

Forum:[Hack Forums](#)

Thread: [CPU miner?](#)

Brain Dead - December 13, 2017, 3:32 pm

Hi, my sibling was on my PC on her email and she got opened a link from a phishing email ever since my cpu has been running at 99% but when i open task manager it goes back to normal, can someone help me analyse this and remove it please?

AsSaSs@iN - December 14, 2017, 2:46 am

Hey Brain Dead,

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!)

~

MalwarebytesDownload and install the free version of [Malwarebytes](#)

NOTE: If you already have Malwarebytes installed, just open up Malwarebytes and check for any updates available.

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

Allow Malwarebytes to scan completely.

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 button. If 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

~~

Farbar Recovery Scan Tool (FRST) - Scan mode

Follow the instructions below to download and execute a scan on your system with FRST, and provide the logs in your next reply. Download the right version of FRST for your system: [FRST 32-bit](#)

[FRST 64-bit](#)

NOTE: Only the right version will run on your system, the other will throw an error message. So if you don't know what your system's version is, simply download both of them, and the one that works is the one you should be using.

Move the executable (FRST.exe or FRST64.exe) on your Desktop

Right-click on the executable and select Run as Administrator (for Windows Vista, 7, 8, 8.1 and 10 users)

Accept the disclaimer by clicking on Yes, and FRST will then do a back-up of your Registry which should take a few seconds

Make sure the Addition.txt box is checked

Click on the Scan button

On completion, two message box will open, saying that the results were saved to FRST.txt and Addition.txt, then open two Notepad files

Copy and paste the content of both FRST.txt and Addition.txt in your next reply

Please post the logs from MBAM and FRST.

Brain Dead - December 14, 2017, 5:40 am

<https://hastebin.com/magoseguwi.tex> - Malware bytes

<https://hastebin.com/etarawimar.tex> - FRST

Thanks for the help

AsSaSs@iN - December 14, 2017, 7:03 am

Quote:Thanks for the help

Happy to help ?

You have a fair few PUP (potentially unwanted programs) entries that were just partially removed, in particular:Conduit

Mindspark

Interstat

I recommend you follow the instructions here from beginning to end to reset Chrome:

<https://forums.malwarebytes.com/topic/214325-chrome-secure-preferences-detection-always-comes-back/>

Quote:Trojan.BitCoinMiner, C:\PROGRAMDATA\SYSTEMFILES\SYSTEMKERNELL.EXE, Quarantined, [71], [435821],1.0.3489

You were right.

I'll respond to your log in the morning ?

Brain Dead - December 14, 2017, 9:20 am

(Dec 14, 2017 08:03 AM)AsSaSs@iN Wrote: [\[CITE\]](#) Happy to help ?

You have a fair few PUP (potentially unwanted programs) entries that were just partially removed, in particular:Conduit

Mindspark

Interstat

I recommend you follow the instructions here from beginning to end to reset Chrome:

<https://forums.malwarebytes.com/topic/214325-chrome-secure-preferences-detection-always-comes-back/>

You were right.

I'll respond to your log in the morning ?

Nice, I look forward to it, thanks again.

AsSaSs@iN - December 14, 2017, 10:11 pm

Sorry for the delay, let's get to it!

You're actually the second person in 2 weeks thats connected to the ESEA client and are complaining of this issue... I'm not sure if this is a coincidence or not...

https://www.theregister.co.uk/2013/11/20/esea_gaming_bitcoin_fine/ (I know this is an old post - food for thought) do you have the installer? I wouldn't mind getting a hold of it to try and do some analysis on the file.

Do you want to keep ESEA?

Do you have Process Hacker installed just to keep an eye on the issue?

It looks like you have a few VPNs installed, did you do this yourself? Are you using them all?

BetterNetVPN

[censored]

TheOpenVPN

Hide.me VPN

OkayFreedomVPN

Farbar Recovery Scan Tool (FRST) - Fix

Follow the instructions below to execute a fix on your system using FRST, and provide the log in

your next reply. Open Notepad and copy/paste the following into notepad:

```
CloseProcesses:  
CreateRestorePoint:  
C:\PROGRAMDATA\SYSTEMFILES  
GroupPolicy: Restriction <==== ATTENTION  
C:\ProgramData\EInjector64.exe  
C:\ProgramData\righ.dll  
EmptyTemp:
```

Save the file as fixlist.txt, and save it on your Desktop (or wherever your FRST.exe/FRST64.exe executable is located)

Right-click on the FRST executable and select Run as Administrator (for Windows Vista, 7, 8, 8.1 and 10 users)

Click on the Fix button

On completion, a message will come up saying that the fix has been completed and it'll open a log in Notepad

Copy and paste its 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

~~

AdwCleaner - Fix ModeDownload [AdwCleaner](#) and move it to your Desktop

Right-click on AdwCleaner.exe and select Run as Administrator (for Windows Vista, 7, 8, 8.1 and 10 users)

Accept the EULA (I accept), then click on Scan

Let the scan complete. Once it's done, make sure that every item listed in the different tabs is checked and click on the Clean button. This will kill all the active processes

Once the cleaning process is complete, AdwCleaner will ask to restart your computer, do it

After the restart, a log will open when logging in. Please copy/paste the content of that log in your next reply

In your next reply please include:Log from FRST

RogueKiller Log

adwCleaner Log

Let me know how your system is running.

Fresh logs from FRST (please include additions.txt this time)

Brain Dead - December 15, 2017, 6:15 am

Hi, I believe the problem came from something of recent, my sister said she opened an "amazon" link from an email so I copied the link address and pasted into a vm browser and the real address was a shady website with some random long string at the end so I guess it was a down-loader for the stub or something, I still have the link if you'd like to do some analysis on it.

I don't really use them VPN's anymore so I can remove them and as for ESEA I don't use that anymore either.

fixlog.txt - <https://hastebin.com/apodenokey.php>

roguekiller - <https://hastebin.com/uhexofumay.md>

adware - <https://hastebin.com/ijutijupim.tex>

Ok so I open task manager and it shows the CPU is running at 100 percent but then it notices that task manager is open so it shows utilization

<https://gyazo.com/7905a57db42545118c26cf7228c7b982> <--- upon opening task manager

<https://gyazo.com/63e034dbb1e8b5d4a39f9f0a83c936ef> <---- after keeping it open

I'm not sure if this is normal but I don't think it is, process hacker shows the real utilization at 95%

addition.txt - <https://hastebin.com/metumohawo.tex>

Thanks again.

AsSaSs@iN - December 15, 2017, 7:46 am

Send me the link in PM ?

Can you post a fresh version of the FRST.txt too from FRST.exe

EDIT: We still have some stuff to do, but it's almost 3am here and I'm wiped. I'll see ya tomorrow.

Brain Dead - December 15, 2017, 6:08 pm

Fresh FRST - <https://hastebin.com/eceqobeqap.tex>

AsSaSs@iN - December 19, 2017, 4:18 pm

Sorry for the delay,

Can you remove the VPNs and ESEA like we discussed earlier?

While you're there, uninstall this old version of Java

Java 8 Update 121 (HKLM-x32\...\{26A24AE4-039D-4CA4-87B4-2F32180121F0}) (Version: 8.0.1210.13 - Oracle Corporation)

CPU Spike: This is normal when you first open task manager - it happens to most people.

It would be good if you could scan this with VirusTotal and post the link to the report here.

C:\Users\miche\Desktop\CrySearch32.exe

~~

Farbar Recovery Scan Tool (FRST) - Fix

Follow the instructions below to execute a fix on your system using FRST, and provide the log in your next reply. Open Notepad and copy/paste the following into notepad:

CloseProcesses:

CreateRestorePoint:

Shortcut: C:\Users\miche\AppData\Roaming\Microsoft\Windows\Network Shortcuts\My Web Sites on MSN\target.lnk -> hxxp://www.msnusers.co

AlternateDataStreams: C:\Users\miche\Desktop\2K+ Email Pass Gaming

Combo.txt:com.dropbox.attributes [168]

AlternateDataStreams: C:\Users\miche\Desktop\Gaming-MiX

15_03_16_15_43_33.txt:com.dropbox.attributes [168]

AlternateDataStreams: C:\Users\miche\Desktop\NetGhost_Proxies_2017.04.26

03.13.09.txt:com.dropbox.attributes [168]

AlternateDataStreams: C:\Users\miche\Desktop\Origin Combos.txt:com.dropbox.attributes [168]

EmptyTemp:

Save the file as fixlist.txt, and save it on your Desktop (or wherever your FRST.exe/FRST64.exe executable is located)

Right-click on the FRST executable and select Run as Administrator (for Windows Vista, 7, 8, 8.1 and 10 users)

Click on the Fix button

On completion, a message will come up saying that the fix has been completed and it'll open a log in Notepad

Copy and paste its content in your next reply

Post the log from FRST and VirusTotal.

Let me know how you go with the uninstalls.

How is everything running?