

Re: svchost.exe connect port 80 and 443

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2004-02/1590.html>

From: Big Will

(spamWspamisamlspamlspamBspam4spamespamvspaaaammesammityrspam_at_nidontlikespamet)

Date: 02/23/04

Date: Sun, 22 Feb 2004 16:12:55 -0800

Duane Arnold wrote:

> Tiago <tiago@nospam.com> wrote in
> news:Xns9497E533437D0tiagonospamcom@213.228.128.15:
>
>
>> "David Barnes" <david@nospam-bitsolve.com> wrote in
>> news:kz3_b.5329\$QB7.49104967@news-text.cableinet.net:
>>
>>
>>> This sounds like a browser hijack / trojan.
>>>
>>> These tend to 'appear' when you install 'free' software or utilities
>>> from sites on the internet (eg kaza). [no such thing as a free
>>> lunch]. Among other things they steal your personal info, log
>>> keystrokes, sites visited, programs run, documents created/viewed,
>>> and obfuscate access to sites on the internet.. [Eg. type in
>>> www.bbc.co.uk and u get cnn.com.. well I've not seen that, but that's
>>> what they do on a subtle scale.] Try looking through add/remove
>>> programs. You may find some strange entries there.. Use google search
>>> to identify anything that looks strange. You could try and remove
>>> anything unwanted.
>>>
>>> I suggest you update your AV software and enable it to 'find unwanted
>>> programs' and do a FULL scan.
>>> Also download and run spybot search and destroy.. this should hunt
>>> out the hijack..
>>
>> No, I don't think it's anything related to any software that I've
>> installed. Though now that I've runned Spybot it found the old DSO
>> exploit, so thanks for that. I don't even use IE (i'm using Opera).
>>> From what I've learned browsing in several sites port 80 and 443 are
>>> used by svchost.exe when one is operating a web server in a computer.
>> So I created a rule in Sygate to block inbound connections on both
>> port 80 and 443, all hosts, TCP remote ports, incoming traffic,
>> Generic Host Process for Win32 Services
>
>

> <snip>
>
> *Port 443 is used for secure web browser communication. Data transferred
> across such connections are highly resistant to eavesdropping and
> interception. Moreover, the identity of the remotely connected server can
> be verified with significant confidence. Web servers offering to accept
> and establish secure connections listen on this port for connections from
> web browsers desiring strong communication security.*
>
> *Once established, web browsers inform their users of these secured
> connections by displaying an icon — a padlock, an unbroken key, etc. — in
> the status region of their window.*
>
> *The "s" in "https" stands for "secure": Hyper Text Transfer Protocol,
> Secure. You may encounter other s-suffix protocols such as ftps or smtps.
> These, similarly, refer to secured-transport versions of the base
> protocol.*
>
> *In the case of https, whereas the default port used for standard non-
> secured "http" is port 80, browser use 443 to be the default port used by
> secure http.*
>
> *Some firewalls filter SSL or port 443 traffic. If this is the case, your
> browser will time out trying to access the SSL-protected areas of the IT-
> Solutions website, by timing out when you try to connect.*
>
> *related ports 80, 81, 82, 8080 and 8090*
>
> <snip>
>
>
>>*Still, sometimes I see in Connection Details svchost.exe CONNECTED to
>>remote port 80. Port 443 never appeared again. In Application Details
>>there isn't any considerable traffic outgoing or incoming in the
>>Generic Host Process for Win32 Services. In fact the only traffic
>>going on right now is in Opera and mIRC. So I guess there isn't any
>>reason to feel worried, even if the port 80 connection with
>>svchost.exe showed a few hours ago with a different IP adress from
>>mine leaves me a bit suspicious.*
>>
>>*If anyone has more opinions on this feel free to to add something in
>>this thread.*
>>
>
>
> *Well, you should not be blocking SVCHOST/Generic Host Process from
> communicating, because that's its job is to communicate on the LAN or WAN
> for the NT based O/S. So, it will lead to you not being able to access
> some legit sites when needed. It's the messenger for the O/S and should
> you kill the messenger just because it delivered the message? You should
> be trying to find out what's using the messenger and killing it.*

>
> *So, one day you let the messenger communicate for some reason, because*
> *you had to. What happened to all the other stuff you were killing the*
> *messenger for and you didn't know what it was using the messenger.*
>
> *The only time you should be killing the messenger (svchost.exe) is if it*
> *is NOT running out of Winnt or Windows \system32 directory for NT 4 and*
> *Win 2K or Win XP or 2K3.*
>
> *Duane :)*
>
>

I disagree with that. At times, svchost.exe will try to connect for no apparent reason, and I'll kill it. Furthermore, because I still use Plug-and-Play (for Windows Sound purposes) I simply block svchost when it tries to connect on TCP 1900. If a communication is remotely initiated, and I don't know why it's being remotely initiated, then I block it, even if it's svchost.exe. If some apps stop working then, then I'm that much the wiser about that particular remote IP address and what it has to do with my PC. I wouldn't say blocking svchost.exe from accessing the internet is killing the messenger, just blocking him from delivering his message.

--
William
If it don't work, hit it.
If it still doesn't work, kick it.
If it works after hitting it and kicking it, then it doesn't matter if hitting it or kicking it helped, what's important is it worked.