

Forum:[Hack Forums](#)

Thread: [FRST Help - Buddy is at 100% CPU usage.](#)

Proposed - April 20, 2024, 2:58 am

I got a buddy i think is infected. I can attach the FRST and Addition but there is something in there that's spammed.

CustomCLSID:

HKU\S-1-5-21-3466471569-2789148286-862051560-1001_Classes\CLSID\{CAFEEFAC-0015-0000-0009-ABCEFFEDCBA}\InprocServer32 -> H:\jdk\bin\jp2iexp.dll (Oracle America, Inc. ->) *Like 50+ lines of this in addition.

Trying to find why his CPU is so high at random times. Any help is greatly appreciated.

FRST + Addition

<https://file.io/hqa7gkYBD9qq>

DramaKing - April 20, 2024, 4:03 am

(Apr 20, 2024 02:58 AM)Proposed Wrote: [\[CITE\]](#) I got a buddy i think is infected. I can attach the FRST and Addition but there is something in there that's spammed.

CustomCLSID:

HKU\S-1-5-21-3466471569-2789148286-862051560-1001_Classes\CLSID\{CAFEEFAC-0015-0000-0009-ABCEFFEDCBA}\InprocServer32 -> H:\jdk\bin\jp2iexp.dll (Oracle America, Inc. ->) *Like 50+ lines of this in addition.

Trying to find why his CPU is so high at random times. Any help is greatly appreciated.

FRST

<https://jmp.sh/s/n55bzP6GvIv3GQXpQRg9>

Addition

<https://jmp.sh/s/uzQrEILn4qBi6wRTfYK1>

First of all, I don't know what any of that is supposed to mean. Second, remove McAfee. Never have more than one antivirus installed.

Bastille - April 20, 2024, 10:46 am

Hello,

Don't have enough time today but I'll take a look tomorrow if nobody checks it before.

Thanks for the FRST reports

Proposed - April 20, 2024, 11:32 am

(Apr 20, 2024 10:46 AM)Yseurk Wrote: [\[CITE\]](#) Hello,

Don't have enough time today but I'll take a look tomorrow if nobody checks it before.

Thanks for the FRST reports

Would be greatly appreciated! Maybe he's just got too much running be he had like 440 items I quarantined on Maleware Bytes.

Binance - April 20, 2024, 3:45 pm

Bippity Boppity, your friends machine has someone mining XMR on his property.

EDIT: can you share what he downloaded with qbittorrent on 30 03 2024?

Burger - April 20, 2024, 8:00 pm

(Apr 20, 2024 03:45 PM)Kalidrex Wrote: [\[CITE\]](#) Bippity Boppity, your friends machine has someone mining XMR on his property.

EDIT: can you share what he downloaded with qbittorrent on 30 03 2024?

Love these comments.

I would recommend only having 1 Antivirus on your PC, either Esset or Malwarebytes are my go to, Check startups and also check registry, remove anything that's unordinary!

Hackers - April 21, 2024, 4:31 am

(Apr 20, 2024 02:58 AM)Proposed Wrote: [\[CITE\]](#) I got a buddy i think is infected. I can attach the FRST and Addition but there is something in there that's spammed.

CustomCLSID:

HKU\S-1-5-21-3466471569-2789148286-862051560-1001_Classes\CLSID\{CAFEEFAC-0015-0000-0009-ABCDEFFEDCBA}\InprocServer32 -> H:\jdk\bin\jp2iexp.dll (Oracle America, Inc. ->) *Like 50+ lines of this in addition.

Trying to find why his CPU is so high at random times. Any help is greatly appreciated.

FRST

<https://jmp.sh/s/n55bzP6Gvlv3GQXpQRg9>

Addition

<https://jmp.sh/s/uzQrEILn4qBi6wRTfYK1>

your jump share images are 404s now

I would definitely make sure to get a proper AV & remove this

happygonutty - April 21, 2024, 2:33 pm

OP should run an AV scan and exclude all the folders that needs to be excluded. Try to upload the DLL at VirusTotal or something similar for a start.

Bastille - April 21, 2024, 5:39 pm

Files not available anymore, let me know when you re-upload them

banonkiel - April 21, 2024, 6:30 pm

He definitely got infected with something.

I would recommend for starters a fresh win installation.

but if he can't pinpoint exactly what download he made started this whole fiasco, then a clean start would be better.

Other than that, from @Kalidrex, I'm assuming your friend downloaded something (via torrent) that started this.

So ye, a fresh start and pick your sources carefully, especially for cracked programs/games/etc (basically any executable)

I believe there's a megathread on r/Piracy and couple of other websites that list all trustworthy(ish) platforms for your needs.

Edit: I remember couple of years ago, a friend PC had similar problem like this.

His solution instead of all what I just mentioned was a CPU control application (can't remember its name top of my head)

Whatever infected his PC would attach itself to a running process and start mining, he waited for it to attach to something, then he would limit the CPU usage to 0.01% lmao.

He always kept an eye on CPU/Network usage and made sure it didn't do anything other than try to mine so he was satisfied with his workaround.

SHADE™ - April 27, 2024, 6:57 pm

Disconnect from the internet: Before starting the malware removal process, disconnect the laptop from the internet to prevent the malware from spreading or communicating with its command and control servers.

Boot into Safe Mode: Restart the laptop and boot into Safe Mode. This will limit the number of running processes and help isolate the malware. To enter Safe Mode, press the F key during startup and select "Safe Mode with Networking."

Update your antivirus software: Ensure that your antivirus software is up-to-date. If you don't have antivirus software installed, download and install a reputable one.

Run a full system scan: Use the antivirus software to perform a full system scan. This will help identify and remove any known malware infections.

Remove suspicious files and programs: If the antivirus software identifies any suspicious files or programs, remove them. Be cautious when removing files, as some may be critical system files.

Check for hidden files and folders: Malware often hides in hidden files and folders. To view hidden files and folders in Windows, go to "Control Panel" > "Appearance and Personalization" > "Folder Options" > "View" and select "Show hidden files, folders, and drives."

Check system files: Malware can infect system files, causing them to become corrupt or malfunction. To check system files for integrity, use the System File Checker (SFC) tool in Windows. Open the command prompt as an administrator and type "sfc /scannow" and press Enter.

Check startup programs: Malware often runs at startup, making it difficult to remove. Check the startup programs by opening the Task Manager (Ctrl+Shift+Esc) and selecting the "Startup" tab. Disable any suspicious or unnecessary startup programs.

Check the registry: Malware can modify the Windows registry, causing system instability or malicious behavior. Be cautious when modifying the registry, as incorrect changes can cause system issues. Use a reputable registry cleaner tool to scan and repair any registry issues.

Install a reputable anti-malware tool: In addition to antivirus software, install a reputable anti-malware tool to provide an additional layer of protection. Run a full system scan with the anti-malware tool to identify and remove any remaining malware.

Change passwords: If the malware infection was severe, it may be necessary to change passwords

for online accounts, email, and other sensitive information.

Proposed - April 30, 2024, 5:47 pm

(Apr 21, 2024 05:39 PM)Yseurk Wrote: [\[CITE\]](#) Files not available anymore, let me know when you re-upload them

A little far behind but just reuploaded on a new website. Hopefully this stays.

<https://file.io/hqa7gkYBD9qq>

(Apr 21, 2024 06:30 PM)banonkiel Wrote: [\[CITE\]](#) He definitely got infected with something.

I would recommend for starters a fresh win installation.

but if he can't pinpoint exactly what download he made started this whole fiasco, then a clean start would be better.

Other than that, from @Kalidrex, I'm assuming your friend downloaded something (via torrent) that started this.

So ye, a fresh start and pick your sources carefully, especially for cracked programs/games/etc (basically any executable)

I believe there's a megathread on r/Piracy and couple of other websites that list all trustworthy(ish) platforms for your needs.

Edit: I remember couple of years ago, a friend PC had similar problem like this.

His solution instead of all what I just mentioned was a CPU control application (can't remember its name top of my head)

Whatever infected his PC would attach itself to a running process and start mining, he waited for it to attach to something, then he would limit the CPU usage to 0.01% lmao.

He always kept an eye on CPU/Network usage and made sure it didn't do anything other than try to mine so he was satisfied with his workaround.

Appreciate this input! Ill look into this!