

Re: Firewall Setup...

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2004-04/0085.html>

From: Duane Arnold (*notme_at_notme.com*)

Date: 04/02/04

Date: Thu, 01 Apr 2004 23:44:55 GMT

"Global_Killa" <global_killa@hotmail.com> wrote in message
news:c4i5ml\$8bp\$1@newsg1.svr.pol.co.uk...

> *Hey all,*
> *I've been wondering for a while what svchost.exe application on my*
> *Windows XP is used for. I have to set a firewall rule for this application*
> *everytime I format my computer, and I don't really know what I should*
> *allow*
> *it to do.*
>
> *The programs location is C:\Windows\system32\svchost.exe. If I block this*
> *program from accessing the Internet, it seems to stop Internet activity.*
>

As you can see, blocking svchost.exe stops your machine from accessing the Internet. Svchost.exe is just the messenger for the O/S and other programs and provides the communication link between machines on the LAN or WAN, along with doing many many other tasks for the O/S. One of the functions of svchost.exe is to provide the communication plumbing for the connection. Yes, Trojan and spyware can use svchost.exe on their behalf too, just like the O/S uses svchost to communicate. Should one kill the messenger or should one try to find what's using the messenger and kill it?

<http://ask-leo.com/archives/000030.html>

If svchost.exe is making connections to unknown remote IP(s), then by all means, one should question why and try to find out what is requesting that svchost provide the connection.

You can find out by using Active Ports to see what remote IP(s) svchost.exe is connecting to, and you can use Process Explorer to look at what programs are using svchost.exe. Both of the utility programs are free (use Google).

If svchost.exe is not running out of the path below (system32), then it's a Trojan.

C:\Windows\system32\svchost.exe

comp.security.firewalls: Re: Firewall Setup...

Don't kill the messenger and try to find out what is using the messenger. :)

I don't stop svchost.exe (the messenger) from doing its job and let it run.

Duane :).