

Re: svchost.exe and the internet.....HELP!!

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2004-02/0491.html>

From: Luvly Jubly (*delat_at_vega.fsnet.co.uk*)

Date: 02/06/04

Date: Fri, 6 Feb 2004 17:13:33 -0000

Hi Neil,

Svchost uses Dcom on port 135 which in turn negotiates a NetBIOS session on your computer using port 137 for file sharing etc. The Blaster worm exploited this process for which Microsoft issued a critical patch.

You have done right to block its access from the internet as it was never intended for use over the internet (so I have I heard)

I use sygate to and if you create a advanced rule for svchost.exe .. to block all incoming/outgoing traffic on ports 135, 137, 139, from all ip addresses. if you do this you wont get any prompts when you log on as sygate will look at the advanced rule first and action it with out disturbing you.

Also create a packet filter log for it if you want to see how many or how often it is trying to communicate.

By it being blocked it will in no way affect your internet use downloading, browsing etc.

Hope this helps in as little detail as I have given

'In the land of the blind the one eyed man is King'

"Neil" <nruddiforth@hotmail.com> wrote in message
news:b33bd93c.0402060825.3dd039@posting.google.com...

> *Hi there*

>

> *I was wondering if someone could help me?*

>

> *A week ago, i installed broadband on my home computer (running Windows
> 2000). As soon as I was up and running I started getting this:*

>

> *"Svchost.exe generated an application error and will be closed by
> Windows. An error log is been genorated"*

>

> *It always happened a few minutes of been logged on, and it wouldnt let
> me disconnect my modem, use ctrl C to copy, and my contol panel went
> haywire (all the icons moved to the left hand side of the window).*

>

> *I did a bit of wading around, to find a few other people were having*

comp.security.firewalls: Re: svchost.exe and the internet.....HELP!!

- > *the same problem. So I took there advice (the best I could, I dont*
- > *really understand all the technical stuff), and did a complete windows*
- > *update via microsoft, service pack 4 etc, downloaded*
- > *Windows2000-KB823980-x86-ENU patch and ran that, downloaded Stinger*
- > *and MS Blast, and ran both of those (no MSblaster worm, but the*
- > *Stinger found one, which it got rid of), ran Spybot, and got rid of*
- > *all the Ad stuff and spyware.*
- >
- > *I also downloaded a Firewall program from Sygate, and installed that.*
- > *Now, im not getting the svchost error message anymore, but the Sygate*
- > *Firewall is telling me after a few minutes of been logged on, someone*
- > *is trying to access my svchost.exe! (every single time I log on)*
- >
- > *It gives me the option to allow it by clicking yes, or decline it by*
- > *clicking no. Ive been clicking no, but im worried that it might be*
- > *important for my internet connection to have my svchost accessed by my*
- > *service provider. Is this the case?*
- >
- > *Please help. I dont know much about this sort of thing, and im worried*
- > *I might be doing the wrong thing.*
- >
- > *Thanks for your time, I hope to hear from you all soon!*
- >
- > *Neil*