

Forum:[Hack Forums](#)

Thread: [Microsoft Defender for Endpoint is unable to detect my threat](#)

SIM-5022267 - January 30, 2025, 1:35 am

I am dealing with chinese APT hacker group, or black hats, and they are able to get into my network, windows PC, phones and more.

I installed Microsoft Defender for Endpoint, and applied a lot of policies and everything possible, scanned all and nothing detected.

How can this be? This stuff is more advanced than stuxnet.

Tha Sneak - January 30, 2025, 1:37 am

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 or to pastebin with the link.

SIM-5022267 - January 30, 2025, 1:56 am

(Jan 30, 2025 02:37 AM)Tha Sneak Wrote: [\[CITE\]](#) 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 or to pastebin with the link.

Hey, thanks for this. But I asked for help many times on other places as well, and they all ask for FARBAR scan, which came back clean. FARBAR is not able to detect whatever sophistication attack I am dealing with.

Tha Sneak - January 30, 2025, 2:00 am

(Jan 30, 2025 02:56 AM)SIM-5022267 Wrote: [\[CITE\]](#) Hey, thanks for this. But I asked for help many times on other places as well, and they all ask for FARBAR scan, which came back clean. FARBAR is not able to detect whatever sophistication attack I am dealing with.
Where else did you post at?

SIM-5022267 - January 30, 2025, 2:01 am

(Jan 30, 2025 03:00 AM)Tha Sneak Wrote: [\[CITE\]](#) Where else did you post at?
Some guy on other forums, like malwarebytes, or bleepingcomputers, malwaretips, they ask to scan and send the same .txt files.

found nothing.

I am dealing with something very sophisticated, RAT, spyware. Can see and remotely control my system.

Tha Sneak - January 30, 2025, 2:08 am

(Jan 30, 2025 03:01 AM)SIM-5022267 Wrote: [\[CITE\]](#) Some guy on other forums, like malwarebytes, or bleepingcomputers, malwaretips, they ask to scan and send the same .txt files.

found nothing.

I am dealing with something very sophisticated, RAT, spyware. Can see and remotely control my system.

I see you referred to Stuxnet, which is an older worm. I'm familiar with it and I've personally removed it from several computers.

What you describe sounds like a worm, however if I have nothing to analyze there's not much I can offer except to recommend to abandon all files and reformat.

The only thing that could survive that is a UEFI rootkit, which in this case wouldn't spread through a network.

SIM-5022267 - January 30, 2025, 2:18 am

(Jan 30, 2025 03:08 AM)Tha Sneak Wrote: [\[CITE\]](#) I see you referred to Stuxnet, which is an older worm. I'm familiar with it and I've personally removed it from several computers.

What you describe sounds like a worm, however if I have nothing to analyze there's not much I can offer except to recommend to abandon all files and reformat.

The only thing that could survive that is a UEFI rootkit, which in this case wouldn't spread through a network.

Also, how can you explain this?

I did abandon all devices and even the network, I purchased a new laptop, with a new internet called 5G hotspot device on-the-go, and brought it with me to a coffee shop to use. Somehow, I got hacked there, and some indian guy kept taking photos of me and following me.

Do you think the APT group could have tracked my location via. my iPhone in pocket, and paid some indian guy to follow me to the coffee shop and setup a hack? The 5G hotspot device kept saying a wifi device is trying to connect to network but I don't see any devices connected, and sources say it's a sign of infiltration.

My amazon account got hacked in 2023 june, and some indian dudes were behind it. The indian dudes then hand the call over to some asian guy in Alberta. That asian guy is their boss.

DramaKing - January 30, 2025, 4:46 am

(Jan 30, 2025 03:18 AM)SIM-5022267 Wrote: [CITE](#) Also, how can you explain this?

I did abandon all devices and even the network, I purchased a new laptop, with a new internet called 5G hotspot device on-the-go, and brought it with me to a coffee shop to use. Somehow, I got hacked there, and some indian guy kept taking photos of me and following me.

Do you think the APT group could have tracked my location via. my iPhone in pocket, and paid some indian guy to follow me to the coffee shop and setup a hack? The 5G hotspot device kept saying a wifi device is trying to connect to network but I don't see any devices connected, and sources say it's a sign of infiltration.

My amazon account got hacked in 2023 june, and some indian dudes were behind it. The indian dudes then hand the call over to some asian guy in Alberta. That asian guy is their boss.

Easy. Drugs or mental illness. I suppose you received an email saying something like "We are Chinese APT and have hacked you." You're not giving any other connection. So someone was following you. Doesn't mean that you were hacked. The WiFi device could have been your own computer.

If you have such deep-seated paranoia, maybe you should live off the grid. Just don't waste our time.