

Re: ntsearch invading my Internet browsing

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6.ieak/2004-06/0097.html>

From: Jerry Arzin (h974483_at_graduate.hku.hk)

Date: 06/12/04

Date: 12 Jun 2004 01:29:01 -0700

"Jim Byrd" <jrbyrd@spamlessadelphia.net> wrote in message
news:<eYKtTb\$TEHA.760@TK2MSFTNGP12.phx.gbl>...

> *Hi Amy – This is a variant of some malware called CoolWebSearch (if not by
> CWShredder, 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.mvps.org/sramesh2k/winsock.htm>

> <http://www.spychecker.com/program/winsockxpfix.html>

> *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:*

>
>

microsoft.public.windows.inetexplorer.ie6.ieak: Re: ntsearch invading my Internet browsing

- > *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.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:*

Re: ntsearch invading my Internet browsing

microsoft.public.windows.inetexplorer.ie6.ieak: Re: ntsearch invading my Internet browsing

- > <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/alexa.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;>
- >
- > 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).
- >
- >

Re: ntsearch invading my Internet browsing

microsoft.public.windows.inetexplorer.ie6.ieak: Re: ntsearch invading my Internet browsing

> *****
> *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:
>
> <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:1b58901c44fd8\$7f9ad400\$a101280a@phx.gbl,
> Amy <anonymous@discussions.microsoft.com> typed:
> > I am suddenly finding that everything I click on in web
> > pages is directing me to an ntsearch web page offering
> > search options. On every web page, there are loads of
> > blue links, and only a few are genuine and direct me to
> > where I want to go, the rest are all ntsearch.
> > It appears that something has invaded my computer, which
> > is only a few weeks old, as this has only been happening
> > for the last few days. I am also constantly being
> > blocked access to trusted and well-used sites.
> > Any advice on how to sort this out?
> > Thanks!
> > Amy

Does it work???

Re: ntsearch invading my Internet browsing