

Forum:[Hack Forums](#)

Thread: [Strange thing happening to my friends computer](#)

Crusher - January 21, 2018, 10:46 am

Let me be quick on this.

First - His computer started making more noise than usual.

Second - After his computer shut down (by itself), he put 4 WRONG characters for his startup password and went to eat. After roughly 10 minutes when he came back, field was blank (those 4 characters were gone).

He asked me if I can find anyone willing to help, check this up, and if it is rat, he would like to know who is doing that to him (trace location). If needed your service can be payed.

PM me or post in thread if you can help. Thanks

AsSaSs@iN - January 21, 2018, 12:47 pm

I'm AsSaSs@iN, I'm a member of the HackForums Malware Removal Team (MRT) and will be assisting you throughout this thread. Before we start just take a second to read through these few requests - these are to ensure we can help you quickly and safely: Only use this thread for help. Please don't create multiple threads, accounts, PM me or post on other forums - if you do just let me know.

Only follow my guidance.

Don't run tools I haven't asked you to run. If you do just let me know so I can take that into consideration when viewing logs.

DO NOT install any other software while we are attempting to clean your machine. It can get quite confusing especially if you are downloading questionable tools.

Please be prompt in responding. I'll do my best to do so. If >48hrs has passed, please either PM me or ask "Are you there, I still need help" in this thread.

Please stick with me until I give you the 'All Clean'. I'll help you cleanup quickly and offer some tips to make you more secure and get your system running faster.

Your malware related tools will be removed. I don't support the tools often distributed on these forums. Scanners will generally remove these - I take no responsibility for any malicious software that is lost.

I (nor does the forum) support pirated software.

If you don't understand something, don't be afraid to ask - I'm here to help. ?

You'll notice the logs are pretty big and you won't be able to post a reply containing it all. Please use ONLY either: <https://hastebin.com> - here you can upload the .txt file directly. <- I prefer this.

<http://pasted.co/> - here you can set a password if you wish to protect your data. Just PM me the password.

And paste the link to the logs in your reply. Post each log separately (each with a separate link). If you're a new member and can't paste links you can fool the forums system by removing the beginning of the link.

e.g.If you can't post this: <https://hastebin.com/raw/epaduvuyic>

Post: I used hastebin, here is the ending /raw/epaduvuyic

If I request you to post an image please use a service like <https://imgur.com>

Let's get to it! (p.s. Call me assass for short!)

Malwarebytes - Clean ModeDownload and install the free version of [Malwarebytes](#)

Note: If you have Malwarebytes already installed, you don't need to install it again. Simply start from the next bullet point

Once Malwarebytes is installed, launch it and let it update his database. You might have to click on the little arrow by Scan Status in the middle right pane for it to do so

Once the database update is complete, click on the Scan tab, then select the Threat Scan button and click on Start Scan

Let the scan run, the time required to complete the scan depends of your system and computer specs

Once the scan is complete, make sure that the first checkbox at the top is checked (which will automatically check every detected item), then click on the Quarantine Selected buttonIf it asks you to restart your computer to complete the removal, do so

Click on Export Summary after the deletion (in the bottom-left corner) and select Copy to Clipboard. Paste the content in your next reply

RogueKiller

Download the right version of [RogueKiller](#) for your Windows version (32 or 64-bit)

Once done, move the executable file to your Desktop, right-click on it and select Run as Administrator (for Windows Vista, 7, 8, 8.1 and 10 users)

Click on the Start Scan button in the right panel, which will bring you to another tab, and click on it

again (this time it'll be in the bottom right corner)

Wait for the scan to complete

On completion, the results will be displayed. Click on the Open Report button in the bottom left corner, followed by the Open TXT button (also in the bottom left corner)

This will open the report in Notepad. Copy/paste its content in your next reply

Please read the guide I constructed here: <https://hackforums.net/showthread.php?tid=5772641>

Post the logs in THIS THREAD

Crusher - January 21, 2018, 1:11 pm

But if we remove the virus we can't trace location of attacker? Are these even signs of infected computer? Thanks

AsSaSs@iN - January 21, 2018, 10:50 pm

You put the thread prefix 'checkup'. Meaning you want a checkup. I won't help trace the location.

satoshin33 - January 22, 2018, 3:16 am

Maybe the keyboard is defect and is making some ghost commands.

Crusher - January 22, 2018, 8:50 am

(Jan 21, 2018 11:50 PM)AsSaSs@iN Wrote: [\[CITE\]](#) You put the thread prefix 'checkup'. Meaning you want a checkup. I won't help trace the location.

Do you perhaps know anyone that is willing to do? Sorry but I didn't know which prefix to use, since we first have to check up if it's even infected.

Super - January 23, 2018, 7:20 am

Hi Crusher,

I'm happy to help you track down the hacker. However, please note that this is normally only possible if you're infected with a RAT or a type of malware that "phones home".

Let's start off with an FRST scan, that way I can find the infection without removing it, allowing us to take a sample of the malware.

Download FRST here: <https://www.bleepingcomputer.com/download/farbar-recovery-scan-tool>

Run it as administrator and click "Scan".

Wait a few minutes for the scan to complete, then post the two logs it generates (FRST.txt and Additional.txt) into <https://hastebin.co> and share the link with me here.

Let me know if you have any questions ?

Dynamo

dg738967 - *January 23, 2018, 12:05 pm*

same thing here with me too..