

Re: 180searchAssistant

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.perform_maintain/2004-07/0756.html

From: Chuck (*none_at_example.net*)

Date: 07/05/04

Date: 5 Jul 2004 13:14:16 -0500

On Mon, 5 Jul 2004 10:40:25 -0700, "Paul" <anonymous@discussions.microsoft.com> wrote:

*>I have aol and lately when i've been getting on i've been
>getting these "pop-ups" from microsoft, i deleted
>180searchassistant and the pop-ups stopped, but then the
>search assistant came back the very next day, every time
>i delete it, it always comes back. now everytime i get on
>the internet, i get about 7 to 9 pop-ups from microsoft,
>it's really annoying, it freezes up my computer so bad
>sometimes i have to turn it completely off. I can't even
>get on the internet much anymore, and these are not aol
>popups, their microsoft, everytime i try to just close
>them i recieve a error report, i've probably sent 20
>something error reports in the last week.*

Paul,

180SearchAssistant sounds like a CWS spyware infection (III below). But you probably ought to consider all 3 known types of popups.

I. "Messenger Service" Pop-Ups

This will be a text only message, and will only hit you when you're online. A Messenger Service pop-up can't contain a clickable link. The window will be titled "Messenger Service".

This type of spam has become quite common over the past year or so, and unintentionally serves as a valid security alert. It demonstrates that you haven't been taking sufficient precautions while connected to the Internet. Your data probably hasn't been compromised by these specific advertisements, but if you're open to this exploit, you most definitely open to other threats, such as the Blaster Worm that still haunts the Internet. Install and use a decent, properly configured firewall.

Messenger Service of Windows

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

Re: 180searchAssistant

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/stopspam.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 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.

II. Regular Browser Based Pop-Ups

This will be an HTML message, and will only hit you when you're online. A browser based popup will probably contain clickable links. The window title will vary.

Get the free Google Toolbar from <<http://toolbar.google.com/>>. Hosts file blocking works on this problem also.

Blocking Ads, Parasites, and Hijackers with a Hosts File

<<http://www.mvps.org/winhelp2002/hosts.htm>>

III. Adware / Spyware

This will be an HTML message, and can hit you when you're online, or offline. An adware based popup will probably contain clickable links. The window title

will vary.

This is where you need a thorough adware / spyware scan, including CWS shredder, AdAware, Spybot S&D, and HijackThis, with expert advice to interpret the HijackThis log.

Start by downloading each of the following free tools:

AdAware <<http://www.lavasoftusa.com/>>

CWS shredder <<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>>

Install and run 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. Spybot S&D has an install routine – run it. The other downloaded programs can be copied into, and run from, any convenient folder.

Start by closing all Internet Explorer and Outlook windows, and running CoolWebSearchSmartKillerMiniRemoval, then CWS shredder. Have the latter fix all.

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 it, or 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/>>

Wilders Security <<http://www.wilderssecurity.com/>>

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.

microsoft.public.windowsxp.perform_maintain: Re: 180searchAssistant

Cheers,

Chuck

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