

Re: Wierd Odd Strange Text Files in C: Drive Windows 2003

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-04/msg00139.html>

- *From:* "David H. Lipman" <DLipman~nospam~@Verizon.Net>
 - *Date:* Mon, 10 Apr 2006 11:00:44 -0400
-

From: "pacific" <cliff@xxxxxxxxxxxxxxxxxxx>

| Hi,

| Occasionally there appear anywhere from 1 to 4 strange files in the C:
| folder.

| Often they have FTP addresses and username and passwords. Sometimes
| they don't have anything in them.

| Sometimes they are accompanied by some small .EXE file. Always when
| these are present FTP, TFTP, etc. try to access the internet but are
| stopped by our Software Firewall.

| Occasionally a strange User appears in the Windows Users. Always with a
| \$ in the front. Example: \$strangename

| I have ran multiple virus scans, trojan scans, and security scans. The
| computer checks out perfectly.

| When the user and files are deleted and the computer is rebooted
| everything is fine.

| Anyone know how the heck these files are appearing and how they are
| triggering FTP and TFTP? How is the strange username being created? Is
| there a way to stop additional Windows Users from being added?

| Thanks,

| Cliff

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

Re: Wierd Odd Strange Text Files in C: Drive Windows 2003

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://harrisonrj.home.comcast.net/step_by_step_pc_cleaning_process.htm#Step 3 %96 Getting Help](http://harrisonrj.home.comcast.net/step_by_step_pc_cleaning_process.htm#Step_3_%96_Getting_Help)

* * * Please report back your results * * *

--

Dave

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

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

.