

Forum:[Hack Forums](#)

Thread: [Business Computer Compromised](#)

Techie - January 29, 2019, 2:34 pm

Hey everyone, i'm in need of some help here.

2 days ago some "Microsoft Technicians" called my mom and sadly she fell for it while using the computer from her store. It's a small business, she works there with my father, but there's a lot of information along with some programs they use to keep their finances in order in this computer that they need.

According to her, they asked her to open Team Viewer and it seems they were chatting for like 2 hours, so guess they had enough time to do whatever the fuck they wanted. She ended up opening her bank account after they closed the Team Viewer connection because they told her to do a certain payment for their services, but no harm was done, since at this point she started realizing that it was probably a scam. When my mom first called me i told them to shutdown any internet connection and to immediately turn the computer off. Any ideas on how they should proceed now? Any way to recover the computer and its Data?

Let me know if you need any other information.

5chn4pp - January 29, 2019, 2:36 pm

(Jan 29, 2019 03:34 PM)Rohac Wrote: [\[CITE\]](#) -

Do this on the computer and I can see if they did anything:

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, do not change any settings.

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 to [pastebin.com](#) and post the url back here.

Techie - January 29, 2019, 2:38 pm

(Jan 29, 2019 03:36 PM)5chn4pp Wrote: [\[CITE\]](#) Do this on the computer and I can see if they did anything:

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, do not change any settings.

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 to [pastebin.com](#) and post the url back here.

Is it safe to turn the computer on? They said the computer would be blocked after being turned on again.

5chn4pp - January 29, 2019, 2:39 pm

(Jan 29, 2019 03:38 PM)Rohac Wrote: [\[CITE\]](#) Is it safe to turn the computer on? They said the computer would be blocked after being turned on again.

Just download FRST64.exe on a USB and use that to transfer the file, it should be fine as long as no internet connection is made.

But I cannot be 100% sure until I actually view the logs.

Aura - January 30, 2019, 4:46 pm

You can run FRST from Windows Recovery mode if needed. Just put it on a USB Flash Drive, access the Recovery mode, open the command prompt and launch X:\FRST64.exe (X:\FRST.exe if it's 32-bit). X:\ being whatever letter will be assigned to your flash drive. It'll save a file called FRST.txt on the USB. Copy/paste/attach/whatever it here.

k2hawk - January 30, 2019, 9:44 pm

Any credential info stored in the computer?

I recommend change all passwords by the another, (not infected) computer for websites which your family used from the computer.