

Re: Pop ups

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6.browser/2004-03/2341.htm>

From: Jim Byrd (jrbyrd_at_spamlessadelphia.net)

Date: 03/06/04

Date: Fri, 5 Mar 2004 16:42:41 -0800

Hi Jo – It sounds like you've been hijacked. If you go to this page at Jim Eshelman's site, here: <http://aumha.org/a/noads.htm> and wait a little bit (be patient), an analysis of a number of possible parasites on your machine will be made to help you identify and remove them. NOTE: You will need to disable Ad Blocking in Zone Alarm 3.x, if present or any other Ad Blocking software which interferes with Java Scripting for this scan to work. You should get a message between the two lines of **** giving the results of the scan.

For the general hijack case, the best way to start is to get Ad-Aware 6.0, Build 181 or later, here: <http://www.javasoftusa.com/support/download/>. UPDATE (even on your first install/run) and run this regularly to get rid of most "spyware/hijackware" on your machine. If it has to fix things, be sure to re-boot and rerun AdAware again and repeat this cycle until you get a clean scan. The reason is that it may have to remove things which are currently "in use" before it can then clean up others.

Another excellent program for this purpose is SpyBot Search and Destroy available here: <http://security.kolla.de/> SpyBot Support Forum here: <http://www.net-integration.net/cgi-bin/forums/ikonboard.cgi>. I recommend using both normally. After UPDATING (even on your first install/run) and fixing things with SpyBot S&D, be sure to re-boot and rerun SpyBot again and repeat this cycle until you get a clean "no red" scan. The reason is that SpyBot sometimes has to remove things which are currently "in use" before it can then clean up others.

Note that sometimes you need to make a judgement call about what these programs report as spyware. See here, for example: <http://www.imilly.com/alex.htm>

Lastly, a very useful utility for examining your system and correcting problems is Hijack This, which you can download here: <http://www.spywareinfo.com/~merijn/files/hijackthis.zip> See also, HijackThis Quick Start Help, <http://www.tomcoyote.org/hjt/> (Recommended) This site has a number of useful references and information also: <http://www.spywareinfo.com/articles/hijacked/> and here <http://www.spywareinfo.com/downloads.php>

Another program giving a good inventory of all of the possible start vectors is AutostartExplorer, here: <http://www.misec.net/aexp.jsp> While it doesn't allow control of startups, it's extremely comprehensive in examining all of the possible sources. Highly Recommended

Next, go here: <http://www.mlin.net/StartupCPL.shtml> and get Mike Lin's Startup Control Panel applet. A somewhat more difficult to use but more extensive program to do the same thing is StartupList from here: <http://www.lurkhere.com/~nicefiles/index.html>, or even better, Autoruns from here: <http://www.sysinternals.com/ntw2k/source/misc.shtml#autoruns>. Be very careful about doing any Registry modifications directly unless you're comfortable with this, and be sure that you BACKUP your Registry before making any changes, so that you can recover if something goes wrong. Changes made with StartUpCPL are less likely to cause problems, and are usually a matter of just re-enabling the particular program. Another program of this type that I can recommend is StartMan, free, here: <http://www.spywareinfo.com/downloads/startman/>. If you have problems with suspected hijackers, you can look up and investigate suspect programs in your StartUp lists here: http://www.pacs-portal.co.uk/startup_pages/startup_full.htm (Recommended) <http://www.3feetunder.com/krick/startup/list.html> (Recommended) http://www.answerthatwork.com/Tasklist_pages/tasklist.htm (Recommended)

Some hijackers install themselves as Browser Helper Objects. Get BHOCop here: BHO Cop <http://www.pcmag.com/article2/0,4149,270,00.asp> (Unfortunately, no longer free from that link but you can read about it there, and here is a direct download link for it: <http://websec.arcady.fr/bhocop.zip>) and take a look at what BHO's are currently installed. Some things like AdShield and Acrobat are normal, but if you see something that doesn't make any sense, try disabling it and see if that helps. Another excellent program for this same purpose is BHODemon, (still free) here: <http://www.definitivesolutions.com/> or here: <http://www.spywareinfo.com/downloads/bhod/> I would recommend both. You can also check/control BHO's using the Tools function of SpyBot S&D.

There's good information about hijacking and fixes available here:

Andrew Clover's parasite page: <http://www.doxdesk.com/parasite/> (Highly recommended)
Robert Allen's parasite page: <http://allentech.net/parasite/index.phtml> (Highly recommended)
<http://www.spywareinfo.com/hijacked.html>
<http://gmpservicesinc.com/Articles/hijack.asp> (links here for .reg files to lock and unlock your homepage, BTW. You can also use this program to toggle locking/unlocking of your homepage:
<http://www.dougknox.com/security/scripts/nosethomepage.vbs> Recommended)
http://www.mvps.org/inetexplorer/answers.htm#home_page

Also, there's a new class of hijacker using Window's Messenger Service (not Instant Messaging, BTW). If you get popups even when your browser is not connected to the Internet with a title bar reading "Messenger Service", then

these are most likely due to open NetBios TCP ports 135, 139 and 445 and UDP ports 135, 137–138. You really need to block these with a firewall as a general protection measure. You can stop the popups by turning off Messenger Service; however, this still leaves you vulnerable. If you have an NT-based OS such as XP or Win2k, you should probably also specifically block TCP 593, 4444 and UDP 69, 139, 445, and install the very important 823980 patch from MS03–026, here: <http://support.microsoft.com/?kbid=823980>.

See: Messenger Service Window That Contains an Internet Advertisement Appears <http://support.microsoft.com/?id=330904> which identifies reasons to keep this service and steps to take if you do.

You can test your system and follow the 'Prevention' link to get additional information here:

<http://www.mynetwatchman.com/winpopuptester.asp> Unless you have very good reasons to keep this active, it should be turned off in Win2k and XP. Go here and do what it says:

<http://www.itc.virginia.edu/desktop/docs/messagepopup/> or, even better, get MessageSubtract, free, here, which will give you flexible control of the service and viewing of these messages:

<http://www.intermute.com/messagesubtract/help.html> Recommended.

(FWIW, ZoneAlarm's default Internet Zone firewall configuration blocks the necessary ports to prevent this use of Messenger Service. I don't know the situation with regard to other firewalls.)

Messenger Service is not per se Spyware or something that MS did wrong – It provides a messaging capability which is useful for local intranets and is also sometimes (albeit nowadays infrequently) used by some applications to provide popup messages to users. However, it can also be (and now frequently is) used to introduce spam via this open NetBios channel. For a single user home computer, it normally isn't needed and can be turned off which will eliminate the spam popups. This DOESN'T, however, remove the vulnerability of having these ports open, when in fact they aren't needed, since they can be perverted in other ways as well, some of which can be much more damaging than just a spam popup.

Unless you have very good reasons to keep this active, it should be turned off in Win2k and XP. Go here and do what it says:

<http://www.itc.virginia.edu/desktop/docs/messagepopup/> or, even better, get MessageSubtract, free, here, which will give you flexible control of the service and viewing of these messages:

<http://www.intermute.com/messagesubtract/help.html> Recommended.

Once you get this cleaned up, you might want to consider installing the SpywareBlaster and SpywareGuard here to help prevent this kind of thing from happening in the future:

<http://www.javacoolsoftware.com/spywareblaster.html> (Prevents malware Active X installs) (BTW, SpyWare Blaster is not memory resident ... no CPU or memory load – but keep it UPDATED) The latest version as of this writing

will prevent installation or prevent the malware from running if it is already installed, and it provides information and fixit-links for a variety of parasites.

<http://www.wilderssecurity.net/spywareguard.html> (Monitors for attempts to install malware) Keep it UPDATED. Both Very Highly Recommended.

See if any of this helps and post back with your results.

--

Please respond in the same thread.

Regards, Jim Byrd, MS-MVP

In news:7ce401c4030d\$67ce7ba0\$a001280a@phx.gbl,
Rockin_Jo <i_fink_i_lost_my_rwoarar@hotmail.com> typed:

> Help me please!
> One day i accidently clicked on a pop up.
> Now everytime i open internet explorer, along with my
> home page, 2 other windows appear, one with a quite dodgy
> website on it! Ive tried everything and i can't get rid
> of them plus i have 2 files in my documents -
> WH4_1843003.dll (1.3.0.0 "webhelper module") and
> WH4_1843003 "configuration settings") these seem to have
> something to do with it, but i can't delete the so-
> called "webhelper module". Can someone help me please??