

Re: bannerfarm and other pop ups

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6.browser/2004-07/5354.htm>

From: LuckyStrike (*LS_at_smokedamagedfurniture.youcandriveitawaytoday.com*)

Date: 07/20/04

Date: Mon, 19 Jul 2004 23:08:05 -0600

Adrienne -

Maybe you ought to check out your "Anti-Spyware" app SpyAssassin. It has a very poor rating.

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

I'd disable Windows Messenger Service (in XP, W2K, NT)

<http://www.itc.virginia.edu/desktop/docs/messagepopup/>

Or WinPopup in W98 and ME

1. Click Start > Search (or Find) > Find Files or Folders.
2. Search for the winpopup.exe file.
3. Right-click on the winpopup.exe file and rename it to "winpopup.bad" (or whatever fun file extension you can think of).
4. Click Yes if prompted.
5. Restart the computer.

OR

1. Go to your Control Panel -> Add/Remove Programs -> Windows Setup -> Accessories
2. Scroll down to the bottom of the list.
3. Uncheck the Winpopup.

<http://www.more.net/security/advisories/2002/021025.html>

http://www.wown.com/j_helmig/winpopup.htm

Then, I'd get better (and free) Anti-Spyware apps. Make sure you get the Real Deal, and not some "knock-off" or "sounds-like" :-) To name but a few:

Ad-Aware

Spybot Search and Destroy

CWShredder

SpywareBlaster

SpywareGuard

Hijack This

microsoft.public.windows.inetexplorer.ie6.browser: Re: bannerfarm and other pop ups

Quick and basic scans from any of the following sites:

Doxdesk parasite scan

<http://doxdesk.com/parasite/>

Jim Eshelmans WSC on-line quick scan

<http://www.aumha.org/a/noads.htm>

Bugs Glitches and Stuff-ups

<http://inetexplorer.mvps.org/Darnit.htm>

More In-Depth on-line scanners for parasites and Trojans:

GFI free on-line Trojan scanner

<http://www.windowsecurity.com/trojanscan/>

Sygate Technologies Trojanscan

<http://scan.sygatetech.com/pretrojanscan.html>

PestPatrol on-line scan

<http://www.pestscan.com/home.asp>

SpywareChecker on-line scan

http://www.spywareguide.com/txt_onlinescan.html

Parasites, spyware malware basics:

<http://aumha.org/a/parasite.htm>

<http://aumha.org/a/quickfix.htm>

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

Check for Spyware – How – to's

First, install the respective programs and then update them immediately, so that they have the current versions, and definitions. Read the Help Files and Tutorials.

After you've Updated Spybot S & D, and SpywareBlaster, you **must** ENABLE the protections as well. These two programs do not automatically enable the newest definitions and updates, so this process but must be done by you manually.

Run them one at a time. With Ad-Aware you may have it generally clean whatever it finds. The same applies for CWShredder. Spybot S&D requires special attention (listed below), as does HijackThis (Only more so. Details listed below) The programs are listed in order of their general strength, safety, and purpose. It is perhaps best to install and run these in this order of appearance. All are freeware programs, but if you are pleased with the results and quality of the utilities, donations to the respective Authors are cheerfully accepted.

Most important – Before you try to remove spyware using any of the following programs, realize that the process of cleaning and removing certain spyware and malware may possibly interrupt and kill your internet connection. Therefore, you should obtain a copy of LSPFIX, and Winsockfix which will then make it possible for you to re-establish your internet connection if it gets terminated.

Download LSPFIX from either of the following sites:

Re: bannerfarm and other pop ups

microsoft.public.windows.inetexplorer.ie6.browser: Re: bannerfarm and other pop ups

<http://www.cexx.org/lspfix.htm>

<http://www.spychecker.com/program/winsockxpfix.html> (For Win2k or XP)

Download Winsockfix here

<http://members.shaw.ca/installations/WinsockFix.zip>

Another thing to consider doing is to run a program (only run one program at a time) a few times consecutively. The reason for this is that the first pass may kill certain Spyware programs, but may not be able to terminate and kill all files and programs which may be running at the time.

That is why a second pass may be necessary to be thoroughly effective.

Also, under the most stubborn cases, running the programs in Safe-Mode will allow for the best cleaning conditions, as there will be a minimum of interference from processes running in the background.

Ad -Aware

<http://www.lavasoftusa.com/support/download/>

Ad-Aware Tutorial (might help if you look through this)

<http://www.bleepingcomputer.com/forums/index.php?showtutorial=48>

CWShredder (cleans all Cool Web Search malware)

<http://www.majorgeeks.com/download4086.html>

CWShredder Tutorial

<http://www.bleepingcomputer.com/forums/index.php?showtutorial=47>

Coolwebsearch Smartkiller

<http://www.safer-networking.org/files/delcwssk.zip>

The above item is sometimes necessary if CWShredder detects a SmartSearch2 variant on your PC.

Spybot S&D

<http://www.safer-networking.org/index.php?page=download>

Spybot Tutorial (Must Read)

<http://www.safer-networking.org/index.php?page=tutorial>

Other tutorials for Spybot S&D (Also must read)

<http://www.bleepingcomputer.com/forums/index.php?showtutorial=43>

<http://tomcoyote.com/SPYBOT/index1.php>

<http://tomcoyote.com/SPYBOT/index2.php>

This item below is designed to *prevent* installation of malware and the like by comparing known CLSID's of these "bad guys" with what is in its definitions. By enabling a *Kill Bit* it prevents known malignant ActiveX from being installed or run on your machine. It doesn't remove anything, nor will it fix anything that is already in your PC. Rather, it will prevent

installation or re-installation of the item once it has been removed either manually, or by the use of another program which will perform the duty of removing the spyware.

microsoft.public.windows.inetexplorer.ie6.browser: Re: bannerfarm and other pop ups

SpywareBlaster (prevents installation of spyware, Trojans, etc.)

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

SpywareBlaster Tutorial

<http://www.bleepingcomputer.com/forums/index.php?showtutorial=49>

SpywareGuard (companion program to SWB, above)

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

SpywareGuard Tutorial

<http://www.bleepingcomputer.com/forums/index.php?showtutorial=50>

If you use Spybot S & D, be sure to clean ***ONLY*** the items displayed in ***RED***. DO NOT clean any items displayed in Black or Green at this time.

Lastly there is HijackThis. Hijack this is a very powerful, last resort type of program which is generally best used in conjunction with help from those who deal with the findings of the log created by the HijackThis scan.

It does nothing in the scan itself; it merely says what is in and running on your PC. The items must be checked—marked to be "cleaned". You must know ***exactly*** what you are checking—off before you proceed.

If you don't, you can quite possibly disable many useful and vital functions of your PC. Remember; read the Tutorials, and seek help at SpywareInfo Forums, Net—Integration, or TomCoyote forums for safety's sake.

HijackThis

<http://www.spywareinfo.com/~merijn/downloads.html>

If the preceding site is down, you may get HijackThis from Major Geeks (amongst other sites as well)

Hijack This (from Major Geeks)

<http://www.majorgeeks.com/download3155.html>

HijackThis Tutorials ****(MUST READ)****

<http://www.spywareinfo.com/~merijn/htlogtutorial.html>

<http://www.bleepingcomputer.com/forums/index.php?showtutorial=42>

<http://hjt.wizardsofwebsites.com/>

Where to seek help with your HijackThis scan log

SpywareInfo Forums

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

other help forums for HijackThis:

Net—Integration

<http://forums.net-integration.net/index.php?c=19>

TomCoyote

<http://forums.tomcoyote.com/index.php?showforum=27>

McAfee AVERT Stinger

<http://vil.nai.com/vil/stinger/>

avast! Virus Cleaner – free virus & worm removal tool

http://www.avast.com/eng/avast_cleaner.html

Re: bannerfarm and other pop ups

NOTE: With the above tools, particularly Avast Virus cleaner, be sure to disable your in PC Anti-virus utility.

Try F-Prot for DOS (I don't know if this will work on XP systems however)

http://www.f-prot.com/products/home_use/dos/

http://www.f-prot.com/products/home_use/

<http://www.claymania.com/f-prot.html>

If you can use this program, be sure to make certain the most recent Updates are obtained for it.

http://www.f-secure.com/download-purchase/dos_updates.shtml

F-Secure Anti-Virus for DOS (F-PROT edition)

Update Macro.def to your system to get up-to-date macro virus protection.

The other Anti-Virus databases, Sign.def and Sign2.def are updated weekly.

They have definitions for all other kinds of viruses except macro-viruses.

MACRO.DEF definition file

SIGN.DEF definition file

SIGN2.DEF definition file

On-Line Virus scanners:

RAV Antivirus Online Virus Scan

<http://www.ravantivirus.com/scan/>

Command on Demand

<http://www.authentium.com/solutions/cod/index.cfm>

Freedom on-line virus check

<http://www.freedom.net/viruscenter/onlineviruscheck.html>

TrendMicro Housecall (also detects some Trojans)

<http://housecall.trendmicro.com/>

BitDefender Scan Online

<http://www.bitdefender.com/scan/licence.php>

Kaspersky Online Virus Scanner

<http://www.kaspersky.com/remoteviruschk.html>

The above scanner works differently from most; it is a server based scanner, and will only scan individual files, or directories which are limited

to 1 MB in total size. It will not do a full system scan.

Hauri LiveCall Online virus scanning

<http://www.globalhauri.com/html/products/livecall.html>

The above is also server based if I remember correctly

Panda on-line virus scan

<http://www.pandasoftware.com/activescan/activescan.asp>

McAfee FreeScan

<http://us.mcafee.com/root/mfs/default.asp>

microsoft.public.windows.inetexplorer.ie6.browser: Re: bannerfarm and other pop ups

Symantec Security Check (page offers security and/or virus scan)

<http://snipurl.com/7gz1>

More general info you should be aware of:

The Parasite Fight; Quick Fix Protocol

<http://www.aumha.org/a/quickfix.htm>

How to surf the Internet more safely with Internet Explorer

<http://www.infinisource.com/techfiles/surf-safe.html>

So how did I get infected in the first place?

<http://boards.cexx.org/viewtopic.php?t=957>

Rogue/Suspect Anti-Spyware Products & Web Sites

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

HTH –

LuckyStrike

LS@smokedamagedfurniture.youcandriveitawaytoday.com

How to make a good newsgroup post:

<http://www.dts-l.org/goodpost.htm>

<http://home.satx.rr.com/badour/html/post.html>

"Adrienne" <anonymous@discussions.microsoft.com> wrote in message
news:035701c46df6\$570934a0\$a301280a@phx.gbl...

- > Amending an earlier request, I am trying to get rid of pop
- > ups boxes titled Microsoft Internet
- > Explorer "bannerfarm." Further checking made it clear it
- > is a common problem, hard to get rid of. I downloaded
- > Spybot, which picked up many problems and removed them.
- > Then I pd. for SpyAssassin and ran it. The pop ups
- > continue: they're usually bannerfarm ads for Tiffany, Red
- > Lobster, AOL, etc. well-known sites. Any other
- > suggestions besides running spyware to get rid of these?
- >
- >