

Re: Spyware & others

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-06/1523.html>

From: Jim Byrd (jrbyrd_at_spamlessadelphia.net)

Date: 06/22/04

Date: Tue, 22 Jun 2004 13:26:07 -0700

Hi Fernando – To answer your specific question, open Windows Explorer and navigate to the folder where these programs are stored, usually |Program Files|Lavasoft|AdAware 6 and |Program Files|Spybot – Search and Destroy and then double clicking on Ad-aware.exe or SpybotSD.exe respectively. You can open Windows Explorer from Start|Run|Programs|Accessories.

However, if you've a CWS problem, a better approach is to use CWShredder, as follows, since it handles more of the CWS variants and is more frequently updated for new ones:

Sounds like this might be a variant of some malware called CoolWebSearch (if CWShredder doesn't fix it, then see AdAware, SpyBot, and HijackThis, below, in that order). Do the following:

Before you try to remove spyware using any of the programs below, download a copy of LSPFIX from any of the following sites:

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

<http://www.spychecker.com/program/winsockxpfix.html> (if your OS is Win2k or XP)

The process of removing certain malware may kill your internet connection. If this should occur, this program, LSPFIX, will enable you to regain your connection.

Download, UPDATE before running, and run:

<http://209.133.47.200/~merijn/files/CWShredder.exe> to remove the parasite.

BE SURE to close All instances of IE and OE. You may also get it here if that link is blocked: <http://www.zerosrealm.com/downloads/CWShredder.zip>

BE SURE that you get v.158 or later!

You will need to show Hidden files first and then at the end clear the malware garbage from your System Restore backups after you've cleaned up. It's best to perform CWShredder (and most other malware fixers too) from Safe mode and then reboot. AFTER cleaning things up, then you can disable and then re-enable System Restore. See ***** below.

microsoft.public.security.virus: Re: Spyware & others

The following links give instructions on how to do these various functions:

HOW TO Restart in Safe Mode

<<http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2001052409420406>>

HOW TO Enable Hidden Files

<<http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2002092715262339>>

HOW TO Disable/Flush System Restore (do this at the end AFTER cleaning or use the suggested procedure for XP at the *****'s)

<<http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2001111912274039>>

(WinXP)

<<http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2001012513122239>>

(WinME)

Then download and run:

http://www.kellys-korner-xp.com/regs_edits/iegentabs.reg to restore your tabs and remove any restrictions that the parasite has put in place.

Now download and run:

http://www.kellys-korner-xp.com/regs_edits/RestoreSearch2.REG to restore your search functions if they've been affected (as they probably will have been).

Be sure that you also download and install hotfix Q816093, here:

<http://support.microsoft.com/?kbid=816093>

which blocks the exploit upon which this parasite family depends.

However, this also indicates that you may have acquired some other malware along the way. 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.

Get Ad-Aware 6.0, Build 181 or later, here:

<http://www.javasoftusa.com/support/download/>. UPDATE 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 and fixing things with SpyBot S&D, be sure to re-boot and rerun SpyBot again and repeat this cycle until you get a

Re: Spyware & others

microsoft.public.security.virus: Re: Spyware & others

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>

Both of these programs should normally be UPDATED and run after doing any other fix such as CWShredder and, as a minimum, normally at least once a week.

If they don't fix it then start here:

Download HijackThis, free, here:

<http://209.133.47.200/~merijn/files/HijackThis.exe> (Always download a new fresh copy of HijackThis [and CWShredder also] – It's UPDATED frequently.)

You may also get it here if that link is blocked:

<http://www.majorgeeks.com/downloadget.php?id=3155&file=3&evp=3304750663b552982a8baee6434cfc13>

In Windows Explorer, click on Tools|Folder Options|View and check "Show hidden files and folders" and uncheck "Hide protected operating system files". (You may want to restore these when you're all finished with HijackThis.)

Unzip the downloaded HijackThis to any convenient folder, start it then press Scan. Click on SaveLog when it's finished which will create hijackthis.log. Now click the Config button, then Misc Tools and click on Generate StartupList.log which will create Startuplist.txt

Then go to one of the following forums:

Spyware and Hijackware Removal Support, here:

<http://216.180.233.162/~swicom/forums/>

or Net-Integration here:

<http://www.net-integration.net/cgi-bin/forum/ikonboard.cgi?s=d3c2c886d536d57b5f65b6e40c55365e:act=ST:f=27:t=>

or Tom Coyote here: <http://forums.tomcoyote.org/index.php?act=idx>

or Jim Eshelman's site here: <http://forum.aumha.org/>

Sign in, then copy and paste both files into a message asking for assistance, Someone will answer with detailed instructions for the removal of your parasite(s).

ONLY IF you've successfully eliminated the malware, you can now make a new, clean Restore Point and delete any previously saved (possibly infected) ones. The following suggested approach is courtesy of Gary Woodruff: For XP you can run a Disk Cleanup cycle and then look in the More Options tab. The System Restore option removes all but the latest Restore Point. If there

microsoft.public.security.virus: Re: Spyware & others

hasn't been one made since the system was cleaned you should manually create one before dumping the old possibly infected ones.

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.javacoolsoftware.com/spywareguard.html> (Monitors for attempts to install malware) Keep it UPDATED. Both Very Highly Recommended

Finally, go to Windows Update and ensure that ALL Critical updates are installed.

--

Please respond in the same thread.

Regards, Jim Byrd, MS-MVP

In news:1f97201c4588d5179af200\$a601280a@phx.gbl,

Fernando Melegrito <anonymous@discussions.microsoft.com> typed:

> I am also attempting to rid my PC from CoolWeb Spyware. I

> have used Adaware and SpyBot with little success. I have

> tried running Adaware and SpyBot in SAFE mode, but neither

> program appears on my desk top when I am in SAFE mode. Is

> there another way I can run the programs while I am in

> safe mode?

>

>> -----Original Message-----

>> Mark,

>>

>> Have you run the spyware programs in safe-mode?

>> Do you have all the latest patches installed on your computer, and is your

>> antivirus up to date?

>> You may want to use a 3rd party web based antivirus scanner to scan your

>> computer if all of the above steps have been completed.

>>

>> Hope that helps!

>>

>> Steve Dodson [MSFT]

>> PSS Security

>> MCSE, CISSP

>>

>> --

>>

>> This posting is provided "AS IS" with no warranties, and confers no rights.

>> Use of included script samples are subject to the terms specified at

>> <http://www.microsoft.com/info/copyright.htm>

>>

>> Note: For the benefit of the community-at-large, all responses to this

>> message are best directed to the newsgroup/thread from which they

Re: Spyware & others

microsoft.public.security.virus: Re: Spyware & others

```
>> originated.
>> -----
>>> Content-Class: urn:content-classes:message
>>> From: "Mark A. Connelly" <anonymous@discussions.microsoft.com>
>>> Sender: "Mark A. Connelly" <anonymous@discussions.microsoft.com>
>>> Subject: Spyware & others
>>> Date: Mon, 21 Jun 2004 11:25:27 -0700
>>> Lines: 23
>>> Message-ID: <1f71701c457bd$202a8730$a401280a@phx.gbl>
>>> MIME-Version: 1.0
>>> Content-Type: text/plain;
>>> charset="iso-8859-1"
>>> Content-Transfer-Encoding: 7bit
>>> X-Newsreader: Microsoft CDO for Windows 2000
>>> X-MimeOLE: Produced By Microsoft MimeOLE V5.50.4910.0300
>>> Thread-Index: AcRXvSAov6ezusLKRvqoUaplUBm7zA==
>>> Newsgroups: microsoft.public.security.virus
>>> Path: cpmsftngxa10.phx.gbl
>>> Xref: cpmsftngxa10.phx.gbl microsoft.public.security.virus:54762
>>> NNTP-Posting-Host: tk2msftngxa12.phx.gbl 10.40.1.164
>>> X-Tomcat-NG: microsoft.public.security.virus
>>>
>>> I am having a problem with spyware & other stuff.
>>>
>>> I took my computer to a computer place and they help
>>> spoon up my computer and they installed Hijack This and
>>> Ad Adaware but I am still getting the pop ups and
>>> redirection to "about:blank".....I keep deleting but to
>>> no avail.
>>>
>>> Here is one of the lines:
>>>
>>> N2-Netscape 6:user_pref("browser.startup.homepage",
>>> "http://home.netscape.com/");
>>> (c:\documents and settings\mark connelly\application data\
>>> mozilla\profiles\default\fx33pwoz.slt\pref.js)
>>>
>>> Detailed information on N2: lop.com
>>>
>>> I have searched high and low but again to no avail.
>>> I don't even use netscape!
>>>
>>> What can I do next.
>>>
>>> TYIA!
>>>
>> .
```