

Re: Adware and spyware

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2004-09/1584.html>

From: Chuck (*none_at_example.net*)

Date: 09/26/04

Date: 26 Sep 2004 09:59:03 -0500

On Sun, 26 Sep 2004 03:20:28 -0700, "Lai" <anonymous@discussions.microsoft.com> wrote:

>Every time I am on the computer I keep getting pop up ads
>and websites on the screen that I have not asked for. I
>have used various types of software to get rid of them
>such as "Ad ware" and "SPYbot" but they keep coming back.
>I also use norton antivirus as well. What can I do to
>stop all these pop up ads and websites coming up on to my
>computer?
>Thanks

Lai,

Pop-ups have at least three variations, and the solutions vary accordingly. Which specific type(s) are you seeing?

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>>

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 HijackThis, with expert advice to interpret the HijackThis log. You did update AA and SSD

before scanning, right?

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>>
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. The other downloaded programs can be copied into, and run from, any convenient folder.

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

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

Next, run AdAware again. 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 again. 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.

IV. Future Protection

Finally, improve your chances for the future.

Harden your browser. There are various websites which will check for vulnerabilities, here are three which I use.

microsoft.public.security: Re: Adware and spyware

<http://www.jasons-toolbox.com/BrowserSecurity/>
<http://bcheck.scanit.be/bcheck/>
https://testzone.secunia.com/browser_checker/

Block Internet Explorer ActiveX scripting from hostile websites (Restricted Zone).

<<https://netfiles.uiuc.edu/ehowes/www/main.htm>> (IE-SpyAd)

Block known dangerous scripts from installing.

<<http://www.javacoolsoftware.com/spywareblaster.html>>

Block known spyware from installing.

<<http://www.javacoolsoftware.com/spywareguard.html>>

Make sure that the spyware detection / protection products that you use are reliable:

http://www.spywarewarrior.com/rogue_anti-spyware.htm

Harden your operating system. Check at least monthly for security updates.

<http://windowsupdate.microsoft.com/>

Block known obnoxious websites with a Hosts file. Three Hosts file sources I use:

http://www.accs-net.com/hosts/get_hosts.html

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

(The third is included, and updated, with Spybot (see above)).

Maintain your Hosts file (merge / eliminate duplicate entries) with:

eDexter <http://www.accs-net.com/hosts/get_hosts.html>

Hostess <<http://accs-net.com/hostess/>>

Secure your operating system, and applications. Don't use, or leave activated, any accounts with names or passwords with trivial (guessable) values. Don't use an account with administrative authority, except when you're intentionally doing administrative tasks.

Use common sense. Yours. Don't install software based upon advice from unknown sources. Don't install free software, without researching it carefully. Don't open email unless you know who it's from, and how and why it was sent.

Educate yourself. Know what the risks are. Stay informed. Read Usenet, and various web pages that discuss security problems. Check the logs from the other layers regularly, look for things that don't belong, and take action when necessary.

Cheers,

Chuck

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

Re: Adware and spyware