

Re: my browser hijacked Help!

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2003-10/0400.html>

From: Kent W. England [MVP] (kwe_at_mvps.org)

Date: 10/03/03

Date: Thu, 2 Oct 2003 19:27:56 -0700

And the removal instructions in that web page you see when you try to search are apparently wrong, if I read the Symantec and Network Associates descriptions rightly. You need to use a tool to remove it or manual instructions.

The reason you see that web page is that the bug redirects your DNS and many search hosts to specific IP addresses. Since these addresses are now known, they can be taken back from the perp and used to advise users of their infection.

--

Kent W. England, Microsoft MVP for Windows
"Bill Sanderson" <Bill_Sanderson@msn.com.plugh.org> wrote in message
news:uamc3VSiDHA.620@TK2MSFTNGP11.phx.gbl...
> I believe you have what Symantec describes here:
>
> <http://www.symantec.com/avcenter/venc/data/trojan.ghosts.html>
>
>
> "chris Scholle" <chrisscholle@hotmail.com> wrote in message
> news:1e61a01c38923\$a7e74c80\$a601280a@phx.gbl...
> When I click on internet explorer and try to type in any
> search engine I get redirected to some site. I ran
> McCaffee and a spy ware and don't see any viruses. How do
> I get control over my browser. This is what I get when I
> type in a www.Google.com. Is it safe to do what it says??
> THIS IS THE MESSAGE:
>
> Are you trying to get to Google?
> Your computer is running software that doesn't allow you
> to use Google.
> You're seeing this page because your computer is trying to
> send you to a website that is pretending to be Google.
> Over the past few weeks, you may have seen a website that
> looks like Google, but launches pop-up windows and does
> not work like Google. That page is not affiliated with
> Google in any way and is intended to deceive you.
>
> Why is this happening?
> Most likely a program was installed on your computer
> automatically and without your knowledge when you
> downloaded an otherwise harmless piece of software. Or you
> may have been tricked into clicking on a disguised
> download button while visiting a website.
>

microsoft.public.security.virus: Re: my browser hijacked Help!

> What can I do about it?
> This problem can be fixed fairly easily, but will require
> that you make changes in a file that is part of your
> computer's operating system. You should always be cautious
> when making these kinds of adjustments, as they may affect
> the performance of your computer. If you are not
> comfortable doing this yourself, you may want to print out
> this page and show it to someone whose technical knowledge
> you trust.
>
> What steps do I take?
> The first step is to remove the entry for Google from your
> hosts file. This entry is telling your computer where to
> send your computer instead of to Google.
>
> In Windows, open the Notepad program. You can do this by
> going to the Start menu in the lower left of your screen,
> selecting "Programs," then "Accessories,"
> then "Notepad."
>
> In the Notepad menu, click on "File," then "Open." You
> will see a new window asking which file to open. You may
> need to change "Files of type" to "All Files" instead
> of "Text Documents". The actual file to open is listed
> below:
>
> If your computer is running Windows XP, Window NT, or
> Windows 2000, the file is located in the folder found by
> following this path:
>
> My Computer >Local Disk(C) >Windows >System32 >Drivers
> >etc >hosts
>
> If your computer is running Windows 98, Second Edition or
> Windows ME, the file is located in the folder found by
> following this path:
>
> My Computer >Local Disk(C) >Windows >hosts
>
> Once you have opened this file, remove entirely any line
> of text that contains "google.com", "www.google.com" or
> other Google domains (such as "google.co.uk"). To remove
> the text, highlight it by dragging your pointer across the
> line while holding down the mouse button. Once the text is
> highlighted, hit the Backspace or Delete button, then
> save the file by going to the File menu and
> clicking "Save." You can now exit Notepad.
>
> What else can I do?
> You might want to try software that attempts to detect and
> uninstall programs like this one. While we do not have a
> relationship with anyone who offers this software and we
> cannot endorse a particular product, the most popular
> programs for doing this seem to be Spybot Search and
> Destroy and LavaSoft's AdAware. The particular program
> affecting your computer is relatively new, so these
> products might not be able to detect and repair this type
> of problem yet.
>
> The next step is to learn more. You can visit
> <http://www.doxdesk.com/parasite/> to review information
> about a number of known self-installing software programs.

microsoft.public.security.virus: Re: my browser hijacked Help!

> Several articles on the web may be helpful, such as
>
> .
> <http://www.theage.com.au/articles/2003/04/14/1050172507212.html>
> html
> . <http://news.com.com/2100-1023-877568.html>
> . <http://news.com.com/2100-1023-257592.html>
>
> Investigate individual programs using search engines. Try
> keywords such as "spyware," "scumware," and "adware."
> Once you're informed, take action. Help your family and
> friends avoid these annoying programs. If you can find the
> site that installed this software on your computer, let
> them know how you feel about it. You might also want to
> track down companies that benefit from having your web
> visits redirected, and share your feelings with them.
>
> Finally, it's quick and easy to file a complaint with the
> Federal Trade Commission (FTC). This U.S. government
> agency handles complaints about deceptive or unfair
> business practices. To file a complaint, visit:
> <http://www.ftc.gov/> and click on "File a Complaint
> Online", or call 1-877-FTC-HELP. Or write to:
>
> Federal Trade Commission
> CRC-240
> Washington, D.C. 20580
>
> If your complaint is against a company in another country,
> you can file it at <http://www.econsumer.gov/>.
>
>