

Forum:[Hack Forums](#)

Thread: [Might have something sketchy on my PC](#)

Dopeish - July 19, 2017, 8:22 am

FRST: <https://pastebin.com/Bf2EtrZJ>

Addition: <https://pastebin.com/NTkM4ZVP>

The screen flashes some times, keys get fucked up for some reason and starts opening programs instead of doing what they should.

5chn4pp - July 19, 2017, 9:02 am

You have a rat, and there is a driver issue with your mouse and keyboard.

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.

Dopeish - July 19, 2017, 9:08 am

(Jul 19, 2017 09:02 AM)Bromo-DragonFLY Wrote: [\[CITE\]](#) You have a rat, and there is a driver issue with your mouse and keyboard.

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.

<https://pastebin.com/BGdneL8D>

The dlhost was my own rat I tested just to see if it were working some time ago, I'm pretty sure of.

5chn4pp - July 19, 2017, 9:13 am

There was also another rat, please upload this folder to <https://share.riseup.net/> and post the link here:

C:\Users\granz\Desktop\19.07.2017_18.05.21.zip

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.

Dopeish - July 19, 2017, 10:05 am

<https://share.riseup.net/#7vekul8egO303FIRTkFtiw>

<https://pastebin.com/9DuVJa3z>

5chn4pp - July 19, 2017, 10:43 am

These files are password stealers and a bitcoin stealer, I recommend you change all of your passwords.

Now to the driver, please open device manager and post a screenshot of the drivers.

Dopeish - July 19, 2017, 6:35 pm

(Jul 19, 2017 10:43 AM)Bromo-DragonFLY Wrote: [\[CITE\]](#) These files are password stealers and a bitcoin stealer, I recommend you change all of your passwords.

Now to the driver, please open device manager and post a screenshot of the drivers. Are they gone now?

<https://i.imgur.com/1VW2BCo.png>

5chn4pp - July 19, 2017, 6:54 pm

Yeah I deleted it, do you see a "Trusted Platform Module 2.0" device in device manager? Try to enable it.

Dopeish - July 19, 2017, 7:25 pm

(Jul 19, 2017 06:54 PM)Bromo-DragonFLY Wrote: [\[CITE\]](#) Yeah I deleted it, do you see a "Trusted Platform Module 2.0" device in device manager? Try to enable it.

Can't find.

5chn4pp - July 19, 2017, 7:51 pm

(Jul 19, 2017 07:25 PM)Dopeish Wrote: [\[CITE\]](#) Can't find.

Then its fine, the malware is gone and that driver wont be important if its not in device manager, if you have any questions please ask, otherwise have a great day ?

Dopeish - July 19, 2017, 8:05 pm

(Jul 19, 2017 07:51 PM)Bromo-DragonFLY Wrote: [\[CITE\]](#) Then its fine, the malware is gone and that

driver wont be important if its not in device manager, if you have any questions please ask, otherwise have a great day ?

Screen still does flash at some times. Just for some ms but still, annoying. What could it be? Thanks for your help and effort so far though.

5chn4pp - July 20, 2017, 4:55 am

Open cmd as administrator and execute this command:

Code sfc /scannow
Post the results here.

Also check your event viewer logs, are there anything in those?

Dopeish - July 20, 2017, 5:36 am

(Jul 20, 2017 04:55 AM)Bromo-DragonFLY Wrote: [\[CITE\]](#) Open cmd as administrator and execute this command:

Code sfc /scannow
Post the results here.

Also check your event viewer logs, are there anything in those?

<https://i.imgur.com/cEjMXzk.png>

Nothing weird in event viewer of what i can find.

5chn4pp - July 20, 2017, 5:46 am

If the screen is flashing, it could be the gpu. You can try to stress test your gpu, what gpu do you have?

Dopeish - July 20, 2017, 6:24 am

(Jul 20, 2017 05:46 AM)Bromo-DragonFLY Wrote: [\[CITE\]](#) If the screen is flashing, it could be the gpu. You can try to stress test your gpu, what gpu do you have?
980Ti from last year.

5chn4pp - July 20, 2017, 6:49 am

You can run FurMark to test your gpu:

<http://www.ozone3d.net/benchmarks/fur/>

If your gpu crashes during the test, then your gpu is likely the problem.

Dopeish - July 20, 2017, 2:47 pm

(Jul 20, 2017 06:49 AM)Bromo-DragonFLY Wrote: [\[CITE\]](#) You can run FurMark to test your gpu:

<http://www.ozone3d.net/benchmarks/fur/>

If your gpu crashes during the test, then your gpu is likely the problem.

Will try, thanks for the effort so far.