

Re: W32 trojan-gen {VB}

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2007-01/msg00060.html>

- *From:* Zakynthos <Zakynthos@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sun, 7 Jan 2007 11:19:00 -0800
-

David,

Scanned i Safe Mode with: Sophos, Trend, McAfee, Kaspersky – only Kaspersky found 2 viruses –(1 known: (W32) and 1 unknown???) – from the log file I can see that it tried and FAILED to disinfect Win32 trojan-gen.

Re-ran Avast in Nomal Mode & it detected again the Win32 trojan-gen – I chose the 'delete permanently' option – log file said that delet was successul – but on reboot and re-run of Avast I can see status is still INFECTED.

So, what now?

Many thanks for your help.

"David H. Lipman" wrote:

From: "Zakynthos" <Zakynthos@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

| My computer is infected with this virus/worm and my antivirus program (Avast)
| is unable to quarantine/remove/rename/move it etc. although I do know the
| path from the dialogue box.

|
| My Windows folder is now showing 15 Gb (with only a 14 Gb hard drive) and I
| believe the virus is copying the contents of Windows to that folder on boot
| (???)

|
| How can I get rid of this virus/worm/trojan?

Download MULTI_AV.EXE from the URL --
http://www.ik-cs.com/programs/virttools/Multi_AV.exe

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

Re: W32 trojan-gen {VB}

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>