

Re: variant of Win32/inject.... SOLVED!

Source:

<http://www.tech-archive.net/Archive/Vista/microsoft.public.windows.vista.general/2008-07/msg07453.html>

- *From:* silver hair <silverhair@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sun, 20 Jul 2008 18:58:56 -0700
-

hi
no problem I click and watch no harm was done
Nonny tanks for the cookie education
--
lucky me I guess

"Willy" wrote:

First of all many thanks to Willy, Mick, and to all you for helping me, and my apology for including the bogus free-scan URL I received copying into my message. I copied the URL as a warning and to better describe the problem, I assumed nobody would just click without reading.

After installing and running Spybot – Search & Destroy several times I finally got rid of the Trojan and Vista is running OK.

Spirit: as I say in my original message, I HAD NOD32, Windows Defender and my entire Vista updates up to date, so it is clear that NOD32 and Defender failed to stop the threat until it was already inside my system.

NOD32 was partially disabled by the Trojan, as it was able to block the browser to go to the fake free-viruscan URL, but I couldn't run it with Vista in Safe Mode nor was NOD32 able to remove the Trojan, Spybot did it

BTW: Windows Defender missed the whole episode..it never even reacted .

Spybot asked for permission to remove several registry keys over a couple of rebooting cycles, afterwards I was really happy and surprised to see that everything is back to normal.

Regards,
Willy.

Re: variant of Win32/inject.... SOLVED!

"Malke" <malke@xxxxxxxxxxxxxxxx> wrote in message
news:uSa1ndZ6IHA.4468@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Willy wrote:

I'm running Vista Ultimate 32 Service Pack-1 with all the
Windows updates, also Windows Defender and
NOD32 antivirus, all up to date and always running. Even so
I got a variant of Win32/injector.BQ Trojan.
Now every time I try to browse a web site or even when
opening a folder a warning pops up that reads:

" your machine is infected with a virus and you should
perform
a free virus scan.then a NOD32 warning appears saying:

<http://free-viruscan.com/00/00/00/error.php>

Description:

Access to the web page was blocked by ESET NOD32
Antivirus.
The web page is on the list of websites with potentially
dangerous
content.

It seems that NOD32 caught this, but my machine is already
infected
as no matter what I do I can't get rid of the problem.

I have performed a full Antivirus and Windows defender
scan, also
I installed Search and Destroy and Adaware, and after
running these
there were some problems detected and apparently
cleaned.but
still the problem.

All mi programs, my e-mail and others are working OK, but

Re: variant of Win32/inject.... SOLVED!

I cant
browse the web or open some folders.

Is there a tool to remove this?

I'll appreciate any help regarding this.

Thanks in advance.
Willy

PS: How I got infected when running NOD32, Windows
Defender, and
my Windows firewall up and running, should I install a
different
antivirus?

NOD32 is excellent. However, from your description of the issue you have
picked up some non-viral malware. Use a malware removal tool to get rid of
it.

Go through these general malware removal steps systematically –
http://www.elephantboycomputers.com/page2.html#Removing_Malware

You obviously don't need to run the antivirus scan unless you haven't done
so in Safe Mode yet. I see that you've already installed Spybot S&D, but I
don't know if you've scanned in Safe Mode, which is important. And
definitely try Malwarebytes' Antimalware program (details at above link).

When all else fails, get guided help. Choose one of the specialty forums
listed at the first link. Register and read its posting FAQ. PLEASE DO NOT
POST LOGS IN THE MS NEWSGROUPS.

Malke
--
MS-MVP
Elephant Boy Computers – Don't Panic!
FAQ – <http://www.elephantboycomputers.com/#FAQ>

--
world
X-No-Archive: Yes