewarrior.com/index.php>>

Tom Coyote: <<http://forums.tomcoyote.org/>>

If removal of any spyware affects your ability to access the internet (some spyware builds itself into the network software, and its removal may damage your network), run LSP-Fix and / or WinsockXPFix.

And Ben, please don't contribute to the spread and success of email address mining viruses. Learn to munge your email address properly, to keep yourself a bit safer when posting to open forums. Protect yourself and the rest of the internet – read this article.

http://www.mailmsg.com/SPAM_munging.htm

Cheers,

Chuck

Paranoia comes from experience – and is not necessarily a bad thing.