

Re: MSN Virus

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2007-07/msg00006.html>

- *From:* "David H. Lipman" <DLipman~nospam~@Verizon.Net>
 - *Date:* Mon, 2 Jul 2007 16:05:27 -0400
-

From: "lil_guy009" <lilguy009@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

| My computer has been infected by a virus spreading around by MSN
| chatting. My Windows Defender calls it
| 'SettingsModifier:Win32/PossibleHostsFileHijack'. This has shut down my Zone
| Alarm firewall, which I reinstalled to no effect. I've tried getting into
| MSConfig, but that opens up for about half a second and then the virus closes
| the window. I'm betting that I have more programs that are shut down, but I
| haven't begun a thorough observation, yet.

| Does anyone know more about this
| SettingsModifier:Win32/PossibleHostsFileHijack virus that spreads by MSN?

| Does anyone know how to remove it? Windows Defender detects it at startup
| and says it successfully cleans/deletes/quarantines it, but it's always
| coming back.

For non-viral malware...

Please download, install and update the following software...

* Ad-aware SE 2007
<http://www.lavasoft.de/>
<http://www.lavasoftusa.com/>
<http://www.lavasoft.de/ms/index.htm>

* SpyBot Search and Destroy v1.4
<http://security.kolla.de/>
<http://www.safer-networking.org/microsoft.en.html>

* SuperAntiSpyware
<http://www.superantispyware.com/superantispywarefreevspro.html>

After the software is updated, I suggest scanning the system in Safe Mode.

For viral malware...

Re: MSN Virus

* Download MULTI_AV.EXE from the URL ---
<http://www.pctipp.ch/downloads/dl/35905.asp>

To use this utility, perform the following...

Execute; Multi_AV.exe { Note: You must use the default folder C:\AV-CLS }

Choose; Unzip

Choose; Close

Execute; C:\AV-CLS\StartMenu.BAT

{ or Double-click on 'Start Menu' in C:\AV-CLS }

NOTE: You may have to disable your software FireWall or allow WGET.EXE to go through your FireWall to allow it to download the needed AV vendor related files.

C:\AV-CLS\StartMenu.BAT --- { or Double-click on 'Start Menu' in C:\AV-CLS }

This will bring up the initial menu of choices and should be executed in Normal Mode.

This way all the components can be downloaded from each AV vendor's web site.

The choices are; Sophos, Trend, McAfee, Kaspersky, Exit this menu and Reboot the PC.

You can choose to go to each menu item and just download the needed files or you can download the files and perform a scan in Normal Mode. Once you have downloaded the files needed for each scanner you want to use, you should reboot the PC into Safe Mode [F8 key during boot] and re-run the menu again and choose which scanner you want to run in Safe Mode. It is suggested to run the scanners in both Safe Mode and Normal Mode.

When the menu is displayed hitting 'H' or 'h' will bring up a more comprehensive PDF help file. <http://www.ik-cs.com/multi-av.htm>

Additional Instructions:

http://pcdid.com/Multi_AV.htm

* * * Please report back your results * * *

Dave

<http://www.claymania.com/removal-trojan-adware.html>

<http://www.ik-cs.com/got-a-virus.htm>

.