

## Re: Browser goes to unwanted page when invalid web address is entered.

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6.browser/2004-04/6700.htm>

---

*anonymous\_at\_discussions.microsoft.com*

*Date:* 04/20/04

Date: Tue, 20 Apr 2004 09:56:33 -0700

Jim:

When I go to the page with the microsoft hotfix, it refers me to the Microsoft Update page, which looks for updates that I do not have. It does not detect that I do not have hotfix Q816093. I checked to see if I already have it, and I do not. Is there anywhere else I can get the fix?

Kevin

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

>Hi Kevin – Sounds like this might be a variant of some malware called

>CoolWebSearch (if not, then see AdAware, SpyBot, and HijackThis, below). Do

>the following:

>

>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>

>

>You will need to disable System Restore and then reboot your system

>in order to clear the CWS garbage from the backups.

After rebooting, then

>re-enable System Restore.

>

>The following link gives instructions on how to disable it:

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

Open&src=sec\_doc\_nam&docid=2001012513122239&nsf=tsngeninfo.  
nsf&view=docid&dtype=&prod=&ver=&osv=&osv\_lvl=

>

>

>

>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.

>

>Be sure that you also download and install hotfix

Q816093, here:

>

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

>

>which blocks the exploit upon which this parasite family  
depends.

>

>Now download and run:

>[http://www.kellys-korner-](http://www.kellys-korner-xp.com/regs_edits/RestoreSearch2.REG)

xp.com/regs\_edits/RestoreSearch2.REG to restore

>your search functions.

>

>

>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-](http://www.net-integration.net/cgi-bin/forums/ikonboard.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>

>

>

>

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

id=3155&file=3&evp=3304750663b552982a8baee6434cfc13

>

>Unzip it 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-](http://www.net-integration.net/cgi-bin/forum/ikonboard.cgi)

bin/forum/ikonboard.cgi?

s=d3c2c886d536d57b5f65b6e40c55365e;act=ST;f=27;t=6949

>

>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).

>

>

>

>

>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

>

>

>--

>Please respond in the same thread.

>Regards, Jim Byrd, MS–MVP

>

>

>

> In news:151a01c42689\$fc5795f0\$a101280a@phx.gbl,

>Kevin <anonymous@discussions.microsoft.com> typed:

>> Hello:

>>

>> Whenever I put an incorrect web address, the browser

>> goes to some Web search page that I do not want.

>> Something called "WebCoolSearch", some pay per click

microsoft.public.windows.inetexplorer.ie6.browser: Re: Browser goes to unwanted page when invalid web address is entered

>> *advertising page. I did a Windows system restore (the  
>> function that takes the computer to a previous date)  
that  
>> still did not correct the problem. I changed the  
address  
>> of the homepage. Nothing works. I believe it is  
because  
>> some type of spyware, but I thought the Windows system  
>> restore would solve the problem. How can I stop the  
>> browser from going to this page?  
>>  
>> Kevin  
>  
>  
>*