KEYWORDS: CRYPTOMINING, CRYPTOJACKING, TEST, ENDPOINT PROTECTION, ENTERPRISE, BUSINESS, CORPORATE, NIOGUARD.

27.08.2019

VERSION 1.6

Anti-Cryptojacking Test

/ JULY 2019

NioGuard Security Lab

Contents

01 Introduction

NioGuard Security Lab (Tester) tests a variety of corporate endpoint security products from the industry leaders in an effort to judge which were the most effective in detecting unauthorized cryptomining called cryptojacking. Each product is exposed to the same threats that represent cryptominers in different forms. The Test Report indicates how effectively the products were at detecting those threats in real time.

The Test follows the AMTSO Testing Protocol Standard and is a subject for a compliance check by AMTSO. For more information see the test page https://www.amtso.org/amtso-ls1-tp014.

02 Cryptojacking

Cryptojacking or malicious cryptomining is a new type of threat that can be described as the unsolicited use of a user's computing device to mine cryptocurrency. There are two types of cryptojacking attack: general purpose and targeted.

In a general purpose attack, cryptominer is installed on the infected device typical as a result of a mass spam campaign that leveraged social engineering techniques to established a foothold on a victim's machine. Alternatively, such attacks may end up in ransomware delivery. Typically, Trojan-Downloaders once executed on a user's machine check for the number of CPU/GPUs and, if there are two or more of them, malware gives a favor to installation of cryptomining software. Examples:

- Jan 2018 - a malicious Monero cryptominer called Smominru (a.k.a. Ismo) spread using the EternalBlue exploit (CVE-2017-0144) and managed to earn 8,900 Monero which was an equivalent of approximately $3M.[1]
- Jan 2018 - Monero and Electroneum miners were distributed using RIG EK via the installation of SmokeLoader malware.[2]
- Feb 2018 - Trickbot, delivered through mass spam campaign, added the Monero cryptomining module.[3]

On the contrary, in the case of a targeted attack, criminals search for ways to get access to corporate environments, mostly located in the cloud, with high computational capacity to mine cryptocurrency at the expense of the compromised tenant. One of the common ways attackers get access to a corporate cluster in the cloud is searching for secrets such as keys, logins and passwords that have been mistakenly published by engineers in configuration files to the public code repository services such as Github and Gitlab. Attackers use for that purpose the secrets crawlers, for example, TruffleHog. Another is scanning the Internet for exposed due to misconfiguration machines using the Shodan vulnerability and exposure scanning service. Examples of targeted cryptojacking attacks:

- Oct 2017 - A security flaw in Oracle's WebLogic Server (CVE-2017-10271) allowed attackers to install miners at universities and research institutions.[4]
- Feb 2018 - Tesla's Amazon Web Services (AWS) account exposed, and hackers deployed cryptocurrency mining software called Stratum to mine cryptocurrency using the cloud's computing power.[5]
- Feb 2018 - CheckPoint said that attackers made more than $3 million by mining Monero on Jenkins exploiting CVE-2017-1000353.[6]
- Sep-Oct 2018 - The misconfiguration in Docker API led to deploying the Monero cryptominer at targets' environments in China, the United States, France, Germany, and the United Kingdom.[7]

[1] https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators
[2] https://blog.malwarebytes.com/threat-analysis/2018/01/rig-exploit-kit-campaign-gets-deep-into-crypto-craze/
[3] https://blog.malwarebytes.com/cybercrime/2018/02/state-malicious-cryptomining/
[4] https://www.fireeye.com/blog/threat-research/2018/02/cve-2017-10271-used-to-deliver-cryptominers.html
[5] https://www.wired.com/story/cryptojacking-tesla-amazon-cloud/
[6] https://research.checkpoint.com/jenkins-miner-one-biggest-mining-operations-ever-discovered/
[7] https://www.bleepingcomputer.com/news/security/misconfigured-docker-services-actively-exploited-in-cryptojacking-operation/

Malicious cryptomining can be also run in the Internet Browser using the Coinhive API. While this technique is not malicious itself, but running it without the user's consent makes it illegal. Therefore, we as well as many other antivirus vendors consider cryptominers as Potentially Unwanted Software (PUS).

03 Test Description

The Test aims to verify detection capabilities of security solutions against cryptomining that may use organization's computing resources (CPUs/GPUs) for unauthorized cryptocurrency mining.

The sources of cryptominers used in the test are:

1. Public code repositories (e.g. Github) that contain the source code and/or binaries of the popular cryptominers.
2. Malware caught in the wild that unsolicitedly use a user's computer to install and run a cryptominer.

All threats are identified, collected and analyzed independently of security vendors directly or indirectly involved in the test.

For negative tests, everyday legitimate activities were taken into account that have a significant impact on CPUs (GPUs) and may lead to potential false positives.

By default, the latest version of a product is used at the moment of running a test unless specific version is requested by a Vendor, which will be mentioned in the Test Report.

The test contains the following scenarios:

1. The publicly available cryptominers.
2. Packed and/or obfuscated versions of the cryptominers mentioned in item 1 to exclude signature-based detection.
3. Malware that start cryptominers on an infected host.
4. Negative tests that include legitimate everyday activities resulting in high CPU/GPU load.

The test aims at testing the capabilities of endpoint security solutions to identify cryptomining activity on a host focusing on behavior blocking functions.

Configuration approach is using the default settings if other is not specified in the Test Report.

04 Testing Process

In case of running cryptominers from the public source code repositories, the compiled miners, if available, are downloaded and run under a user with regular privileges via the command line. If compiled versions of the miners are not available, the miners are compiled. If a cryptominer requires installation of addition software or framework (e.g. Java Platform), this will be installed in a test environment. The default wallets and mining pools are used for cryptomining in the tests. The test environments are built on the Windows 10 OS with all patches available to the moment of test.

05

Test Environments

CPU test environment

VirtualBox Windows 10 virtual machine
CPU 2 (Intel Core i5-3210 2.50GHz)
RAM 4,00 GB
Windows 10 17134 64-bit

GPU test environment

Intel Core i7-4710HQ 2.50 GHz
RAM 16.0 GB
Intel HD Graphics 4600
NVIDIA GeForce GTX 850M 4 GB
Windows 10 1809 64 bit

06

Tested Products

Product Vendor	Product Name	Version
Acronis	Acronis Backup	12.5, build 13400

The test also includes the anonymous testing results for seven more top endpoint security solutions to evaluate the anti-cryptojacking protection level in the industry, so we could assign a relative protection class to the tested products with the help of a cluster analysis.

According to the Opt-Out Policy mentioned in the test plan, it should be noted that Avast with the Avast Business Antivirus Pro Plus product has participated in the test but decided to opt-out after the Feedback and Dispute Resolution stage.

F-Secure stated to have been a non-participant and was removed from the participant list.

07

Results Evaluation

The following occurrences during the Test will be recorded and all contribute to the product effectiveness measure.

- Threat detection in the form of pop-up information messages or requests for action.
- Threat blocking in the form of:
  - Execution blocking.
  - Process blocking.
  - Network connection blocking.
- Details of the threat, as reported by the product (e.g. threat name; attack type).
- Unsuccessful detection of threats.
- Legitimate processes allowed to run without blocking.

Measuring Product Effectiveness: Each Target System is monitored to detect a product’s ability to detect, block, or neutralize threats that are executed. As cryptominers considered by some Vendors as Potentially Unwanted Application (PUA) and their Products do not block but only notify a user, we do not distinguish product’s reactions such as detection, blocking, or neutralizing cryptominers assigning them the same score for any type of reactions that help a user identify cryptomining activity.

Protection Rating is calculated according to the following formula:

$$Protection\ Rating = \sum_{i} dw \cdot x_i, \tag{1}$$

where

dw - detection weight, in particular:
dw = 1, if a positive test (a threat) is prevented from execution but not detected;
dw = 2, if a positive test (a threat) is detected and corresponding notification is shown;
$x_i = \{0, 1\}$, represents a product's reaction to the positive test *i.*
0: stands for no reaction from the product side;
1: a product reacts by detecting or blocking a specific test;
$i \in [1, N]$, where *N* is the total number of positive tests.

In addition, we calculate True Positive Rate (TPR), False Positive Rate (FPR), and Accuracy.
TPR (2) measures the proportion of true positive detections that are correctly detected as such. FPR (3) measures the proportion of false positive results that are incorrectly identified as such among all negative tests.

Accuracy (4) shows the relation of the correct detections to the overall number of test cases.

$$TPR = \frac{TP}{TP + FN}, \tag{2}$$

$$FPR = \frac{FP}{FP + TN}, \tag{3}$$

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}, \tag{4}$$

where

- TP (True Positive) — correctly detected,
- FP (False Positive) — incorrectly detected,
- TN (True Negative) — correctly skipped,
- FN (False Negative) — incorrectly skipped.

Assigning Protection Class: To assign a protection class (AAA, AA, A), the tested products are clustered with the help of Hierarchical Clustering taking into account their Protection Rating. The higher protection class is assigned to the products within the cluster that has higher average Protection Rating. If a product earns less than 50% of Protection Rating, it does not pass the test and is excluded from the Protection Class assigning procedure.

08

Test Results

Product	False Positive Rate	Protection Rating	Protection Rating, %	Accuracy	Protection Class[1]
Acronis Backup	0%	68	94%	95%	AAA
Solution A	0%	16	22%	28%	Not Passed
Solution B	0%	70	97%	97%	AAA
Solution C	0%	54	75%	77%	A
Solution D	0%	68	94%	95%	AAA
Solution E	0%	53	74%	77%	A
Solution F	0%	56	78%	79%	A
Solution G	0%	50	69%	72%	A
Solution H	0%	59	82%	85%	AA

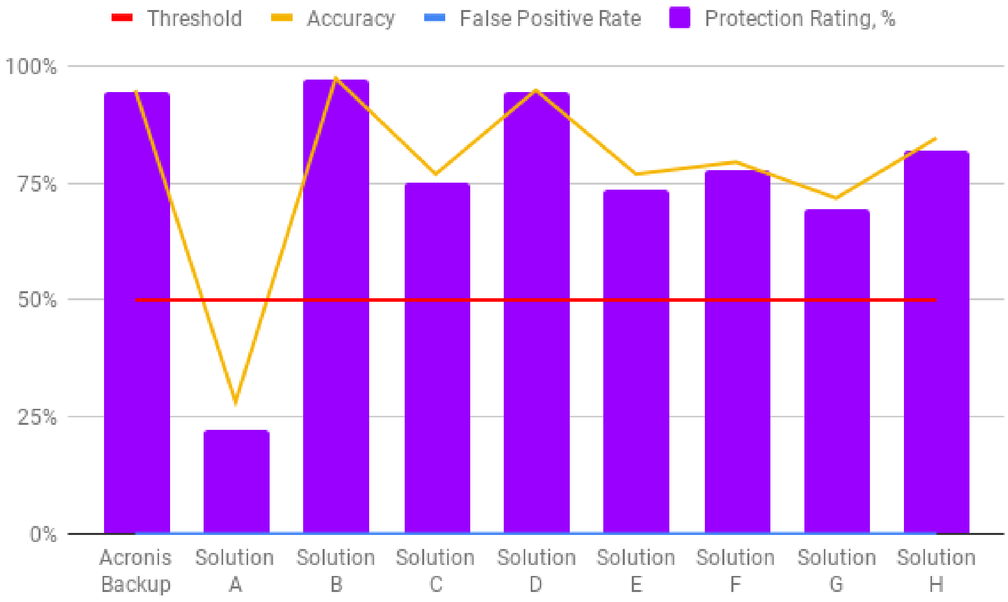

Figure 1. Distribution of Protection Rating, False Positive Rate, and Accuracy among the tested products.

[1] Protection class is assigned according to three clusters created by the Hierarchical Clustering based on Protection Rating values.

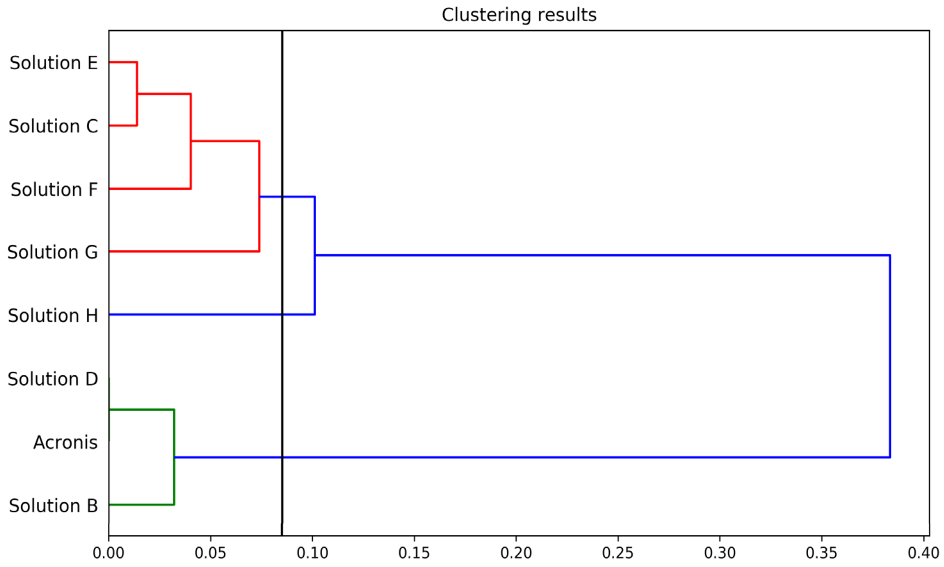

Figure 2. The dendrogram that shows the results of Hierarchical Clustering based on the normalized Protection Rating values of the products.

09 Conclusions

The test covered cryptojacking attacks that became popular during the last several years. The attack vector has shifted from mass campaigns to targeted attacks and hijacking corporate environments, whether on-premise or in the cloud, that have become an attractive target for criminals having plenty of computing resources.

The test measured True Positive (TPR), True Negative (TNR) rates, Accuracy of detection and Protection Rating. As a result of the test, Acronis Backup 12.5 earned the highest protection class **AAA** showing very good protection capabilities to detect CPU and GPU cryptominers with Protection Rating equal to **94%**. One tested product did not pass the test with **22%**. No products have False Positives.

10 Awards

Acronis Backup

11 Copyright and Disclaimer

Any use of the results provided in this report is only permitted after the explicit written agreement with NioGuard Security Lab prior to any publication.

We are not responsible for any damage or loss that might occur in connection with the use of the information provided in this paper including the test script. We do not guarantee the correctness and completeness of the content provided in this report.

For more information regarding NioGuard Security Lab and the testing methodology, please visit our website or contact us via email: ada@nioguard.com.

12 Appendix A: Cryptominers

No	Name	Description	CPU/GPU
1	Auto-miner	An XMRig cryptominer built on the MinGW POSIX WinThreads for Windows library source code: https://sourceforge.net/p/mingw-w64/mingw-w64/ci/master/tree/mingw-w64-libraries/winpthreads/ . It was used by the Plurox backdoor discovered by MalwareHunterTeam in January 2019. Detected as Win32:CryptoMiner-L[Trj].	CPU
2	CoinImp	CoinImp from node.js is used for mining Monero (XMR) and Electroneum (ETN) cryptocurrencies.This Project is a fork of CoinHive, which uses CoinImp instead of CoinHive to mine cryptocurrencies. Detected as JSCoinminer.	CPU
3	Ethminer	Ethminer is an Ethash GPU mining worker: with ethminer you can mine every coin which relies on an Ethash Proof of Work thus including Ethereum, Ethereum Classic, Metaverse, Musicoin, Ellaism, Pirl, Expanse and others. Detected as Win64:Malware-gen.	GPU
4	Dual Miner	Claymore's dual Ethereum miner is a great option that can allow for the dual mining of cryptocurrency. In addition to mining Ethereum, the software allows you to also mine Decred, Siacoin, Pascal, and more without affecting the main Ethereum mining speed. Detected as Win64:Malware-gen.	GPU
5	XMR Stak	XMR-Stak is a universal Stratum pool miner. This miner supports CPUs, AMD and NVIDIA GPUs and can be used to mine the crypto currencies Monero, Aeon and many more Cryptonight coins. Detected as Win64:Malware-gen.	CPU
6	XMRig	XMRig is a high performance Monero (XMR) CPU miner, with official support for Windows. Originally based on cpuminer-multi with heavy optimizations/rewrites and removing a lot of legacy code, since version 1.0.0 completely rewritten from scratch on C++. Detected as Win32:CryptoMiner-L[Trj].	CPU

No	Name	Description	CPU/GPU
7	CPU miner	This is a multi-threaded CPU miner for Litecoin and Bitcoin. Detected as Multi:BitCoinMiner-F[Trj].	CPU
8	NiceHash Miner	NiceHash Miner is an easy to use CPU & GPU cryptocurrency miner for Windows. Detected as Miner.Bitcoinminer.	CPU
9	NemosMiner	NemosMiner Monitors mining pools in real-time in order to find the most profitable Algo. Detected as Multi:BitCoinMiner-F[Trj].	CPU
10	BMiner	Bminer is a highly optimized cryptocurrency miner that runs on modern AMD / NVIDIA GPUs. Bminer is one of the fastest publicly available miners today -- we use various techniques including tiling and pipelining to realize the full potentials of the hardware. Detected as Trojan.Gen.9.	GPU
11	CCMiner_Alexis78	Based on Christian Buchner's & Christian H.'s CUDA project, no more active on github since 2014. Fork by tpruvot@github with X14,X15,X17,Blake256,BlakeCoin,Lyra2RE, Skein,ZR5 and others, check the README.txt A part of the recent algos were originally wrote by djm34. ccMiner release 1.7.1 (Jan 2015) "Sibcoin & Whirlpool midstate".	GPU
12	CCMiner_Dumax	Based on Christian Buchner's & Christian H.'s CUDA project. A part of the recent algos were originally written by djm34 and alexis78. Detected as Trojan.Gen.MBT.	GPU
13	CCMiner_KlausT	Based on Christian Buchner's & Christian H.'s CUDA project based on the Fork by tpruvot@github with X14,X15,X17,WHIRL,Blake256 and LYRA2 support , and some others, check the README.txt Reforked and optimized by sp-hash@github and KlausT@github. Detected as Win64:Malware-gen.	GPU
14	CCMiner_spmod-git11	Based on Christian Buchner's & Christian H.'s CUDA project, no more active on github since 2014. suprminer sp-mod (august 2018) optimized x16r algo without any dev fee. Detected as Win32:Malware-gen.	GPU
15	CCMiner_Tpruvot	Based on Christian Buchner's & Christian H.'s CUDA project, no more active on github since 2014. "phi2 and cryptonight variants". Detected as PUA.Gen.2.	GPU
16	CCMiner-x22i	Based on Christian Buchner's & Christian H.'s CUDA project, no more active on github since 2014. ccminer 2.2 (August 2017) "Equihash, tribus and optimized skunk". Detected as Win64:Malware-gen.	GPU
17	CCMiner_xevan	Based on Christian Buchner's & Christian H.'s CUDA project, no more active on github since 2014. ccMiner release 1.7.1 (Jan 2015) "Sibcoin & Whirlpool midstate". Detected as Trojan.Gen.2.	GPU
18	EWBFEquihashminer	equihash144 zhash equihash192 equihash-btg equihash96 Detected as Win64:Malware-gen.	GPU

No	Name	Description	CPU/GPU
19	Equihash NiceHash Miner	Equihash miner for NiceHash. Detected as Win32:Miner-DC[Trj].	CPU
20	Zcash	Zcash cuda miner. Detected as Trojan.Gen.2.	GPU
21	Computta Smart Miner	Computta is a first of a kind service created by cryptocurrency professionals to enable anyone and everyone's computer to make digital money for their owners completely on autopilot. It is the first service which provides simple two-click cryptocurrency mining application available for anyone to use on any Windows OS computer. eth-miner xmr-cl-miner xmr-cl-miner-v3 xmr-cpu-miner xmr-cuda-miner Detected as PUA/CoinMiner.	CPU
22	BitMinter	Multiplatform ASIC and GPU miner. Detected as Miner.B.	GPU