

Forum:[Hack Forums](#)

Thread: [Unknown computer trying to connect to svchost.exe and it isn't running](#)

Benjamin Franklin - *October 13, 2012, 8:06 am*

I was playing some minecraft, and comodo firewall came up with a warning "Unknown computer trying to access svchost.exe" I click block, and it came up again. I blocked it again. Comodo never came up with any other warnings. I stopped playing MC and looked through my tasks, and found that svchost.exe was not running. Is this a possible RAT? If so, how? I never downloading anything. Kingsoft AV, and MBAM found nothing. Does anyone know what's going on? Any help would be great. Thanks.

TeamPublicNull - *October 13, 2012, 8:16 am*

Hmm, it could be just Comodo overreacting. That has happened to me ALOT.

And I really don't know what to do either :/ As you have already scanned with MBAM and AV, and they found nothing, I am really out of ideas. You SHOULD be fine if Comodo blocked that connection, right? I think that there is no need to worry right now, because your Comodo blocked the connection :) But if something else happens, be sure to make a new post! :)

?Mind_?Control™ - *October 13, 2012, 9:35 am*

Comodo tends to "overreact" quite often. Nevertheless, it may be someone attempting to connect to your computer through a falsified svchost, so block it.

IF you think you're infected, here is what to do.

Infected? Here is what to do:

Firstly, you want to restart your computer and disconnect from the internet. Also, when I say disconnect, I mean turn off your router, just in case you ARE actually infected.

Look for the suspicious infected file and delete it.

Then, look through your process list, check to see if there are

any unusual processes running that are taking a lot of CPU power. If found, end the process tree.

If that doesn't work, open up Ccleaner and Disk Defragment and start cleaning up your PC.

Defragging usually helps in cases of files not opening up due to computer LAG.

If the problem persists, check your recent files, if nothing is there, run a system restore.

Be sure to make the system restore 2 days prior to when you think this problem began.

After restoring, repeat the above process. If the problem persists, PM Phyber on HF. He is a professional White Hat and knows a lot about computer security.

On the side, get AVG Anti-Virus Free 2012 Edition, it's the best out there at the moment.

If you know yourself, and somehow want to have a secondary protection besides your own mental capabilities, look for a good Anti-Virus.

Here are a few I can recommend:
AVG Anti-Virus Free 2012 Edition

AVG advances in catching infectious tools and Remote Administration Tools.

Avast! Home Edition

Avast! Home Edition is great for catching the average worm or standardized virus, but it lacks much in the field of Remote Administration Tools.

Malware Bytes Anti-Malware 2012

Malware Bytes Anti-Malware 2012 catches and is able to remove majority of malware found on standardized computers today.

Microsoft Security Essentials

Surprisingly, Microsoft Security Essentials is what I PERSONALLY use, at the moment. It's caught 2 "FUD" JDBs so far by simply running a deep scan. Written by Microsoft, they know Windows 7 the best, right?

Hope this helped. If it didn't, I do apologize. :(

Benjamin Franklin - October 13, 2012, 9:36 am

(Oct 13, 2012 08:16 AM)TeamPublicNull Wrote: [\[CITE\]](#) Hmm, it could be just Comodo overreacting. That has happened to me ALOT.

And I really don't know what to do either :/ As you have already scanned with MBAM and AV, and they found nothing, I am really out of ideas. You SHOULD be fine if Comodo blocked that connection, right? I think that there is no need to worry right now, because your Comodo blocked the connection :) But if something else happens, be sure to make a new post! :)

I was thinking the same thing, but since svchost isn't on the task list, I was worried. Everything is fine at the moment. No account's have been stolen. I'll keep my eye out on it. I will also look through the inbound and outbound connections to try to find anything fishy.

(Oct 13, 2012 09:35 AM)?Mind ?Control™ Wrote: [CITE](#) Comodo tends to "overreact" quite often. Nevertheless, it may be someone attempting to connect to your computer through a falsified svchost, so block it.

IF you think you're infected, here is what to do.

Infected? Here is what to do:

Firstly, you want to restart your computer and disconnect from the internet. Also, when I say disconnect, I mean turn off your router, just in case you ARE actually infected.

Look for the suspicious infected file and delete it.

Then, look through your process list, check to see if there are any unusual processes running that are taking a lot of CPU power. If found, end the process tree.

If that doesn't work, open up Ccleaner and Disk Defragment and start cleaning up you PC.

Defragging usually helps in cases of files not opening up due to computer LAG.

If the problem persists, check your recent files, if nothing is there, run a system restore.

Be sure to make the system restore 2 days prior to when you think this problem began.

After restoring, repeat the above process. If the problem persists, PM Phyber on HF. He is a professional White Hat and knows a lot about computer security.

On the side, get AVG Anti-Virus Free 2012 Edition, it's the best out there at the moment.

If you know yourself, and somehow want to have a secondary protection besides your own mental capabilities, look for a good Anti-Virus.

Here are a few I can recommnd:

[/list]

[*]AVG Anti-Virus Free 2012 Edition

AVG advances in catching infectious tools and Remote Administration Tools.

[*]Avast! Home Edition

Avast! Home Edition is great for catching the average worm or standardized virus, but it lacks much in the field of Remote Administration Tools.

[*]Malware Bytes Anti-Malware 2012

Malware Bytes Anti-Malware 2012 catches and is able to remove majority of malware found on standardized computers today.

[*]Microsoft Security Essentials

Suprisingly, Microsoft Security Essentials is what I PERSONALLY use, at the moment. It's

caught 2 "FUD" JDBs so far by simply running a deep scan. Written by Microsoft, they know Windows 7 the best, right?

Hope this helped. If it didn't, I do apologize. :(

I've known Phyber for awhile now. I PM'd him awhile back when I was infected with a keylogger.

?Mind_?Control™ - October 13, 2012, 9:46 am

Oh, alright.

Well if he was able to help you out, check with him again.

Benjamin Franklin - October 13, 2012, 9:50 am

(Oct 13, 2012 09:46 AM)?Mind_?Control™ Wrote: [\[CITE\]](#) Oh, alright.

Well if he was able to help you out, check with him again.

He helped me out a lot! I'll check in with him in a bit. I haven't spoken to him in awhile, though.

?Mind_?Control™ - October 13, 2012, 9:55 am

(Oct 13, 2012 09:50 AM)Annihilation Wrote: [\[CITE\]](#) He helped me out a lot! I'll check in with him in a bit. I haven't spoken to him in awhile, though.

That won't matter.

He is very eager to assist people.

Benjamin Franklin - October 13, 2012, 10:00 am

(Oct 13, 2012 09:55 AM)?Mind_?Control™ Wrote: [\[CITE\]](#) That won't matter.

He is very eager to assist people.

I know. I was just stating that out of random.

Pr?nce - October 13, 2012, 10:03 am

This happens to me quite often as well, I just block it and ignore it.

Freebooter - October 13, 2012, 12:44 pm

Svchost.exe always running if svchost.exe was not running Windows OS will not boot or if the svchost.exe was terminated Windows OS will shutdown without warning because svchost.exe host

services for Windows OS if you want to view all the services each Svchost.exe host click "Show processes from all users" button from the Task Manager and right click svchost.exe and select "Go to Services" to view the services hosted by svchost.exe the services mark with blue are the ones hosted by the svchost.exe there will be more than one svchost.exe running and each one will host different services you can pause the Task Manager update speed from View tab this will help you to view services hosted by each running instances of the svchost.exe also enable the "Command Line" column from the View tab this will help you to find out the folder path of the svchost.exe make sure svchost.exe located in C:\Windows\System32\svchost.exe or C:\Windows\SysWOW64\svchost.exe if the svchost.exe folder path is different than the default folder location than the Windows OS is infected by malware you should run a virus scanner also make sure the svchost.exe name is correct because sometimes malware will change the name of the svchost.exe to hide it self and about not allowing network connection for services hosted by svchost.exe this can cause network connection problem for example DHCP Client service could get block by firewall this means computer NIC will not be assign a dynamic IP address by the Router also Windows Update if block by firewall will not get new updates i don't know if the Comodo Firewall show you the name of the service hosted by svchost.exe if not it should show you the IP address of the network connection you can use foreign IP address to find out the who the IP address belongs to there is lots of IP address lookup websites google search "whois ip lookup" to find IP address lookup websites.

Benjamin Franklin - October 13, 2012, 3:22 pm

(Oct 13, 2012 12:44 PM)Freebooter Wrote: [\[CITE\]](#) Svchost.exe always running if svchost.exe was not running Windows OS will not boot or if the svchost.exe was terminated Windows OS will shutdown without warning because svchost.exe host services for Windows OS if you want to view all the services each Svchost.exe host click "Show processes from all users" button from the Task Manager and right click svchost.exe and select "Go to Services" to view the services hosted by svchost.exe the services mark with blue are the ones hosted by the svchost.exe there will be more than one svchost.exe running and each one will host different services you can pause the Task Manager update speed from View tab this will help you to view services hosted by each running instances of the svchost.exe also enable the "Command Line" column from the View tab this will help you to find out the folder path of the svchost.exe make sure svchost.exe located in C:\Windows\System32\svchost.exe or C:\Windows\SysWOW64\svchost.exe if the svchost.exe folder path is different than the default folder location than the Windows OS is infected by malware you should run a virus scanner also make sure the svchost.exe name is correct because sometimes malware will change the name of the svchost.exe to hide it self and about not allowing network connection for services hosted by svchost.exe this can cause network connection problem for example DHCP Client service could get block by firewall this means computer NIC will not be assign a dynamic IP address by the Router also Windows Update if block by firewall will not get new updates i don't know if the Comodo Firewall show you the name of the service hosted by svchost.exe if not it should show you the IP address of the network connection you can use foreign IP address to find out the who the IP address belongs to there is lots of IP address lookup websites google search "whois ip lookup" to find IP address lookup websites.

This problem has been resolved. Thanks.