

## Re: Tools/internet options restricted

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6.browser/2004-06/3730.htm>

---

**From:** Jim Byrd ([jrbyrd\\_at\\_spamlessadelphia.net](mailto:jrbyrd_at_spamlessadelphia.net))

**Date:** 06/14/04

Date: Sun, 13 Jun 2004 19:42:36 -0700

Hi Helliott – 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.

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>>

microsoft.public.windows.inetexplorer.ie6.browser: Re: Tools/internet options restricted

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](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](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.lavasoftusa.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 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>

Re: Tools/internet options restricted

microsoft.public.windows.inetexplorer.ie6.browser: Re: Tools/internet options restricted

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>

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 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:

Re: Tools/internet options restricted

microsoft.public.windows.inetexplorer.ie6.browser: Re: Tools/internet options restricted

<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:1bdb301c451b55f2f43e80\$a501280a@phx.gbl,  
anonymous@discussions.microsoft.com <anonymous@discussions.microsoft.com>  
typed:

> Adaware and Spybot dont produce any results. Haven't  
> tried hijackthis yet.

>

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

>> Sounds like Spyware. When you said you could not find it what did you  
use

>> to look for it with?

>>

>> Do you have Anti-Spyware protection?

>>

>> Here are two good programs. You should use both. They are both free.

>> Please read the instructions. Both sites have help and forums if you  
need

>> it. Once you download them check for Updates Before you scan. This is

>> important. New variants of spyware are spread daily and these programs  
need

>> to be updated before you scan.

>> Spybot - <http://www.safer-networking.org>

>> Ad-aware - [www.lavasoftusa.com](http://www.lavasoftusa.com)

>>

>> Spyware Tools:

>> Hijack This - <http://209.133.47.200/~merijn/files/HijackThis.exe>

>> CWShredder - <http://209.133.47.200/~merijn/files/CWShredder.exe>

>>

>> Alternate Download sites:

>>

>> Hijack This - <http://tomcovote.com/hit>

>> CW Shredder - <http://aumha.org/downloads/cwshredder.zip>

>>

>> Spyware Info. - Helpful Links

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

>> <http://www3.telus.net/dandemar/slowcom.htm>

>> <http://www.pestpatrol.com/>

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

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

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

>> <http://www.aumha.org/>

>> <http://secunia.com/>

>> <http://www.unwantedlinks.com/intro.htm>

>>

Re: Tools/internet options restricted

microsoft.public.windows.inetexplorer.ie6.browser: Re: Tools/internet options restricted

```
>> Once you have cleaned your system check for Windows Updates.
>>
>> Windows Updates - Update Windows regularly (at the very least once a
>> month) - ALWAYS download Critical Updates. You can set your computer for
>> automatic updates if you prefer.
>>
>>
>> "helliott" <anonymous@discussions.microsoft.com> wrote in message
>> news:1b96b01c4517e$6712c8f0$a601280a@phx.gbl...
>>> Something has put a restriction on my "tools" menu and
>>> wont allow me to use "internet options". I get msg:
>>> "This operation has been cancelled due to restrictions
>>> placed on this computer."
>>> I can get to Internet Options thru Control Panel but the
>>> Home Page is locked out so I cant change it. I suspect
>>> spyware but cant find it. ( I run XP, and this does not
>>> show up on other family members IE.)
>>> Any suggestions would be appreciated.
>>
>>
>> .
```