CryptoMiner Documentation

Intro

XMRig is a high performance, open source, cross-platform RandomX, KawPow, CryptoNight and Argon2 CPU/GPU miner, with official support for Windows. It is used for the mining process of cryptocurrencies and is known for its effectiveness and ease of use. It's important to note that while this tool is legitimate, it can be misused by malicious actors. This kind of tool can be detected by our NovaGuard and NovaCommand, and our platform is cable of logging the whole stack trace. Therefore provide informations such as wallet address (help identify owner of crypto wallet) and Pool server, etc. Also on the platform we have the ability to deal with the malware, quarantine the malware and perform a full virus scan.

Disclamer

Please be aware that this document includes a demonstration of potentially harmful software. It is crucial that you strictly follow the instructions provided. Any deviation from these instructions could result in unintentional damage to your systems.

Instructions

1. On the workstation or server, start demo.exe
2. Click on run to release the crypto miner
3. Read the instructions and click on ok
4. New window pops up, with CryptoMiner.zip in it
5. Unzip it with password **forenova**
6. Go into the folder and double click to run the main program, usually named main.bat, main.exe, main.vbs for windows and main.sh, main.AppImage, main for linux
7. It will be automatically stopped after one minute, then incident is automatically generated

Behaviors

1. Connect and communicate with the Monero pool donate.v2.xmrig.com
2. Retrieve system information, including supported CPU instructions
3. Open and read the config.json file
4. Attempt to load the WinRing0x64.sys driver file
5. This process may lead to high CPU usage and power consumption

reference

https://www.virustotal.com/gui/file/aa5aa045006070e1781dd6bc25215d363ed1628741207b5f3afdf040ecf36c0c/behav

https://www.joesandbox.com/analysis/1315785/0/html