

Re: Files in system32/drivers/etc

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help_and_support/2007-05/msg02003.htm

- *From:* "Wesley Vogel" <123WVogel955@xxxxxxxxxxxxx>
 - *Date:* Sat, 19 May 2007 09:06:10 -0600
-

Ok, there is no Version Tab in properties, all the files were created on same day.

No Version tab usually means that they are 16-bit applications.

The legitimate smss.exe and svchost.exe are NOT 16-bit applications.

Both smss.exe and svchost.exe can be many different trojans. And being in the wrong folder makes yours good candidates.

WINDOWS\system32\drivers\etc\smss.exe

Here is an entry from someone's HijackThis log I got from the web...

O23 - Service: Session Manager Subsystem (Windows smss) - Unknown owner - C:\WINDOWS\system32\drivers\etc\smss.exe
This is NOT legitimate!

WINDOWS\system32\drivers\etc\svchost.exe

Here is an entry from someone's HijackThis log I got from the web...

O4 - HKLM\..\Run: [Windows SP2 Firewall 2005.12.09] c:\windows\system32\drivers\etc\svchost.exe
This is NOT legitimate!

UPDATE your antivirus software and run a full system scan.

UPDATE whatever anti-spyware applications that you have and run a full system scan with each one.

You might want to start in Safe Mode to run your antivirus and anti-spyware software.

Running a full system antivirus scan or anti-spyware scan in Safe Mode can be a good idea. Some viruses and other malware like to conceal themselves in areas Windows protects while using them. Safe mode can prevent those applications access and therefore unprotect the viruses or other malware allowing for easier removal.

Re: Files in system32/drivers/etc

"In safe mode, you have access to only basic files and drivers (mouse, monitor, keyboard, mass storage, base video, default system services), just the minimum device drivers required to start Windows."

Because of that some malware does not load in Safe Mode and is easier to get rid of.

How to start Windows in Safe Mode Windows XP

<http://www.bleepingcomputer.com/forums/index.php?showtutorial=61#winxo>

C:\WINDOWS\system32\edit.com, for example, is a legitimate XP file, is 16-bit and has no Version tab.

<quote>

Identify a 16-bit Program

To identify a 16-bit program:

1. Use Windows Explorer to open the folder that contains the program's executable (.exe) file.
2. Right-click the .exe file, and then click Properties.
3. A 16-bit program does not have a Version tab in this dialog box.

Identify 16-bit Programs that Are Running

To determine if any 16-bit programs are currently running, and identify any that are:

1. Start Task Manager. To do so, right-click a blank spot on the taskbar, and click Task Manager.
2. On the Processes tab, note the contents of the Image Name column.
3. If any 16-bit programs are running, you see an entry for Ntvdm.exe, which is the virtual DOS machine that is provided by Windows XP. You also see wowexec.exe (the Windows on Windows subsystem), and the executable name of each 16-bit program that is running in that WOW virtual machine. As a helpful visual aid, wowexec.exe and the 16-bit executable file names are indented.

<quote>

from...

HOW TO Identify a 16-bit Program in Windows XP

<http://support.microsoft.com/kb/320127>

--

Hope this helps. Let us know.

Wes

MS-MVP Windows Shell/User

In news:FE36344E-9F1A-414C-90C1-24D76CA45AF7@xxxxxxxxxxxxxx,

Alexandr Klein <AlexandrKlein@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> hunted and pecked:

Ok, there is no Version Tab in properties, all the files were created on same day.

I have one active process running from this directory and that is

C:\WINDOWS\system32\drivers\etc\smss.exe, when I kill this process it reappears again after few seconds.

So i guess these files are not safe.

What is disturbing me is, that no AS or AV program found this problem!!

Re: Files in system32/drivers/etc

Thank you

"Wesley Vogel" wrote:

Here's what I have in C:\WINDOWS\system32\drivers\etc\
HOSTS
lmhosts.sam
networks
protocol
quotes
services

Right click the smss.exe and svchost.exe in the etc folder and click Properties.
Compare this info with the smss.exe and svchost.exe in the System32 folder.

There should be a description on both General and Version tabs.
On the Version tab.
Click a category on the left to display the information on the right.
Other version information
Item Name:
Company
File Version
Internal Name
Language
Legal Trademarks
Original File Name
Product Name
Product Version

Chances are that you should delete the smss.exe and svchost.exe from the etc folder.

—

Hope this helps. Let us know.

Wes
MS-MVP Windows Shell/User

In
news:5F7B5618-E547-4C1A-8CCD-9055BDCACAC2@xxxxxxxxxxxxxxxx,
Alexandr Klein <Alexandr Klein@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> hunted
and
pecked:

Hi, can anyone tell me which files should be in directory
system32/drivers/etc? hosts, lmhosts.sam, networks, protocol
and
services only or possibly other files too?

Re: Files in system32/drivers/etc

Re: Files in system32/drivers/etc

I have on my computer some other files in this dir – for example smss.exe, svchost.exe, which should be only in directory system32. If I scan my computer with various antispysware and antivirus programs and online scanners, they find nothing suspicious.

I am little bit confused now, are these files ok or not?