

RE: Virus causing System32 folder to be opened at startup?

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help_and_support/2006-02/msg01084.htm

- *From:* "paulibus" <paulibus@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 7 Feb 2006 18:32:27 -0800
-

Some malware will come with their own backups to recreate it after it has been removed. The backups have gibberish names, which sometimes are changed by the perpetrator to avoid deletion by a/v software. If you remember the date the trojan was put on your computer, the backups will have the same date.

"elp70" wrote:

Every time I log on or reboot the System32 folder opens up. This started after I had found a virus Trojan Downloader.Win32.Zlob.ad, which was subsequently removed.

I have read the previous threads on the System32 folder opening topic and have done the following:

1. I read the article at <http://support.microsoft.com/?kbid=170086> regarding two Windows registry keys. This fix did not help as I do not have any anomalous looking registry entries based on the support page. No open ended , etc. These registry entries looked OK.

2. I tried to run the edit on Kelly's site:
http://www.kellys-korner-xp.com/xp_tweaks.htm
Line 260: System32 Folder Opens Upon Boot

I received the error message:
This script cannot repair your issue. The expected registry value was not found.

3. I checked our other identical computer at home (referenced as good from now on) and found something interesting. On the problem computer there was an entry at HKCU\Software\Microsoft\Windows\CurrentVersion\Run for the data value ctfmon.exe at C:\WINDOWS\system32. The good computer does NOT have this value.

4. Next, I ran msconfig but did not see anything unexpected under Startup other than ctfmon.exe located at
HKCU\Software\Microsoft\Windows\CurrentVersion\Run.

RE: Virus causing System32 folder to be opened at startup?

The good computer does NOT have ctfmon.exe under Startup.

5. I tried deleting this entry from the registry of the failing computer. Once I did this it disappeared from the msconfig Startup screen as expected.

6. Rebooting does not prevent the System32 folder from reappearing. The ctfmon.exe is NOT listed under the Startup tab of msconfig, but it is then listed under the following registry key:
HKCU\Software\Microsoft\Windows\CurrentVersion\ShellNoRoam\MUICache\ with the data CTF Loader.

7. Rebooting again does not prevent the System32 folder from reappearing, but now the ctfmon.exe registry key is gone and the msconfig Startup reference is gone.

8. As soon as I start IE6, the ctfmon.exe registry key and Startup references are back.

9. Any idea on how this is happening? I was focusing on ctfmon.exe because of differences between the 2 computers and because I found some references to a virus masquerading as the ctfmon.exe file. I checked and found only one ctfmon.exe file on the failing computer, and it was located in the C:\WINDOWS\System32 directory.

Any help you can provide me with fixing this problem would be greatly appreciated. I m not sure what to do next other than a reinstall. I ve tried 4 different virus scanners and they all come up clean.