H E A D Q U A R T E R S
CYBERSPACE SECURITY GROUP
COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS SERVICE
ARMED FORCES OF THE PHILIPPINES
Camp General Emilio Aguinaldo, Quezon City

CSG4 08 April 2020

SUBJECT: **Daily Cyber Awareness Bulletin**

TO: **Commander, CEISSAFP**
P o s t
Attn: AC of CEISS for Operation, C3

1. Reference: Approved CSG STL dtd 07 April 2020 Subj: Daily Cyber Awareness Bulletin.

2. Per above reference, attached is the daily cyber awareness bulletin for uploading to AFP Website.

3. For information and reference.

NESTOR C CASPILLO JR
LCDR PN
Group Commander

CoinMiner is a type of malicious software that abuses computer resources (such as CPU and, most recently, GPU) in order to mine digital currency such as Bitcoin or Monero by performing complicated mathematical calculations. These funds are directly transferred to malicious actors' wallets over the internet. While cybercriminals profit from this activity, victims have to suffer from lag, errors, system crashes, overheating issues, as well as increased electricity bills. To make matters worse, the Coin Miner virus can also be used as a means to install other malware on the host machine.

CoinMiner removal steps

Updated anti-virus utility will block the threat before it settles on the system, so make sure you install reliable security software before it gets onto your computer without your approval and starts mining cryptocurrency for your money. According to some users[6], Windows Defender and another third-party software did not help them remove CoinMiner virus. In that case, you may run the scan with SpyHunter 5, Malwarebytes, or similar malware removal software. Reimage will help you fix virus damage.

In case the crypto-coin miner infiltrated your PC system together with another Trojan or backdoor, restart the computer in Safe Mode and run a full scan with your anti-virus to find hidden trojan components.

In case you are dealing with a browser-based infection, regular CoinMiner removal steps might not be effective. During the operation of your PC, a multitude of files are created on your system to access them quickly, and these files can be used by malicious programs as well – in this case, cryptocurrency mining.

Therefore, you need to make sure you delete the following from your web browsers:

- Temporary files from websites
- History
- Download History

https://www.2-spyware.com/remove-win32-coinminer.html

CoinMiner found in third-party Zoom download

Doug Olenick

The bad news for Zoom keeps coming rolling in with Trend Micro researchers finding CoinMiner being bundled with a legitimate installer of the video conferencing software.

The good news is the installer, Zoom installer version 4.4.0.0, is not from the company's official download center, but likely from a fraudulent third-party store, Trend Micro reported. However, it does install a working version of zoom, along with the cryptocurrency mining malware.

CoinMiner is capable of mining bitcoin, Monero and Ethereum and when operating soaks up the majority of a systems computing resources causing it to run slowly and use a great deal of extra power.

Related Articles

- NYC schools step away as Zoom sets remediation plan
- Cybercriminals targeting Zoom, Google and Teams domains
- Default exploited by 'Zoom bombers' could by used by cybercrooks

Once injected into a system the malware first does a system check. Using the CPUinfo tool it determines whether the device is running a 64 or 32-bit system and will then drop into any 64-bit computer encountered. There is no 32-bit version of the malware being used.

Further information on the systems GPU, operating system, video controllers and processors is then gathered along with a determination if the target is running Windows Defender, Microsoft Smartscreen or a antivirus program and if found the malware will attempt to hide itself.

Trend Micro has contacted Zoom to help that firm communicate the problem with its customers. The security firm also noted the only way to avoid being hit with this type of malware is to only download software from the company's official download site.

CoinMiner found in third-party Zoom download | SC Media

www.scmagazine.com ›