New computer threat: Drive-by Crypto-Miners

- *Is your computer lagging or freezing?*
- *Is the CPU (Central Processing Unit) or GPU (Graphics card Processing Unit) in your device suddenly working harder than usual?*
- *Is the fan is going crazy for seemingly no reason?*
- *Is your device overheating?*
- *Is your battery quickly depleting?*
- *Is your electricity usage abnormally high?*

These might be signs that someone is using your computer to "mine" for cryptocurrency using much, if not all, of the capacity of your CPU (Central Processing Unit) and GPU (Graphics Processing Unit).

You would have heard of digital or crypto currencies such as Bitcoin, Monero, etc. If you don't know what these are, see more information here (take note of the "Mining" section): https://en.wikipedia.org/wiki/Cryptocurrency. For a good video that explains how cryptocurrencies and their block chains work, see http://www.bbc.com/news/av/technology-43026143/bitcoin-explained-how-do-cryptocurrencies-work

Anyone can manufacture digital coins using a process called "mining". Mining just a single coin requires a massive amount of CPU power – far beyond the capability of a single PC, tablet, or smartphone. *In fact in Iceland, for example, electricity use for Bitcoin mining data centres is likely to exceed that of all Iceland's homes.*

In late 2017, a company called Coinhive launched a service that could mine for a digital currency known as *Monero* directly within a web browser. A miner using this service could utilise the power of millions of PCs, tablets and smartphones, and generate valuable crypto-coins for him/herself. This is done without your knowledge or consent. It is technically not malware and not illegal, and there are many web sites employing this service to make money.

Since then there are a number of similar services being offered.

These invasive services utilise JavaScript and work on all modern browsers on all devices. If you visit a web site that utilises one, the Javascript for the service may be installed **without your knowledge. Y**our device's CPU (Central Processing Unit) and/or GPU (Graphics Processing Unit) processing capability is hijacked by the miner. Some of these services can steal 100% of your CPU/GPU power, alternatively by a process called "throttling", use a smaller percentage so you don't notice its presence as easily. Furthermore, the script can continue to run even when your browser is closed because it creates a hidden browser window that stays operative.

This mining script can easily be embedded in many web sites, even some Australian Government web sites have been hacked.

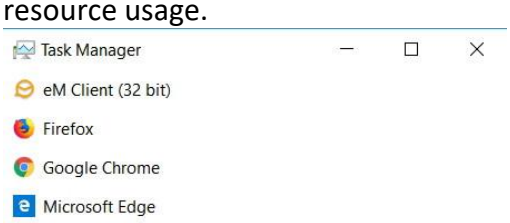
The only indication that you have this crypto-miner hijack is that your CPU and/or GPU usage increases and you may experience slow responses from your device. *Your device is now generating income for a digital miner somewhere.* This can significantly increase your electricity usage, and shorten the life of your device.

How to determine if you may have a digital miner active on your *Windows computer*

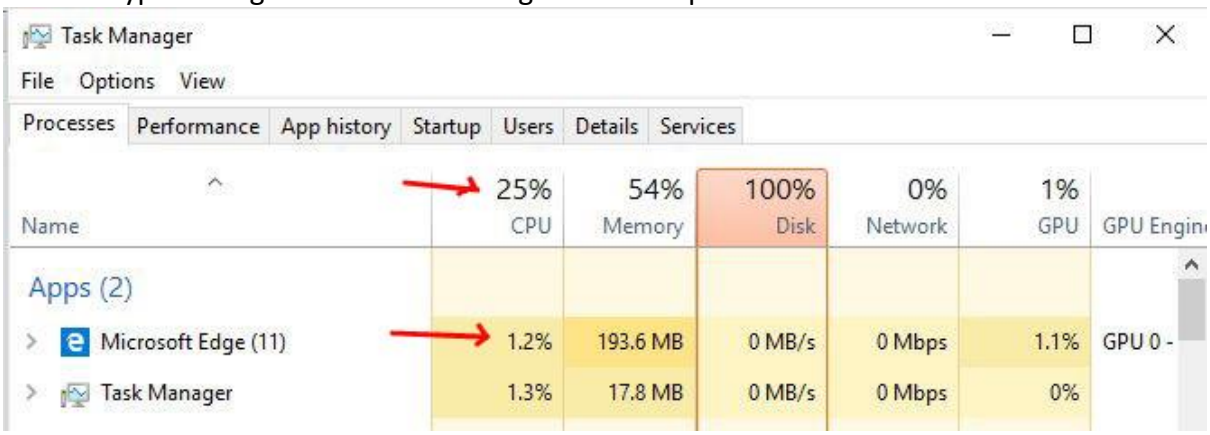
The first indication is that your device becomes very slow and unresponsive, particularly when a browser is or has been open.

You can see what is using your CPU or GPU (Graphics Processing Unit) in a Windows utility called *Task Manager*.

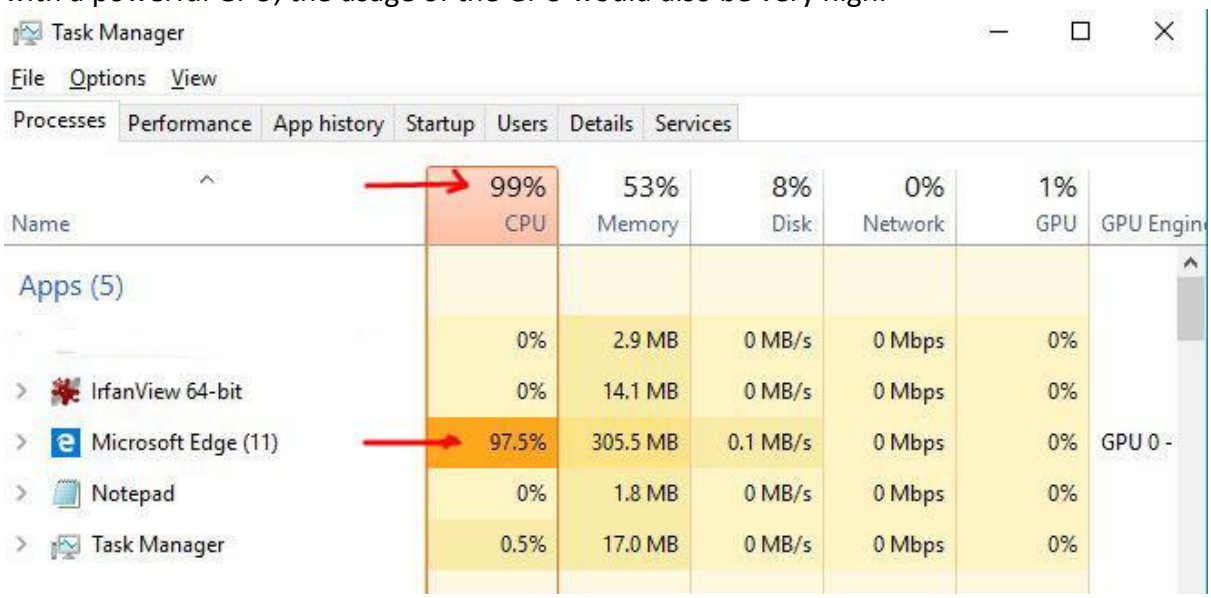
To start *Task Manager*, **right** click the Windows Start button and click *Task Manager*. When *Task Manager* opens, click on the *More details* at the bottom to display the system resource usage.



This is a typical usage with Microsoft Edge browser open but idle



If you have visited a page containing a Crypto-Miner, the CPU/GPU percentage will be very high, or 100%. In this case, with a Crypto-miner running, Edge is consuming 97.5% of the CPU, with a total CPU usage of 99%. In the following example, the computer does not have a good GPU so the Crypto-miner is not using it. If the miner was running on a computer with a powerful GPU, the usage of the GPU would also be very high.



To stop the Crypto-Miner, close all the tabs in your browser and restart the computer. Then have another look at your CPU/GPU usage – it should be back to normal. Note: just closing the browser may not stop it - you need to restart as well because later versions of these data miners can continue running even if you close the browser - they set up an invisible browser windows so they can continue to operate.

But if you again visit a page in your browser containing a Crypto-Miner the CPU/GPU usage will skyrocket again.

How to determine if you may have a digital miner active on your Smart-phone or Tablet

The main indicators are: degrading of the device's performance, and rapid battery depletion. Over time this can cause wear & tear of the device and shorten its battery life.

How to stop drive-by Crypto-Miners

Windows computers

Malwarebytes Premium and Kaspersky are two security programs that remove Crypto-miners. Microsoft security and other vendors of security products may follow over time.

Meanwhile, there are other effective options that are free:

Option 1. Install and run *Anti-WebMiner*

This is the safest and most effective option. It involves downloading a zip file containing the *Anti-WebMiner* program then running it once to add a list of crypto-mining web sites to the Windows "Hosts" file. This prevents any browser or any other application on the computer accessing the crypto-mining sites.

The list needs to be updated periodically which you do by simply running the program again. Alternatively, if you want to try something a bit more complicated, you can get the program to check for updates every day, when you login, or when the computer starts, by adding a task to the *Windows Task Scheduler.*

For details on how to install and use Anti-WebMiner, click here…

Option 2. Install and use Opera browser

The free *Opera* browser has built in protection against Drive-by Crypto-Miners. Opera can be downloaded from http://www.opera.com/

Option 3. Install *Adblock Plus* extension in Microsoft Edge, Firefox or Google Chrome, then add the "Nocoin filter list" to its list of filters

For more information see https://adblockplus.org/
Note: This does not work with Internet Explorer

For details on how to install *Adblock Plus* and how to add the *Nocoin filter list* to Adblock's lists – click here….

Option 4. For Firefox or Google Chrome only, install the *No Coin* extension

*Note: The **No Coin extension**, and the **Nocoin filter list associated with Adblock** are two different entities.*

For details on how to install the *No Coin* extension in Firefox and Chrome – click here...

Smartphones & Tablets

Be careful selecting an app claiming to stop crypto-mining. Some of them actually cause crypto-mining to occur. **Opera** browser does prevent crypto-miners on these devices, but the latest version for Android cannot be recommended because Opera insert their own ads and the browser is quite unfriendly. The following apps are safe:

Android

Free option: Install Firefox browser app (NOT Firefox Focus), then install the *No Coin* Firefox Extension. This will block crypto-miners but ONLY when you use Firefox browser**.**

Paid option: Install the Adguard app. It will protect all browsers on your device from crypto-miners. https://adguard.com/en/adguard-android/overview.html

For details – click here…

iOS

Install the app called *1blocker* and activate it. It will protect you from crypto-miners, but only when you use Safari browser.

For details, click here...