

Re: svchost.exe PLEASE HELP

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2003-09/4767.html>

From: Philip Herlihy (*foof8500_at_REMOVEherlihy.eu.com*)

Date: 09/29/03

Date: Mon, 29 Sep 2003 10:42:32 +0100

2nd posting – first appears to have been dropped (already) from the server
(?)

There are too many possibilities to write a "cookbook" like that, as we don't know what we're looking for. You can read more about svchost.exe here:

<http://support.microsoft.com/default.aspx?scid=kb:en-us:314056> (XP, with link to Win2K version)

(It's Tasklist /SVC that will list the "passengers" of a svchost process).

The only time I had this problem recently was when using Internet Connection Sharing with my XP Pro laptop as host. I got a message "Generic Host Process for Win32 Services..." (that's svchost to you and me) "... has encountered a problem and needs to close..." and my Internet connection wouldn't work. It finally turned out that my firewall (ZoneAlarm Pro) was somehow causing this, and now I disable it (relying on the built-in one) when I use ICS. I have to say that I didn't get any useful information out of Tasklist (which was run before and after, with much comparison of process ids) but you may be luckier. Sometimes you get a situation where you need to get expert help.

What I would suggest: every time this problem happens, go immediately to the Event Log (System and Application) and look at the entries for the last couple of minutes. You may find you spot the same one coming up. Post details of that here, and someone might recognise the cause.

I just looked again at the exact wording of the error message and became suspicious – I doubt a real error message would refer to "svchost.exe" instead of "Generic Host Process...." and probably wouldn't say it "created" an error. This makes me suspect a virus/worm. I typed the exact error message into Google and found this conversation:

<http://www.annoyances.org/exec/forum/win2000/t1063653193>

microsoft.public.security.virus: Re: svchost.exe PLEASE HELP

and this:

http://www.experts-exchange.com/Operating_Systems/Win2000/Q_20706331.html

and this:

<http://bermangraphics.com/problems/blasterworm.htm>

.. and others, all pointing to the Blaster worm.

So, I'd suggest you update your virus definitions asap, run a full scan. Then visit your AV provider's website and search for further advice. You get the Blaster worm if your system isn't updated adequately, so visit www.microsoft.com/windowsupdate and expect a long downloading session.

```
--
#####
## PH, London ##
#####
W. Watson wrote:
> Any further information on the tools you mentioned?
>
> I find looking at the Event Log daunting, or looking at the task mgr
> the same. Who knows what all that stuff means? It would be nice to
> have a written procedure like:
>
> 1. Dialog box appears with message that svchost.exe will be stopped.
> Do not click OK.
> 2. Go to the event log and look for xyz.
> or
> Go to the task mgr and look for abc.
> 3. then note ...
> 4. etc.
>
> Philip Herlihy wrote:
>
>> It's possible that it isn't a virus - if your DAT files really are
>> completely up-to-date then you'd expect them to pick it up.
>>
>> Have a look in the Event Log to see if you can pick up any clues -
>> note that entries are time-stamped. Try running the System File
>> Checker (sfc.exe)
>>
>> http://www.microsoft.com/windows2000/en/datacenter/help/system\_file\_checker.
>> htm
>> in case you have a damaged file.
>>
>> svchost.exe (also known as "Generic Host Process for Win32 services)
>> is a wrapper process which provides a vehicle for other processes to
>> run as services. There are tools which can show you what's running
>> within each instance of svchost (can't think which tool I used at
>> present, and don't have time to research it - missus hovering).
>> Sorry I can't be more helpful.
>>
>> --
>> #####
>> ## PH, London ##
>> #####
>>
```

Re: svchost.exe PLEASE HELP

microsoft.public.security.virus: Re: svchost.exe PLEASE HELP

```
>> Elvis wrote:
>>> I am using Win 2000 prof. and McAfee antivirus which is
>>> always up to date cause I update it daily.
>>>
>>> -----Original Message-----
>>>> I continue getting this error message "svchost.exe has
>>>> created an error and will be closed by windows. I have
>>>> been told that this is as a result of a virus. I was
>>>> attacked by a virus which was detected by my antivirus and
>>>> then cleaned. I have no idea how can it still affect my
>>>> system. Is there anything I can do to get rid of this
>>>> virus and message?
>>>> Thanx
>>>> .
```