

Forum:[Hack Forums](#)

Thread: [How To Remove A Silent BTC Miner From PC?](#)

Juxtapoze - April 9, 2023, 2:48 pm

My 13 y/o little brother seems to likely have a silent crypto miner on his PC, his GPU usage is at 90% at all times I am just trying to help him out. His father just passed away unexpectedly about a month ago and video games are one of the ways that he has fun with his friends and he hasn't been able to do that lately so I am trying to help him out, any help would be much appreciated. Also, I apologize if I posted this in the wrong place.

ObsidianMD - April 9, 2023, 3:16 pm

Just run Malware bytes or any reputable AV and if for some reason it can't detect then just backup the data and reinstall the operating system.

Sand Ferret - April 9, 2023, 3:23 pm

As above, just run an AV or reinstall.

Reinstall would be best.

Dread.Reaper - April 9, 2023, 4:20 pm

(Apr 9, 2023 03:23 PM)Sand Ferret Wrote: [\[CITE\]](#) As above, just run an AV or reinstall.

Reinstall would be best.

Re-installs such a pain in the ass though, a good AV can usually nuke it.

@OP Take a close look at the advanced options of Task manager for GPU useage and identify the process thats killing it so badly is a good start.

DramaKing - April 10, 2023, 6:16 am

Take a good look at the AV for any tampering, check for sketchy downloads, check Task Manager to see what process is using that much of the GPU, and run netstat -ano in Command Prompt. The miner needs an established connection to a pool, so finding a connection could identify it.

Sand Ferret - April 10, 2023, 6:20 am

(Apr 9, 2023 04:20 PM)Dread.Reaper Wrote: [\[CITE\]](#) Re-installs such a pain in the ass though, a good AV can usually nuke it.

@OP Take a close look at the advanced options of Task manager for GPU useage and identify the process thats killing it so badly is a good start.

Yeah true, I just like being on the safe side.

Plus, I do love a clean install of Windows lol.

Dread.Reaper - April 10, 2023, 6:25 am

(Apr 10, 2023 06:20 AM)Sand Ferret Wrote: [\[CITE\]](#) Yeah true, I just like being on the safe side.

Plus, I do love a clean install of Windows lol.

Cant argue that one.

Pokes his 5 year old ASUS ROG laptop with its still base factory install

Ph4n70M Phr34K - April 10, 2023, 6:27 am

(Apr 9, 2023 04:20 PM)Dread.Reaper Wrote: [\[CITE\]](#) Re-installs such a pain in the ass though, a good AV can usually nuke it.

I wouldn't say that. For me it takes 20-30 minutes to reinstall OS + all applications and during this time i mostly watch a progress bar.

(Apr 9, 2023 02:48 PM)fishmixxx Wrote: [\[CITE\]](#) My 13 y/o little brother seems to likely have a silent crypto miner on his PC, his GPU usage is at 90% at all times I am just trying to help him out. His father just passed away unexpectedly about a month ago and video games are one of the ways that he has fun with his friends and he hasn't been able to do that lately so I am trying to help him out, any help would be much appreciated. Also, I apologize if I posted this in the wrong place.

- Check task manager to see which process is using GPU.
- You may use Autoruns(<https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns>) and uncheck everything you don't recognize or anything that is not "verified".
- Check windows defender exclusion list.
- Check task scheduler and common startup directories and registry entries.

Dread.Reaper - April 10, 2023, 6:34 am

(Apr 10, 2023 06:27 AM)Ph4n70M Phr34K Wrote: [\[CITE\]](#) I wouldn't say that. For me it takes 20-30 minutes to reinstall OS + all applications and during this time i mostly watch a progress bar.

- Check task manager to see which process is using GPU.
 - You may use Autoruns(<https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns>) and uncheck everything you don't recognize or anything that is not "verified".
 - Check windows defender exclusion list.
- Best thing MS did in a long ass time was buy out Sysinternals.

metheslayer4 - April 10, 2023, 12:49 pm

Hmm...

- 1.) Identify high GPU usage processes:
 - a. Open Task Manager by pressing Ctrl + Shift + Esc.
 - b. Click on the "Performance" tab and select "GPU" from the left panel.
 - c. Click on the "Processes" tab and sort by the "GPU" column to find processes with high GPU usage.
 - d. Take note of any unfamiliar processes consuming significant GPU resources.
- 2.) Investigate suspicious processes:
 - a. Right-click on the suspicious process in Task Manager and select "Open file location."
 - b. Research the process name and file location online to determine if it's legitimate or potentially malicious.
- 3.) Run a malware scan:
 - a. Download and install Malwarebytes.
 - b. Update virus definitions to the latest.
 - c. Perform a full scan and remove any detected threats.
- 4.) Check startup programs:
 - a. In Task Manager, click on the "Startup" tab.
 - b. Look for suspicious programs or programs related to the identified high GPU usage processes.
 - c. Right-click on any suspicious or unnecessary programs and select "Disable."
- 5.) Uninstall suspicious applications:
 - a. Open Control Panel and click on "Uninstall a program" or "Programs and Features."

- b. Sort the list by the "Installed On" column to find recently installed applications.
 - c. Uninstall any suspicious or unwanted applications by right-clicking on them and selecting "Uninstall."
- 6.) Remove associated files and folders:
- a. Go to the file location of the suspicious process identified in step 2.
 - b. Delete any files and folders related to the suspicious process.
 - c. Use the search function in File Explorer to look for other files or folders with similar names and delete them as well.
- 7.) Update GPU driver:
- a. Determine the make and model of your brother's graphics card (e.g., NVIDIA GeForce GTX 1060).
 - b. Visit the GPU manufacturer's website (e.g., NVIDIA or AMD) and locate the latest drivers for the specific graphics card model.
 - c. Download and install the latest drivers, then restart the PC.

SIM-5300886 - April 10, 2023, 4:40 pm

I can connect on TeamViewer to help you out if you like with malware removal. Good luck OP.

cyberroots90 - April 10, 2023, 4:56 pm

use malware scanner or a good antivirus as from thousands of files i cant find if there is any thing u are looking for