

Forum: [Hack Forums](#)

Thread: [So many svchost?](#)

1tap - October 11, 2017, 5:54 am

I need a checkup, svchost is running under my user and there is so many of them?

<https://i.gyazo.com/2a323b308f83b7c66892213dcf59d232.png>

ON win10

Biker BoyZ - October 11, 2017, 5:55 am

I have so many on win 10 as well. i think its normal.

1tap - October 11, 2017, 5:55 am

(Oct 11, 2017 05:55 AM)Biker BoyZ Wrote: [\[CITE\]](#) I have so many on win 10 as well. i think its normal.

Running under your user aswell?

5chn4pp - October 11, 2017, 5:57 am

Its common but I can also check anyways.

Please download [Farbar Recovery Scan Tool](#) and save it to your Desktop.

Note: You need to run the version compatible with your system. If you are not sure which version applies to your system download both of them and try to run them. Only one of them will run on your system, that will be the right version.

Right click to run as administrator. When the tool opens click Yes to disclaimer.

Press Scan button.

It will produce logs called FRST.txt and Addition.txt in the same directory the tool is run from.

Please copy and paste the logs back here.

1tap - October 11, 2017, 6:02 am

FRST <https://pastebin.com/Y8D0NDbP>

Addition <https://pastebin.com/F6WbY21h>

Biker BoyZ - October 11, 2017, 6:03 am

(Oct 11, 2017 06:02 AM)1tap Wrote: [\[CITE\]](#) FRST <https://pastebin.com/Y8D0NDbP>

Addition <https://pastebin.com/F6WbY21h>

you run my sort of software too. steam and vulkan.

1tap - October 11, 2017, 6:04 am

(Oct 11, 2017 06:03 AM)Biker BoyZ Wrote: [\[CITE\]](#) you run my sort of software too. steam and vulkan.

Wth is vulkan? lmao

Biker BoyZ - October 11, 2017, 6:04 am

(Oct 11, 2017 06:04 AM)1tap Wrote: [\[CITE\]](#) Wth is vulkan? Imao just a graphics platform.

BITW - October 11, 2017, 6:07 am

Is your Resource usage normal as well? Can you check?

5chn4pp - October 11, 2017, 6:10 am

Download [fixlist.txt](#) file and save it to the Desktop.

NOTE: It's important that both files, FRST/FRST64 and fixlist.txt are in the same location or the fix will not work.

NOTICE: This script was written specifically for this user, for use on that particular machine. Running this on another machine may cause damage to your operating system

Run FRST/FRST64 and press the Fix button just once and wait.
If for some reason the tool needs a restart, please make sure you let the system restart normally.
After that let the tool complete its run.
When finished FRST will generate a log on the Desktop (Fixlog.txt). Please post it to your reply.

Please download [RogueKiller](#) and save it to your desktop. Quit all running programs.

Right-click on the program and select Run as Administrator to start and when prompted allow it to run.

Read and accept the EULA (End User License Agreement)

Click Scan to scan the system.

When the scan completes select "Report", a log will open. Close the program > Don't Fix anything!

Post the contents of the log in your next reply.

1tap - October 11, 2017, 6:14 am

(Oct 11, 2017 06:07 AM)RootLayer_Sales Wrote: [\[CITE\]](#) Is your Resource usage normal as well? Can you check?

Looks fine

<https://i.gyazo.com/151c09e02d7aefaca15dc21f55221552.png>

BITW - October 11, 2017, 6:17 am

(Oct 11, 2017 06:14 AM)1tap Wrote: [\[CITE\]](#) Looks fine

<https://i.gyazo.com/151c09e02d7aefaca15dc21f55221552.png>

Then i think it is fine. :)

5chn4pp - October 11, 2017, 6:23 am

(Oct 11, 2017 06:17 AM)RootLayer_Sales Wrote: [\[CITE\]](#) Then i think it is fine. :)

"Lets ignore the malware since we don't see it on task manager, must be nothing xddd"

Can we stop assuming and actually use our brains here?????

BITW - October 11, 2017, 6:26 am

(Oct 11, 2017 06:23 AM)Bromo-DragonFLY Wrote: [\[CITE\]](#) "Lets ignore the malware since we don't see it on task manager, must be nothing xddd"

Can we stop assuming and actually use our brains here?????

He should also use a good security provider like an antivirus provider + malware protection.

Otherwise, We can't tell 100% okay.

It seems fine but not guaranteed.

5chn4pp - October 11, 2017, 6:28 am

(Oct 11, 2017 06:26 AM)RootLayer_Sales Wrote: [\[CITE\]](#) He should also use a good security provider like an antivirus provider + malware protection.

Otherwise, We can't tell 100% okay.

It seems fine but not guaranteed.

You cant read logs but I can.

I say he is infected, you say he isn't and hes fine.

Why does nobody use logic, lets trust the guy with only 40 posts in the whitehat section, don't worry about that guy with like 3000.

BITW - October 11, 2017, 6:32 am

(Oct 11, 2017 06:28 AM)Bromo-DragonFLY Wrote: [\[CITE\]](#) You cant read logs but I can.

I say he is infected, you say he isn't and hes fine.

Why does nobody use logic, lets trust the guy with only 40 posts in the whitehat section, don't worry about that guy with like 3000.

I think it is fine but did not tell i confirmed.

You are an expert & You just help that guy via teamviewer or something to end the story. He needs help as he is confused.

I just asked OP to see if there is any abnormal resource usage on Task manager. i did not ask to see if any unknown process present in task manager.

5chn4pp - October 11, 2017, 6:35 am

(Oct 11, 2017 06:32 AM)RootLayer_Sales Wrote: [\[CITE\]](#) I think it is fine but did not tell i confirmed.

You are an expert & You just help that guy via teamviewer or something to end the story. He needs help as he is confused.

No he doesn't, he simply needs to follow post #10, if he was confused then it would be because you posted, could've just not posted and made this mess.

1tap - October 11, 2017, 6:41 am

(Oct 11, 2017 06:28 AM)Bromo-DragonFLY Wrote: [\[CITE\]](#) You cant read logs but I can.

I say he is infected, you say he isn't and hes fine.

Why does nobody use logic, lets trust the guy with only 40 posts in the whitehat section, don't worry about that guy with like 3000.

Im infected??:(

Also running roguekiller RN, taking a while.

5chn4pp - October 11, 2017, 6:44 am

(Oct 11, 2017 06:41 AM)1tap Wrote: [\[CITE\]](#) Im infected??:(

Also running roguekiller RN, taking a while.

Ofcourse you are, that's why I posted a fix, when other people interfere with my cleaning process it screws it up.

1tap - October 11, 2017, 6:46 am

(Oct 11, 2017 06:44 AM)Bromo-DragonFLY Wrote: [\[CITE\]](#) Ofcourse you are, that's why I posted a fix, when other people interfere with my cleaning process it screws it up.

What am i infected with?

BITW - October 11, 2017, 6:46 am

(Oct 11, 2017 06:35 AM)Bromo-DragonFLY Wrote: [\[CITE\]](#) No he doesn't, he simply needs to follow post #10, if he was confused then it would be because you posted, could've just not posted and made this mess.

I know what i should ask and post.

I just asked for resource usage and said that is fine. Did i say he is not infected?

You started the mess actually by taking this discussion thread a Debating place.

We should close our personal debating here to keep the environment clean.

1tap - October 11, 2017, 6:47 am

Roguekiller <https://pastebin.com/1JgF0Uuf>

fixthing <https://pastebin.com/pC8qnmiU>

If you are talking about this, thats an actual cheat for a game.

Code FirewallRules: [{EBB1EEFA-12D9-4E23-8E5B-DE07C1491FA5}] => (Allow)

E:\chodmeme\jfhhknovdgde.exe

FirewallRules: [{EA5B0038-C68C-44D1-944B-EE5C602EBE13}] => (Allow)

E:\chodmeme\jfhhknovdgde.exe

FirewallRules: [{175ADE7D-2ADE-4333-A4DC-98C166EEB1BC}] => (Allow)

E:\chodmeme\jfhhknovdgde.exe

FirewallRules: [{240C72BE-13D9-4930-8E44-F2BDFF5DFD2F}] => (Allow)

E:\chodmeme\jfhhknovdgde.exe

5chn4pp - October 11, 2017, 6:51 am

(Oct 11, 2017 06:46 AM)1tap Wrote: [\[CITE\]](#) What am i infected with?

I don't know, looks like a loader.

(Oct 11, 2017 06:46 AM)RootLayer_Sales Wrote: [\[CITE\]](#) I know what i should ask and post.

I just asked for resource usage and said that is fine. Did i say he is not infected?

You started the mess actually by taking this discussion thread a Debating place.

We should close our personal debating here to keep the environment clean.
You said "Then i think it is fine" which gave the impression to him that there was no malware, without looking at logs. You cant rely on task manager alone with malware.

(Oct 11, 2017 06:47 AM)1tap Wrote: [\[CITE\]](#) Roguekiller <https://pastebin.com/1JgF0Uuf> fixthing <https://pastebin.com/pC8qnmiU>
Make roguekiller delete everything called "PUP.Gen1" in the registry tab, after that your computer is clean.

(Oct 11, 2017 06:47 AM)1tap Wrote: [\[CITE\]](#) If you are talking about this, thats an actual cheat for a game.
Not that, still removed it since it shouldn't be in firewall.

Autowall - October 11, 2017, 6:53 am

(Oct 11, 2017 06:26 AM)RootLayer_Sales Wrote: [\[CITE\]](#) He should also use a good security provider like an antivirus provider + malware protection.

Otherwise, We can't tell 100% okay.

It seems fine but not guaranteed.
Another retard who thinks he knows what he is doing but in reaity thinks having an AV is the safest thing and wont allow you to get infected. Dont ever post in this section again. Bromo is trained in this and handles this shit in a professional manner to help remove the infection completely.

lucalollion - October 11, 2017, 6:55 am

it never happened to me it could easily be that there are just a lot of processes open.

BITW - October 11, 2017, 7:00 am

(Oct 11, 2017 06:51 AM)Bromo-DragonFLY Wrote: [\[CITE\]](#) I don't know, looks like a loader.

You said "Then i think it is fine" which gave the impression to him that there was no malware, without looking at logs. You cant rely on task manager alone with malware.

Make roguekiller delete everything called "PUP.Gen1" in the registry tab, after that your computer is clean.

Not that, still removed it since it shouldn't be in firewall.
There might be a misunderstanding here? Why he would just believe me as many are replying here and giving ideas?

Also, I just asked for resource usage and meant the resource usage fine. Did i say OP was totally fine from all ends and ask OP to close the thread? Did i?

if you have misunderstood me, Now you should understand what i meant and let's finish this really useless topic. OP has no issue with my post as he understood already what i meant and following the instructions given.

After all, It is a discussion thread and i have rights to post what i thought important. After the end of the day, It is OP, who will decide what to do.

If this was a misunderstanding, Just close it.

Wish you guys a best of luck

(Oct 11, 2017 06:53 AM)Autowall Wrote: [\[CITE\]](#) Another retard who thinks he knows what he is doing but in reality thinks having an AV is the safest thing and won't allow you to get infected. Don't ever post in this section again. Bromo is trained in this and handles this shit in a professional manner to help remove the infection completely.

If you guys only know how to misunderstand simple words, what can I say?

I should be jailed because I just asked for resource usage and said that (Resource usage) was fine.

Yeah, I will try to post here daily. Thanks for the advice.

?

1tap - October 11, 2017, 7:05 am

Thanks for the help, Bromo.

Closing this now.