

Forum: [Hack Forums](#)

Thread: [Need help cleaning up](#)

y389525 - February 8, 2019, 8:17 pm

I ran a malwarebytes scan as I felt something was wrong with my PC sure enough there was and I had quarantined them already, here are the results of the scan.

Will be running a RKill scan and FRST scan. Have quarantined and removed the threats in MBAM & Rkill. Help will be greatly appreciated. Did the scans with my internet off if that needs to be stated.

MBAM: <https://hastebin.com/etojubuziy.sql>

RKill(quick scan): <https://hastebin.com/wodaviruka.cs>

RKill(standard scan): <https://hastebin.com/uzifaguzuk.m>

FRST.txt: <https://hastebin.com/mafemicaxu.md>

Addition.txt: <https://hastebin.com/sugefofovo.makefile>

5chn4pp - February 9, 2019, 10:02 am

(Feb 8, 2019 09:17 PM)y389525 Wrote: [\[CITE\]](#) I ran a malwarebytes scan as I felt something was wrong with my PC sure enough there was and I had quarantined them already, here are the results of the scan.

Will be running a RKill scan and FRST scan. Have quarantined and removed the threats in MBAM & Rkill. Help will be greatly appreciated. Did the scans with my internet off if that needs to be stated.

MBAM: <https://hastebin.com/etojubuziy.sql>

RKill(quick scan): <https://hastebin.com/wodaviruka.cs>

RKill(standard scan): <https://hastebin.com/uzifaguzuk.m>

FRST.txt: <https://hastebin.com/mafemicaxu.md>

Addition.txt: <https://hastebin.com/sugefofovo.makefile>

I really doubt that wmimgmt.exe was malicious, because I have seen another user with the exact same file 6 years ago. However just keep it deleted since I also can't find a good use for it.

You currently have TaskbarNoNotification set to 1, this means you don't get notifications. Do you want me to change that or leave it?

I also need you to upload the following files to virustotal.com and post the result here:

C:\Users\Family\sidchg64.exe

C:\Users\Family\AppData\Local\Temp\450f2c3.exe

C:\Users\Family\AppData\Local\Temp\500b5214.dll

C:\Users\Family\AppData\Local\Temp\97388.exe

C:\Users\Family\AppData\Local\Temp\9d2e9795.dll

y389525 - February 9, 2019, 10:12 pm

(Feb 9, 2019 11:02 AM)5chn4pp Wrote: [\[CITE\]](#) You currently have TaskbarNoNotification set to 1, this means you don't get notifications. Do you want me to change that or leave it?

I also need you to upload the following files to virustotal.com and post the result here:

C:\Users\Family\sidchg64.exe
C:\Users\Family\AppData\Local\Temp\450f2c3.exe
C:\Users\Family\AppData\Local\Temp\500b5214.dll
C:\Users\Family\AppData\Local\Temp\97388.exe
C:\Users\Family\AppData\Local\Temp\9d2e9795.dll

I don't understand what you mean by TaskbarNoNotification set to 1 what is this related to?

sidchg64.exe:

<https://www.virustotal.com/#/file/e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855/detection>

450f2c3.exe:

<https://www.virustotal.com/#/file/b7ed5f7117aabf581995410d0b324a74177fd1256304ad4230f0e585f831c85b/detection>

500b5214.dll:

<https://www.virustotal.com/#/file/adcd46db13d1005c9188cf2bb146fac19b65ecd4c0c35e86ae92229e09f73cb3/detection>

97388.exe:

<https://www.virustotal.com/#/file/3d6738d0ba078a233901015e897b7cfc33973870a98991dd4d54f4a0e5edf835/detection>

9d2e9795.dll:

<https://www.virustotal.com/#/file/5966f6e7dff9cf1f335fd4eca5023533a10380cd36a806c6192576f0c39a1a03/detection>

5chn4pp - February 10, 2019, 7:42 am

(Feb 9, 2019 11:12 PM)y389525 Wrote: [\[CITE\]](#) I don't understand what you mean by TaskbarNoNotification set to 1 what is this related to?

sidchg64.exe:

<https://www.virustotal.com/#/file/e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855/detection>

450f2c3.exe:

<https://www.virustotal.com/#/file/b7ed5f7117aabf581995410d0b324a74177fd1256304ad4230f0e585f831c85b/detection>

500b5214.dll:

<https://www.virustotal.com/#/file/adcd46db13d1005c9188cf2bb146fac19b65ecd4c0c35e86ae92229e09f73cb3/detection>

97388.exe:

<https://www.virustotal.com/#/file/3d6738d0ba078a233901015e897b7cfc33973870a98991dd4d54f4a0e5edf835/detection>

9d2e9795.dll:

<https://www.virustotal.com/#/file/5966f6e7dff9cf1f335fd4eca5023533a10380cd36a806c6192576f0c39a1a03/detection>

Its a policy setting in windows itself, it makes you unable to get Desktop notifications, this can either be set by you or malicious software.

Go ahead and delete all of those files from that folder.

y389525 - February 18, 2019, 3:57 am

(Feb 10, 2019 08:42 AM)5chn4pp Wrote: [\[CITE\]](#) Its a policy setting in windows itself, it makes you unable to get Desktop notifications, this can either be set by you or malicious software.

Go ahead and delete all of those files from that folder.

Ok I have just deleted the files, sorry disappeared for a week cause I was in hospital, noticed two

programs that appeared without installing it. Highlighted em. So what do I do next?

<https://imgur.com/a/9yRpnO3>

5chn4pp - February 18, 2019, 4:46 am

(Feb 18, 2019 04:57 AM)y389525 Wrote: [\[CITE\]](#) Ok I have just deleted the files, sorry disappeared for a week cause I was in hospital, noticed two programs that appeared without installing it. Highlighted em. So what do I do next?

<https://imgur.com/a/9yRpnO3>

Those can just be uninstalled from the control panel, you can do that if you want to.

Also, I really need an answer to the disabled notification thing.

y389525 - February 18, 2019, 6:44 am

(Feb 18, 2019 05:46 AM)5chn4pp Wrote: [\[CITE\]](#) Those can just be uninstalled from the control panel, you can do that if you want to.

Also, I really need an answer to the disabled notification thing.

Well, I am not really sure as to what it does but by all means if it causes problems to the system I would like it back on.

5chn4pp - February 18, 2019, 1:00 pm

(Feb 18, 2019 07:44 AM)y389525 Wrote: [\[CITE\]](#) Well, I am not really sure as to what it does but by all means if it causes problems to the system I would like it back on.

Alright, make sure you save all of your work before running this. Also make sure you have an internet connection because I need to upload a file to virustotal.com

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

NOTE: It's important that both files, FRST.exe/FRST64.exe 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 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 copy and paste the log to [pastebin.com](#) and post the url back here.

y389525 - February 19, 2019, 3:45 am

I get this message when I want to save it what do I do?

<https://imgur.com/a/A5tn9wK>

5chn4pp - February 19, 2019, 9:35 am

(Feb 19, 2019 04:45 AM)y389525 Wrote: [\[CITE\]](#) I get this message when I want to save it what do I do?

<https://imgur.com/a/A5tn9wK>

That message is fine, ignore it.

However I see that the file is named fixlist.txt.txt, it should just be fixlist.txt otherwise it wont work.

y389525 - February 19, 2019, 11:30 pm

Alright it is done.

<https://pastebin.com/uqAU9xQh>

5chn4pp - February 20, 2019, 12:04 am

(Feb 20, 2019 12:30 AM)y389525 Wrote: [\[CITE\]](#) Alright it is done.

<https://pastebin.com/uqAU9xQh>

Looks good, your computer should be clean now.

If you want me to do an extra check, you can run FRST and post fresh logs, but its not required.

y389525 - February 23, 2019, 3:54 am

(Feb 20, 2019 01:04 AM)5chn4pp Wrote: [\[CITE\]](#) Looks good, your computer should be clean now.

If you want me to do an extra check, you can run FRST and post fresh logs, but its not required.

If I need help I'll let you know thanks for your time:)