

Re: Virus – 100% CPU resources utilized

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-07/1640.html>

From: Chek (chek_16_at_hootmail.com)

Date: 07/23/04

Date: Fri, 23 Jul 2004 21:34:05 +0100

Steve,

Most current Malware seems to infect IE through the BHO weakness, and switching to another browser will mask the symptoms, while leaving your PC still infected if dormant for the moment.

The resource usage is probably because a little onboard spamming factory goes into action as soon as IE is online.

It's becoming a complex business, and to ensure that you are using the programs you have so far properly and effectively, try following some of the malware removal threads at:

<http://forums.spywareinfo.com/index.php?showforum=18>

You may find it helpful, particularly about using the tools in safe mode and in order.

DO NOT go online afterwards without a firewall activated first.

Hope this helps

Chek

--

Change 'boos' to 'bos' in address to email directly
"Malke" <malke@nospoonnotreally.com> wrote in message
news:OH5baaaaaEHA.596@TK2MSFTNGP11.phx.gbl...

> steve wrote:

>

> > I have a virus and don't know what it is but it uses up
> > 100% of my CPU resources and it is either used up by
> > iexplorer.exe or explorer.exe - I am running Windows2000
> > Prof and have tried McAfee Ver8 but unsuccessful.

>

> What does it mean that you tried McAfee but were unsuccessful? Do you
> mean that you were running without an av installed, thought you had a
> virus, and then tried to install McAfee? If this is the case, here is a
> way to deal with that:

>

> It sounds like you have picked up a virus that immediately breaks any av
> installed. This could happen if you had an older antivirus version,
> weren't updating its definitions or didn't renew your subscription. The
> usual way to deal with this is to:

>

> 1) Take the infected machine off the Internet and any lan immediately.

microsoft.public.security.virus: Re: Virus – 100% CPU resources utilized

> 2) From a different, clean machine download Stinger
> (<http://vil.nai.com/vil/stinger/>) and run it in Safe Mode. Stinger is a
> limited virus checker, but its advantage is that it is standalone and
> doesn't need to be installed.
> 3) Hope that Stinger cleans up the machine enough to be able to
> reinstall your av or install a new, current one. Update its definitions
> and do a full scan.
> 4) Continue the cleaning process by removing any spyware with Spybot
> Search & Destroy (<http://www.safer-networking.org>) and Ad-aware
> (<http://www.lavasoftusa.com>). These programs are free, so run them both
> since they complement each other. You may also want to run CWS shredder
> and HijackThis from <http://aumha.org/freeware.htm>. Although CWS shredder
> is no longer being updated, it will still clean older variants of the
> CoolWebSearch malware. Be sure to update these programs before running
> them. Always read the instructions before running a spyware removal
> tool. It is best to run antivirus and spyware removal tools in Safe
> Mode.
> 5) After you've installed your full-featured av, updated its definitions
> and run a full system scan.
> 6) Make sure you are running a firewall.
> 7) Go to Windows Update and apply all security patches for your
> operating system. Do not install drivers from Windows Update.
>
> Malke
> --
> MS MVP - Windows Shell/User
> Elephant Boy Computers
> www.elephantboycomputers.com
> "Don't Panic!"