# Advanced Behavior-Based Technique for Cryptojacking Malware Detection

Dmitry Tanana
*Laboratory of Combinatorial Algebra*
*Ural Federal University*
Yekaterinburg, Russia
ddtanana@urfu.ru

Galina Tanana
*Department of Mathematics, Mechanics and Computer Science*
*Ural Federal University*
Yekaterinburg, Russia
g.v.tanana@urfu.ru

***Abstract*—With rising value and popularity of cryptocurrencies, they inevitably attract cybercriminals seeking illicit profits within blockchain ecosystem. Two of the most popular methods are ransomware and cryptojacking. Ransomware, being the first and more obvious threat has been extensively studied in the past. Unlike that, scientists have often neglected cryptojacking, because it's less obvious and less harmful than ransomware. In this paper, we'd like to propose enhanced detection program to combat cryptojacking, additionally briefly touching history of cryptojacking, also known as malicious mining and reviewing most notable previous attempts to detect and combat cryptojacking. The review would include out previous work on malicious mining detection and our current detection program is based on its previous iteration, which mostly used CPU usage heuristics to detect cryptojacking. However, we will include additional metrics for malicious mining detection, such as network usage and calls to cryptographic libraries, which result in a 93% detection rate against the selected number of cryptojacking samples, compared to 81% rate achieved in previous work. Finally, we'll discuss generalization of proposed detection technique to include GPU cryptojackers.**

***Keywords—Cryptojacking, malicious mining, behavioral analysis, malware detection, cryptocurrencies, cybercrime***

## I. INTRODUCTION

Cryptocurrency mining is becoming more and more popular nowadays, with an estimated value of 350 billion dollars as of August 2020 [1], which is 50% more than in 2019 [2]. Potential profits keep attracting many people to become cryptocurrency miners around the world. Due to the high demand for cryptocurrency, the mining becomes more difficult, as the algorithm usually becomes more complicated and requires more processing power to successfully mine at least one coin. Moreover, processing power comes from electrical one – only Bitcoin network consumes 120 GW every second as of April 2020 [3], which leaves significant environmental impact and costs tremendous amounts of money for miners themselves.

Naturally, this attracts cybercriminals, who want to mine cryptocurrencies without paying for hardware or electricity. They are deploying specific kind of malware – cryptojackers, which are also known as malicious miners on the victims' computers in order to use their processing power and energy supply to gain profit for themselves. Cryptojackers are vastly different from other major blockchain ecosystem malware – ransomware. Where ransomware makes its presence obvious to the victim as soon as it finishes encrypting files, malicious miners benefit from being undetected and often employ sophisticated schemes in order to avoid detection. For example, it's well known that many cryptojacker specimen go idle when the user opens Task Manager. Attackers also resort to various tricks in order to start mining on someone else's device. For example, the cryptojacker installer may be disguised as a known program.

Cybersecurity experts, such as Kaspersky [4], Symantec [5], and Eset [6] reported ever-increasing amount of attacks, which result in cryptojacking activity on victims' computers. In the first half of 2019, there have been registered around 50 millions of cryptojacking attacks, which is 450% more comparing to the same period of 2018 [7]. Additionally, cybercriminals benefit from current COVID-19 lockdown, masking malicious miner programs as Zoom or Discord installers [8] and taking advantage of yet another Bitcoin price increase, which is higher than it was in 2018 and 2019.

Originally, cryptojacking, then named "browser-based mining" was proposed in 2013 in a project called TidBit [9], which presented itself as the alternative for regular advertisement. The project, developed on student hackathon, allowed site owners to use a percentage of every visitor CPU power instead of showing them annoying ads, thus effectively monetizing their website. Keeping the human brain free from junk ads, while utilizing the CPU. The project was subpoenaed and eventually shut down because of potential misusage. However, cybercriminals heavily abused the original idea in 2017, when the Bitcoin boom happened.

Another key feature of cryptojacking is that it doesn't harm its victims directly. The only damage is indirect one – higher electricity cost, faster wear-and-tear of hardware and lack of peak processing power, when the user is launching his own heavy applications. That doesn't sound too bad compared to some other malware types like ransomware, but malicious mining offsets its relatively low harm with a scale of propagation. In order to gain profit, cybercriminals infect hundreds of thousands computers, for example in 2019 a botnet counting more than 400000 computers belonging to Bayrob Group was found and dismantled by USA officials [10].

Therefore, it's imperative to detect cryptojacking activity on the infected system as quickly as possible, because it will minimize the losses for victims. In this paper, we will propose an upgrade for the method described in our previous paper "Behavior-based detection of cryptojacking malware" [11]. In that upgrade we will modify our algorithm to deal with multi-core processors and introduce a few additional detection techniques based on the internet connection usage and cryptographic libraries calls monitoring. Finally, we'll present a prototype detection program which can discover potential malicious mining processes in OS Windows with 93% detection rate, compared to 81% rate achieved by program presented in our previous paper [11].

This work was supported by the Ministry of Science and Higher Education of the Russian Federation, project no. FEUZ-2020-0016.



978-1-7281-9972-6/20/$31.00 ©2020 IEEE

## II. CRYPTOJACKERS CLASSIFICATION AND PREVIOUS WORK

### A. Classification

Malware detection is one of the most important tasks for information security. Over the years, there were two main approaches to solve this problem – static analysis and dynamic analysis. Static analysis is most commonly used by antivirus tools. It looks for specific signatures, attributed to malware, in every new file on the computer. Those signatures are stored in vast databases, which are regularly updated by the tools' developers. The advantage of static analysis is a high degree of reliability upon detection. The disadvantage is that it's useless if there's no signature within the database, making it unusable against zero-day attacks, or if the malware is difficult to detect, like in the case of cryptojackers.

Dynamic analysis studies behavior of already running program, that's why it's also called behavioral analysis. It tries to determine whether the behavior of the program is malicious or not. Both of those approaches have been applied towards malicious mining malware in the past.

There're three main types of cryptojacking, according to Varonis [12]. The first type is file-based cryptojackers, which are regular executable-type malware. File-based cryptojackers are delivered onto victims' computers as payload of another malware, by masking themselves as legitimate software, for example, Zoom, or simply via email attachment. After installation, file-based malicious miners will try to spread themselves across the local infrastructure, mimicking virus behavior.

Second type, which is most prominent, is browser-based cryptojackers, those are JavaScript code fragments embedded in infected website. Every time a victim enters infected website, malicious miner is launched right in the browser tab. Even more troubling is the fact that the site owner might be unaware that his site is infected – infection might happen by installing corrupted WordPress plugin or by adding malicious advertisement link.

Third and the rarest type is cloud cryptojacking. Cloud cryptojacking is a specific kind of attack, when cybercriminals are trying to get API keys for a cloud infrastructure of a business. Then, they would be able to use full processing power of a business cloud for their own gain, resulting in an enormous increase of cloud account costs for business.

We think that dynamic analysis is most suited for detecting cryptojackers. It can work even with fileless malware, like browser-based cryptojackers, it can detect malware which is absent in signature databases and relies on a one thing cryptojackers cannot fake or mask – they must mine cryptocurrencies on infected machine. And in order to mine they must heavily use CPU, as we're considering only CPU-based cryptojackers in this paper, have constant internet connection and frequently call cryptographic libraries.

### B. Previous work

S. Eskandari et al. in their paper "A first look at Browser-Based Cryptojacking" [13] studied web sites to detect those with CoinHive, CryptoLoot and JSEcoin web-miner presence. Their primary method is looking for suspicious script links within web page body, such as "coinhive.min.js". While the method is very simple and allowed authors to detect a sizeable amount of infected sites, it also produced vast amount of false positives, mostly on security sites and some number of false negatives due to stealth techniques used by cybercriminals.

Quite similarly, W. Wang et al. in their paper "SEISMIC: SEcure in-lined script monitors for interrupting cryptojacks" [15] focused detecting and interrupting unauthorized, browser-based cryptojacking based on semantic signature matching. Unlike Eskandari's work, their approach was based on semantic signature matching, which is more robust towards stealth techniques than current static code analysis defenses.

D. Carlin et al. in their work "Detecting Cryptomining Using Dynamic Analysis" [14] are using Random Forest machine learning algorithm to analyze opcodes of non-executable files such as infected HTML pages. Their approach allowed them to distinguish between cryptojacking sites, weaponized benign sites, de-weaponized cryptojacking sites and real world benign sites with detection rate up to a 100%. While their results are quite impressive, they don't deal with file-based cryptojackers at all and their sample set is somewhat limited for machine learning algorithms.

H. Darabian et al. in their work "Detecting Cryptomining Malware: a Deep Learning Approach for Static and Dynamic Analysis" [16] are using deep learning techniques such as Long Short-Term Memory (LSTM), Attention-based LTSM and Convolutional Neural Networks, to capture system call events and opcodes of file-based cryptojackers, achieving 99% success rate on a selection of 1500 samples. Unfortunately, their research is limited to the file-based cryptojackers and doesn't deal with browser ones at all.

S. Aktepe et al. in their paper "MiNo: The Chrome Web Browser Add-on Application to Block the Hidden Cryptocurrency Mining Activities" [17] describe development of a web browser add-on, which offers double-layer protection against browser-based cryptojackers. With first layer being a static analysis of web page contents using external database and second layer being high CPU usage detection. However, their CPU usage detection is a simple "more than 80% over the period of 10 seconds" and they don't deal with file-based cryptojackers.

In our previous paper "Behavior-Based Detection of Cryptojacking Malware" [11] we've designed a prototype program for detecting both browser-based and file-based cryptojacking malware with a success rate of 81% over 50 samples. The program was tested on a virtual machine with Windows 7, 3GHz single-core CPU and 4GB RAM. Our algorithm was based on the mean quadratic deviation of CPU usage by given process over a minute with additional parameters being CPU usage and RAM usage, resulting in decision tree algorithm seen on figure 1.

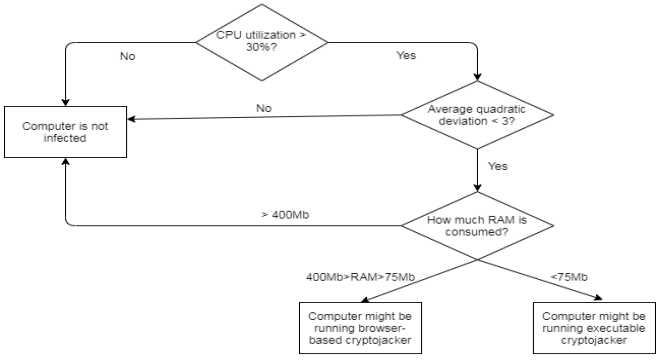


Fig. 1. Cryptojacking malware detection algorithm [11].

In order to obtain data about running processes and application we were using Windows Management Instrumentation (WMI) [18], since regular means, such as using Task Manager can activate cryptojackers' stealth techniques.

However, our program achieved only limited success and wasn't able to detect cryptojacking malware with dynamic CPU load or advanced stealth techniques, which didn't trigger our initial switch – minimum 30% CPU utilization. Additionally, we didn't test it against multi-core CPU usage.

## III. Detection Algorithm Enhancements

### A. Multi-core CPU usage

As it turns out, the multi-core CPU usage by cryptojackers is quite simple. We've tested 50 samples and seen only 3 use cases on a quad-core system. First and most prominent case (42 out of 50 samples) – cryptojacking malware used all cores evenly. Second case (6 out of 50 samples) – malware used only core 0 and core 1 evenly. Third case (2 out of 50 samples) – cryptojacking malware used only core 0. So, in order to translate our single-core decision tree scheme onto multi-core system, we need to monitor only core 0 in multi-core system and extrapolate results from core 0 onto the whole multi-core CPU. When we'll write about CPU utilization share in the following paragraphs, we would mean core 0 CPU share.

### B. Network access

Additionally, we will introduce network access as a factor for file-based cryptojackers. If the process doesn't use network at all, it's certainly not a cryptojacker, or at least not an active one. Without network it cannot execute C&C with cybecriminals' server or even simply mine cryptocurrencies.

However, nowadays quite a few legitimate applications have some kind of network service, be it cloud capability or some kind of web license. The key difference between them and cryptojacking malware is the permanence of network connection – malicious miner needs to access network on a constant basis. After monitoring network usage by 20 file-based cryptojacking samples for an hour with WMI, we've empirically determined that a malicious mining malware has to use network at least every 40 seconds to be active, with more than 50% samples attempted to access network every 5 seconds or less and the most passive behavior we've observed was one network call every 25 seconds.

### C. Cryptographic libraries calls

As determined by H. Darabian [16], the cryptojackers usually rely on standard windows cryptography libraries and more than 90% calls are to the libraries seen in table 1.

TABLE I. Cryptolibraries Used by Cryptojackers [16]

| Library | Description |
|---|---|
| bcryptprimitives.dll | Windows cryptographic primitives library |
| crypt32.dll | Crypto API32 |
| cryptbase.dll | Base cryptographic API DLL |
| cryptdll.dll | Cryptography manager |
| cngaudit.dll | Windows cryptographic next generation audit library |
| rsaenh.dll | Microsoft enhanced cryptographic provider |
| cryptsp.dll | Cryptographic Service Provider API |

In order to investigate cryptojacking possibility, we would hook onto those libraries using CoreHook library [19] and monitor all calls to them from processes with more than 10% CPU share. As we would deem only processes with more 10% CPU share as potential cryptojackers, which will help us to detect even cryptojackers with advanced stealth techniques. However, just like with network access, cryptojackers require constant access to cryptographic libraries. After monitoring 20 file-based cryptojacker samples for an hour we've empirically determined that a malicious mining malware has to use cryptographic library at least every 10 seconds, with 16 samples calling cryptographic library multiple times per second and the most passive behavior we've observed was one cryptolibrary call every 4 seconds.

### D. Enhanced algorithm

Taking all those additional factors into account, as well as lowering the initial requirement of at least 30% CPU usage, introduced in our previous work, we'll be able to upgrade our decision tree algorithm as seen on figure 2.

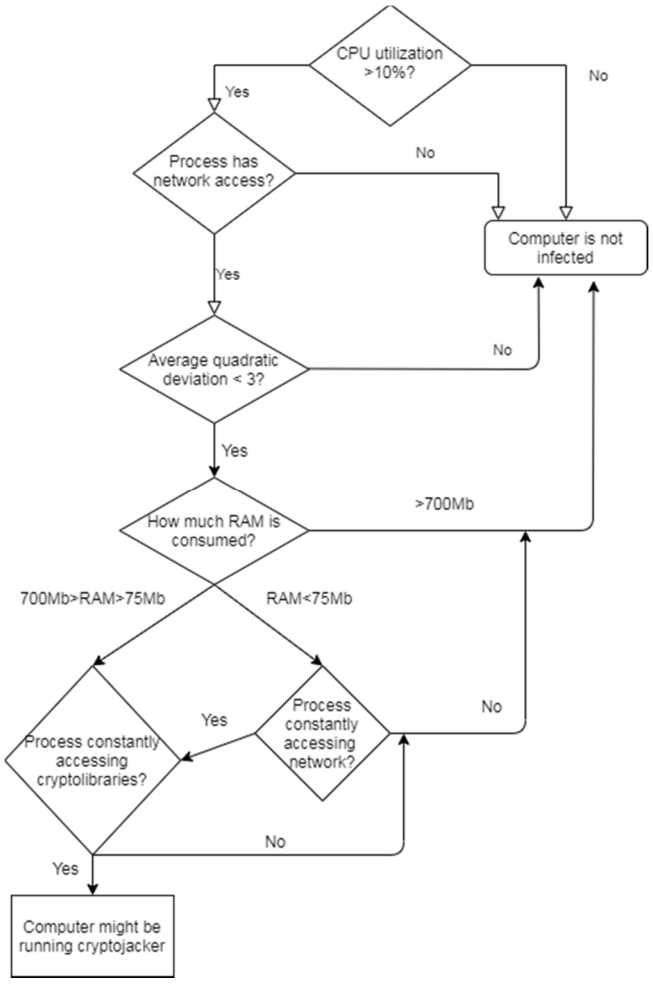


Fig. 2. Enhanced cryptojacking malware detection algorithm.

With initially lower CPU utilization share we'll be able to detect cryptojacking malware with advanced stealth techniques or generally lower CPU load, while our additional network and cryptolibraries requirements are fine-tuning detection process.

We've developed special cryptojacking detection program based on the experimental data and newly enhanced algorithm. It suggests to the user processes, which might be mining cryptocurrencies on his computer – both browser-based and file-based. And then it's the user who makes a decision, whether to terminate potential cryptojacking process using standard Windows tools such as Task Manager or not.

## IV. Results and Conclusion

In order to validate our cryptojacker detection program, we've tested it on 100 more cryptojacking malware samples, 70 browser-based and 30 file-based from VirusShare, somewhat mimicking real-world distribution, described by S. Pastrana [20], as well as some other legitimate applications. The tests were performed on VirtualBox virtual machine with following characteristics: Windows 10 OS, quad-core 3GHz CPU and 8GB RAM.

Legitimate applications mostly didn't trigger our detection program with only one exception: obviously, our program detected legitimate mining programs, such as MoneroX CPU miner. Unlike the previous program [11] this iteration had no false positives on synthetic CPU tests such as PCMark or CPU Z.

Out of 100 cryptojacking malware samples, our program was able to detect 93. We weren't able to detect 7 malicious miners: 5 out of them were browser-based samples using JavaScript web-based cryptographic libraries and 2 more were somehow going completely idle while our detection program was running. Overall success of our prototype detection program on experimental malware set is 93%, as seen in table 2.

TABLE II. Results for Enhanced Detection Program

| Cryptojacking malware set | Number of samples | Number of successes |
|---|---|---|
| Previous detection program | 50 | 41 |
| Browser-based validation | 70 | 65 |
| File-based validation | 30 | 28 |

The cryptojacking attacks are on the rise again, exploiting two additional factors. The first one being coronavirus lockdown, which forced many people without any security education to buy and use new powerful computers, which are tremendously susceptible for cryptojacking attacks. And the second being bitcoin price reaching its highest, since 2017 peak. Therefore, it's certain that cryptojacking problem will stay relevant as long as the cryptocurrency price remains high. In future we're planning to study the difference in behavior between legitimate and malicious mining applications, also we'd like to focus on detection of GPU-based malicious miners.

## References


[1] B. Mason, "The Crypto Daily – Movers and Shakers", Available at: https://www.fxempire.com/news/article/the-crypto-daily-movers-and-shakers-august-2nd-2020-664428.

[2] M. Szmigiera, "Market capitalization of cryptocurrencies from 2013 to 2019", Available at: https://www.statista.com/statistics/730876/cryptocurrency-market-value/.

[3] D. Bradbury, "How much power it takes to create a Bitcoin", Available at: https://www.thebalance.com/how-much-power-does-the-bitcoin-network-use-391280.

[4] M. Robot, "Rise of the cryptojackers", Available at: https://www.kaspersky.com/blog/cryptojacking-rsa2019/25938/.

[5] B. O'Gorman, "Internet security threat report 2019", Available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf.

[6] A. Keeve, "Cryptojacking shows no signs of slowing down in 2019, says ESET", Available at: https://www.eset.com/us/about/newsroom/press-releases/cryptojacking-shows-no-signs-of-slowing-down-in-2019-says-eset/.

[7] J. Zorabedian, "Cryptojacking rises 450 percent as cybercriminals pivot from ransomware to stealthier attacks", Available at: https://securityintelligence.com/cryptojacking-rises-450-percent-as-cybercriminals-pivot-from-ransomware-to-stealthier-attacks/.

[8] J.J. Low, "Legit Zoom downloaders could be packed with crypto-mining malware", Available at: https://techhq.com/2020/04/legit-zoom-downloaders-could-be-packed-with-crypto-mining-malware/.

[9] L. Pick, "Tidbit, New Jersey and a Subpoena: When Bitcoin Mining Gets Invasive", Available at: https://www.financemagnates.com/cryptocurrency/innovation/tidbit-new-jersey-and-a-subpoena-when-bitcoin-mining-gets-invasive/.

[10] R. Macfarlane, "Romanian Hackers Sentenced", Available at: https://www.fbi.gov/news/stories/members-of-bayrob-romanian-hacking-group-sentenced-022020.

[11] D. Tanana, "Behavior-Based Detection of Cryptojacking Malware", Proceedings of 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology, May 2020, pp. 0543-0545.

[12] R. Sobers, "What Is Cryptojacking? Prevention and Detection Tips", Available at: https://www.varonis.com/blog/cryptojacking/.

[13] S. Eskandari, A. Leoutsarakos, T. Mursch, J. Clark, "A First Look at Browser-Based Cryptojacking", Proceedings of 3rd IEEE European Symposium on Security and Privacy Workshops, April 2018, pp. 58-66.

[14] D. Carlin, P. Orkane, S. Sezer, J. Burgess, "Detecting Cryptomining Using Dynamic Analysis", Proceedings - 16th Annual Conference on Privacy, Security and Trust, August 2018.

[15] W. Wang, B. Ferrell, X. Xu, K.W. Hamlen, S. Hao, "SEISMIC: SEcure in-lined script monitors for interrupting cryptojacks", Computer Security. ESORICS 2018. Lecture Notes in Computer Science, vol 11099, August 2018, pp. 122-142.

[16] Darabian, H., Homayounoot, S., Dehghantanha, A. et al., "Detecting Cryptomining Malware: a Deep Learning Approach for Static and Dynamic Analysis", J Grid Computing, vol. 18, January 2020, pp. 293–303.

[17] S. Aktepe, C. Varol and N. Shashidhar, "MiNo: The Chrome Web Browser Add-on Application to Block the Hidden Cryptocurrency Mining Activities," 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 2020, pp. 1-5.

[18] "About Windows Management Instrumentation", Available at: https://docs.microsoft.com/en-us/windows/win32/wmisdk/about-wmi.

[19] T. Bizimungu, "CoreHook library manual", Available at: https://github.com/unknownv2/CoreHook.

[20] S. Pastrana, G. Suarez-Tangil, "A first look at the crypto-mining malware ecosystem: A decade of unrestricted wealth", Proceedings of the ACM SIGCOMM Internet Measurement Conference, October 2019, pp. 73-86.