

## Re: HELP SVCHOST

**Source:**

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.termsserv.apps/2004-09/0097.html>

---

**From:** Gustavo Castillo ([gcastillo\\_at\\_evolutionmarketplace.com](mailto:gcastillo_at_evolutionmarketplace.com))

**Date:** 09/10/04

Date: Thu, 9 Sep 2004 19:35:51 -0500

Hi, Question...

svchosts.exe??

svchosts.exe; part of a backdoor trojan.

<http://www.2-spyware.com/file-svchosts-exe.html>

or svchost.exe ?

1. Service Host – Generic Host Process for Win32 Services. Windows 2000/XP only. SVCHOST is a generic process which acts as a host for processes that run from DLLs rather than EXEs. At startup SVCHOST checks the Services portion of the Registry to construct a list of DLL-based services that it needs to load, and then loads them. There can be many instances of SVCHOST running, as there will be one instance of SVCHOST for every DLL-based service or grouping of services (the grouping of services is determined by the programmers who wrote the services in question). Under Windows XP Professional you can find out what DLL-based services SVCHOST is running by typing Tasklist /SVC at a Command Prompt (MS-DOS Prompt – this command is not available in Windows XP Home), while under Windows 2000 you need to use the TLIST -s command from a Command Prompt (MS-DOS Prompt).

**Recommendation :**

An integral part of the operating system, leave alone – multiple instances of SVCHOST is a normal occurrence. If you experience SVCHOST errors, the problem is most likely not with SVCHOST but with the DLLs it is hosting.

2. Many viruses masquerade themselves as SVCHOST to escape detection. Some have names that are similar, such as SCCHOST, while others actually drop a program file called SVCHOST in the Windows or Windows System directory.

**Recommendation :**

The first recommendation is a simple one : always have a good antivirus product which is regularly updated (automatically preferably) and always renew your updates subscription when it expires. To detect if you have a virus that calls itself SVCHOST, first see if it shows up in Starter – if it does, then it is almost certain you have a virus. Secondly, if you have Windows 95/98/ME rather than WinNT4/2000/XP, then it is almost certain you have a virus. Thirdly, go to "Control Panel \ Administrative Tools \

microsoft.public.win2000.termsserv.apps: Re: HELP SVCHOST

Services" and look for any of the following services – if you find any of them, then you probably have a virus : System Important Message service

Svchost.exe in Windows XP

<http://support.microsoft.com/?kbid=314056>

Svchost.exe in Windows 2000

<http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q250/3/20.ASP&N>

Gustavo Castillo

MCP – MVP IIS

gcastillo@elsoporte.com

gac21@hotmail.com

"heather" <anonymous@discussions.microsoft.com> wrote in message  
news:574201c491ae\$1be1dae0\$a601280a@phx.gbl...

> *why all of a sudden does svc.host take up 99% of my cpu.*

> *if it is a virus mcafee does't find it what can i*

> *do?????????*

>