Survey on Security and Privacy Issues of Cryptojacking Attacks

Neha Goud Baddam[*1], Purandhara Maharshi Chidurala[*2], Naga Sai Sumanth Muppasani[*3]
Poojitha Maridi[*4], Srija Merlyn Tupelly[*5], Koushik Kalva[*6]

[#]*Computer Science Department, University of North Texas*
1155 Union Circle, Denton, Texas.

[1]nehagoudbaddam.my@unt.edu

[2]nagasaisumanthmuppasani@my.unt.edu

***Abstract*— This article inspects the issues of crypto-jacking attacks and how it affects individuals and business. It also examines the mitigation measures and attack detection mechanisms used in cryptojacking attacks.**

***Keywords*— Cryptojacking, cryptocurrencies, cryptomining, Hijackers, victims.**

I. Introduction

In a world that is moving toward the digitization of things, cryptocurrencies are a huge invention of the generation. Cryptocurrencies are digital currencies that are part of a decentralized system that maintains and verifies all transactions using cryptography [10]. The word **cryptojacking** is derived from the word "Hijack", it is an illegal way of mining cryptocurrency using the victim's devices (Eskandari et al. 2018). The hijackers usually send malware through emails and websites, once the malware is downloaded on the victim's device, the hacker misuses the victim's device resources and processing power to mine cryptocurrencies, the process of mining cryptocurrencies is also known as **cryptomining** (Benetton et al.). The victims remain unaware of the attack, posing security ramifications for individuals and businesses.

II. Related Works

Kshetri Nir claim that 17% of organizations worldwide with cloud-based infrastructures had cryptojacking activity from December 2020–to February 2021 [1]. Many researchers studied crypto-jacking attacks and came up with few detection and mitigation measures.

Below are a few main cryptojacking methods suggested by many researchers:

1. Behaviour-Based Detection of Cryptojacking Malware. Dimitry Tanana describe this method of detecting cryptojacking based on the behaviour of the device. [2] [16]
2. Browser-based cryptojacking mechanism. Shayan Eskandari, Andreas Leoutsarakos, Troy Mursch and Jeremy Clark explained Browser-based cryptojacking. [3] It was also explained by M. Saad et al. in his paper. [20]
3. Website Cryptojacking Detection Using Machine Learning. Venkata Sai Krishna and Avinash Nukala explained how machine learning can be used in detecting cryptojacking on websites. [4]
4. Cryptojacking Detection with CPU Usage Metrics. Faiguebio Gomes and Miguel Correia et al. in their paper "Cryptojacking

Detection with CPU Usage Metrics," [5] provide methods to detect cryptojacking attacks by analyzing CPU usage of the victim's device.

Giorgio Di Tizio; Chan Nam Ngo et al. in his paper defined some other crypto-jacking methods are as follows: [6]

1. Analyzing executed JavaScript code and WebSocket traffic frames for obfuscated JavaScript.
2. Searching Source code if any known strings can be found.
3. Call stack observation and seeking for periodic executions
4. Verifying CPUs L1 and L3 cache usage and characteristics of crypto mining to identify mining scripts.
5. Employment of API method.

Among the many mitigation measures, below are the few main defending mechanisms and mitigation measures from cyptojacking.

1. A Cross-Stack Approach Towards Defending Against Cryptojacking. Nada Lachtar; Abdulrahman Abu Elkhail; Anys Bacha; Hafiz Malik [7] explained Cross-Stack Approach to defend against cryptojacking.
2. Mitigation of Cryptojacking Attacks Using Taint Analysis. A. D. Yulianto, P. Sukarno, A. A. Warrdana and M. A. Makky et al. in their paper [8] explained that whenever sensitive data elements are accessed by a JavaScript program, it ensures that the results are considered malicious.

III. History of Cryptocurrency and Cryptojacking

In the late 1980s, the idea of cryptocurrency emerged, the currency did not require centralized entities like banks for transferring money. In 1995, electronic money called DigiCash was implemented which uses software to perform electronic payments. Later in 1998, Bit Gold was invented, which is considered the precursor to Bitcoin, it involved solving cryptographic puzzles, and users who solved the problem received the money rewards. On 31st October 2008, Bitcoin was invented using blockchain technology. The value of bitcoin was negligible in the first few months, it was 14 cents in 2010 when it started trading, and in 2022 it is $40,200.

From 2014-to 2016, the number of scams related to cryptocurrencies rose, due to the lack of a centralized system, giving opportunities to criminals. Mt.Gox, one of the largest bitcoin exchanges was hacked and all the bitcoins were stolen, though it was not the only event it served as a cautionary tale. To avoid these kinds of attacks, users were advised to use digital wallets to store the cryptocurrencies that were hard to hack during that period.

Later in 2017, a new blockchain technology called Ethereum was invented that generates over 200,000 different projects that have their own cryptocurrencies.

Bitcoin and Ethereum are quite robust, digital currencies have sparked the interest of both individuals and businesses. Currently, there are over 4,000 cryptocurrencies that have the potential to transform the global banking system.

It has become popular after 2017 when attackers started to exploit legal mining scripts, especially Coinhive scripts. Coinhive was actually a

legal mining service that provided scripts and servers for in-browser mining activities. Nevertheless, over 10 million web users had been victims every month before the Coinhive shutdown that happened in Mar 2019. [18]

IV. Cryptojacking Attacks

The vulnerability that the user is unaware of is called zero-day vulnerability. These attacks are unpredictable and can be exploited easily. Large amounts of these kinds of attacks are seen in Microsoft products and Acrobat products. [9]

Attacks involving zero-day vulnerabilities[9]:

Attacks	Description
Aurora	Focused mostly on acrobat and google products and can exploit many zero-day vulnerabilities to attack victim systems.
Iframe injection attack	All the iframes are directed to a particular IP address that abuses zero-day vulnerabilities to download malicious files.
Luckycat	An email is sent to the user that opens the malware.
Stuxnet	This self-replicates through networks and even removable devices until it reaches the target system. This is the first to show that malware is not restricted by isolation from the internet.
RSA APT Breach	Advanced persistent threat (APT) is used to steal RSA two factor authentication secureID and links with malware are sent to victims.
Red October	The attackers attacked various government agencies with emails and documents with malware.
PLEAD attacks	This attack uses emails to attack the victim's system. If the victim opens the emails, it triggers installation of malware in the victim system that gathers information.
DarkLeech attack	These attacks are targeted mostly on web servers. Most of the victims used the Apache tomcat server.
CFR Watering hole breach	On the Council of foreign relations website malicious content was hosted which in turn exploited victims' systems.

LadyBoyle malware	This malware uses files that exploit buffer overflow errors with corrupted animation tags for remote code execution.
MiniDuke attack	This uses an adobe reader to deliver malware called ItaDuke which is distributed in the form of a PDF file using JavaScript.
DeputyDog	This attack uses network monitoring for uploading and downloading files creating backdoors and controlling processes.
SnowMan attack	This attack targeted American military personnel through the US Veterans of Foreign Wars' website.
Clandestine Fox	It mainly targeted government organizations for remote execution exploits in Internet Explorer.
Sandworm attack	This uses spear-phishing emails to deliver malware to victims. This attack looks for disabled drivers in target systems and replaces them with malicious copies and enables them.
Dailymotion.com breach	Dailymotion visitors are redirected to a website with malicious files which compromises the target systems.
Russian Doll	This attack uses an adobe flash player to deliver a payload to the target system which exploits a vulnerability in Windows to steal data from the victim.
Cloudy Omega	This attack delivers documents and payloads to victims to steal sensitive information from the target system.
Hurricane Panda	This attack uses a web shell to compromise the system and a script is uploaded to a web server using SQL injection.

V. Cryptojacking Detection Methods

Below are a few main methods used across businesses to detect cryptojacking attacks[9]:

Detection-Methods	**Description**

Anomaly-based detection	The system will use its knowledge of pre-existing and already known anomalies to detect if the present attack is an attack or not. This method employs a set of rules to analyze threats and judge the nature of the event. Programs that will not pass the rules are considered a threat to the system. Then these are removed and sent for manual inspection. This method checks for any abnormalities and suspicious activities or potential danger, if found then the code is sent for inspection.
Signature-based detection	This method involves the use of analysis of different attributes in a piece of code that generates a unique signature to check if the code is safe for execution or not. Given a part of code, there are many algorithms that can generate digital signatures of code. When a certain part of the code is scanned and found to be malware then the signature of that code is appended to a database of known attacks. This is mostly used for malware detection. The ease of this method makes it a widely used technique.
Completely Automated analysis	This method uses the already existing tools for malware analysis. This tool generates studies about network use and resource use etc. This method provides great insight into malware and prevention options.
Static Analysis	This method involves code checking without execution. This method can be useful because it doesn't require any high computational power for the execution of code. There is no execution of code, so the malware attack is not possible. This method pauses the code execution and investigates the code for inspection. There are many factors that indicate the possibility of malware attacks.
Interactive behaviour analysis	Sandbox is used for the execution of malicious code. There is no interaction of code with system resources and the probability of malware attack is low. This will open opportunities for experiments on malware and give us insight into many zero-day attacks.
Code reversal	This technique involves manually searching every module and executing a particular change and this method is extremely time-consuming. This method requires in-depth logic of working on the computer and makes it the least preferred option.
CPU with machine learning-based analysis	When a website is visited, a tool will run for CPU monitoring to gather metrics which are later supplied to the machine learning classifier. Then the classifier assigns a class as cryptojacking or not.[5]
CPU usage metrics analysis	When a website has malware, then the target system CPU performance would be low with high cache activity. Keeping in check with cache activity helps to recognize the presence of malware [4].

Apart from the above complex methods, even a layman can detect cryptojacking attacks by using the following methods:

1. **Decrease in device performance:** One of the major signs of cryptojacking is the poor performance of the devices. The battery drains out faster than usual. The system runs slowly and crashes.
2. **Overheating of the devices:** Cryptojacking utilizes victims' resources that can cause overheating of the computing devices leading to damage or shortening of the device's lifespan.
3. **Central Processing Unit (CPU) usage:** Increase in CPU usage even if the user is not using any devices.

VI. Mitigation Measures of Cryptojacking

Below are a few mitigation measures to prevent cryptojacking

1. **Obtaining Consent:** Protection is better and required than Detection. Protection isn't that simple, some norms are to be accepted by users to be protected. Authedmine is one such service from Coinhive where user consent is taken first to implement the Security practice.[8]

   We have seen many cases of click-based jacking attacks where iframes are used in the hijacking user web sessions which can also be reduced by using a defensive approach frame busting which doesn't let the website function anymore once it's loaded inside that frame optimizing system calls browser pass to OS.[8]

2. **Browser level mitigation:**
   a. Scripting technique can be implemented on the client-side by limiting the requests received on the server in a particular period.End-users will be warned when an excessive number of resources are consumed. And also these sources are blocked. [8]
   b. Blocking cryptojacking scripts using 'NoCoin' blacklist like Opera.[8]
   c. Informing users via notifications to make decisions whether to track resource consumption and to give warnings like Security Socket Layer/Transport Layer Security warnings when the End user is expecting to visit one website but the browser cannot confirm it or if the encryption is not adequate enough to the data path sent by the user.[8]

Apart from the above complex methods, below are a few steps that can be taken to prevent cryptojacking attacks:

1. Installing the latest cybersecurity programs.
2. Following and understanding the latest cryptojacking trends.
3. Using browser extensions that block cryptojacking. (Example: minerBlock, No Coin, and Anti Miner)
4. Using ad blockers that can detect and prevent harmful cryptojacking codes.

5. Disabling JavaScript on the browser, to prevent cryptojacking code from corrupting the system.
6. Install applications that prevent harmful pages that deliver cryptojacking scripts.

VII. Cryptocurrencies Mining with CPUs and GPUs

In recent years the use of GPUs for mining tasks is very popular [11] [12]. The integration process depends on using modern processors that combine CPUs and GPUs. This process is very important which considers some tasks that could benefit from GPU processing to improve efficiency where applicable. This study selects many cryptocurrencies for mining and tests these cryptocurrencies using GPUs and CPUs to extract the actual results. There are over 1,000 cryptocurrencies created, over 1,000 cryptocurrencies.[13]

Both the CPU and GPU can work together to enhance the speed of information transfer and the number of simultaneous calculations within the application. Initially, GPUs were manufactured for multimedia and graphical purposes such as creating images, viewing videos, and computer games. In 2010, this was the first use of GPUs to speed up calculations involving massive amounts of data. We cannot replace the CPU with the GPU but the GPU complements the architecture of the CPU. We mean the application instructions that have to run in parallel can run in GPUs while the major program continues executing on the CPU [14][15]

VIII. Some Common Features

Below are a few common features among the cryptojacking attacks that have been identified during this survey.

Method of Attacks	**Cryptojacking Attacks**
Phishing emails	Lucky Cat Attack, Sandworm Attack & Plead Attack.
Web server	Dark Leech Attack, Hurricane Panda.
Files (PDF/doc)	Aurora, Red October, Russian Doll, Cloudy Omega & Mini Duke.Attack
Website	CFR Watering hole breach & SnowMan attack.
Network attack	Stuxnet, IFrame injection attack & Deputy Dog Attack.

Overall, this paper makes the following contributions:

1. It presents an overview about cryptocurrencies and cryptojacking.
2. It shows the history of the attacks and how they have emerged throughout the timeline.
3. It describes the most popular cryptojacking attacks.
4. It also presents mitigation measures to protect businesses/individuals from cryptojacking attacks.
5. It also briefs about cryptocurrency mining using CPUs and GPUs.

After conducting this survey we have found out that the number of cryptojacking attacks grew in the past year. [17]

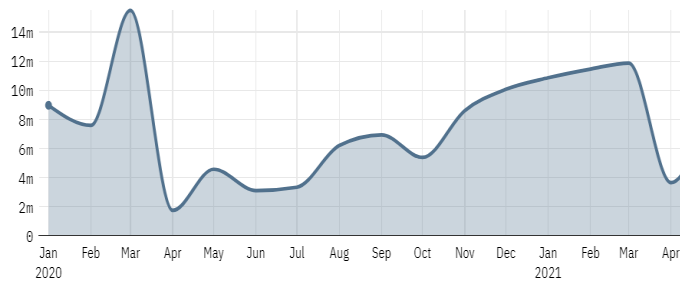

Fig.1 Number of cryptojacking attacks detected globally (January 2020 - June 2021)

IX. Future Work

The results from the various existing research gives us a simple idea that using CPU in mining not profitable all the time while using GPU in mining will give more profitable results because the GPU can handle many complex mathematical computing in parallel method. Also, the GPU architecture depends on many factors such as VRAM which makes it handle many processes more efficiently in the same time. This research can be used in future research to produce useful findings and datasets that can be used in machine learning to extract useful knowledge about the best approach and to precisely define methods in mining. [13]

Machine learning (ML) is a subset of artificial intelligence (AI). It falls into two models: static and dynamic. Static ML starts with providing an AI solution with offline training. Dynamic ML (often called deep learning) solutions train themselves while online. They do not entirely rely on humans taking them offline to provide new observed behaviors. Dynamic ML uses big data resources containing malicious behavior and cognitive patterns to learn what is and is not anomalous behavior. Big data resources for ML include years of data about how threats behave on a network or a system. This data is then combined with an organization's baselines. It is better at identifying zero-day attacks.The use of dynamic machine learning is growing as an augmentation to traditional antimalware approaches. When looking for network and device protection solutions with ML, organizations must ask the right questions to ensure they are getting genuine dynamic ML that includes both continuously maintained and comprehensive vendor data pools and meaningful input from their own information resources. [21]

X. Conclusion

Due to the lack of knowledge of the cryptojacking attacks, the threat from these attacks is high. Individuals and Businesses should understand and study the mitigation measures and the different types of crytojacking attacks to protect themselves from these attacks.

Present security solutions are not robust enough to secure cryptojacking attacks. Vulnerabilities do not seem evident at first but can be exploited in the long run. With recent outbreaks and an ever-growing list of malicious software, the importance of malware analysis has increased. Multiple methods have been proposed but a unified solution does not exist. With new attacks like Cryptojacking, a study in this region is required.

Acknowledgment

It was a great opportunity for us to do a survey about cryptojacking and finding different attacks, mitigation measures and common features among the attacks. We got a chance to explore various websites and paper publications that helped us get acquainted with the concept of cryptojacking.

We acknowledge with gratitude to professor Amir Mirzaeinia and assistant professor Himan Namdari, who have been helpful in guiding us through the process of this survey.

We hope that this paper will be useful to everyone who is interested in cryptojacking. This paper gives a high-level understanding of cryptojacking.

We have tried our best to gather as much information as possible from the existing data. There is still a lot of scope for analyzing this issue of cryptojacking, as it is still a booming issue in the current work of digital currencies.

References

[1] N. Kshetri and J. Voas, "Cryptojacking," in Computer, vol. 55, no. 1, pp. 18-19, Jan. 2022, Cryptojacking | IEEE Journals & Magazine doi: 10.1109/MC.2021.3122474.

[2] D. Tanana, "Behavior-Based Detection of Cryptojacking Malware," 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), 2020, pp. 0543-0545, Behavior-Based Detection of Cryptojacking Malware - IEEE Xplore doi: 10.1109/USBEREIT48449.2020.9117732.

[3] Shayan Eskandari, Andreas Leoutsarakos, Troy Mursch, Jeremy Clark, A FIRST LOOK AT BROWSER-BASED CRYPTOJACKING, 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 09 July 2018.A First Look at Browser-Based Cryptojacking - IEEE Xplore

[4] Venkata Sai Krishna, Avinash Nukala, "Website Cryptojacking Detection Using Machine Learning", 2020 IEEE Conference on Communications and Network Security (CNS): Posters, 29 June-1 July 2020 Cryptojacking: How the crypto boom is driving malware infections(Cryptojacking: How the crypto boom is...)

[5] Faiguebio Gomes, Miguel Correia, " Cryptojacking Detection with CPU Usage Metrics", 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA), 24-27 Nov. 2020

[6] Giorgio Di Tizio; Chan Nam Ngo, "Are You a Favorite Target for Cryptojacking?" Are You a Favorite Target For Cryptojacking? A Case-Control Study ...A Case-Control Study On The Cryptojacking Ecosystem, 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 22 October 2020.

[7] Nada Lachtar; Abdulrahman Abu Elkhail; Anys Bacha; Hafiz Malik, "A Cross-Stack Approach Towards Defending Against Cryptojacking", 10 IEEE Computer Architecture Letters, 18 August 2020

[8] Arief Dwi Yulianto; Parman Sukarno; Aulia Arif Warrdana; Muhammad Al Makky, Mitigation of Cryptojacking Attacks Using Taint Analysis, November 2019, Available: Mitigation of Cryptojacking Attacks Using Taint Analysis | IEEE Conference Publication | IEEE Xplore

[9] Kiran Radhakrishnan, Rajeev R Menon, Hiran V Nath, "A survey of zero-day malware attacks and its detection methodology", TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), 17-20 Oct. 2019A survey of zero-day malware attacks and its detection methodology

[10] Jonathan Chiu and Thorsten V. Koeppl, "Blockchain-Based Settlement for Asset Trading," published in the Review of Financial Studies, vol. 32, no. 5. .https://doi.org/dig.v49.n9.3

[11] T.Matsumoto and M. L. Yiu, "Accelerating exact similarity search on CPU-GPU systems," Proc. - IEEE Int. Conf. Data Mining, ICDM, vol. 2016-Janua, pp. 320–329, 2016, doi: 10.1109/ICDM.2015.125.

[12] B. Guo, R. Zhang, G. Xu, C. Shi and L. Yang, "Predicting Students Performance in Educational Data Mining," 2015 International Symposium on Educational Technology (ISET), Wuhan, 2015, pp. 125-128, doi: 10.1109/ISET.2015.33.

[13] Alkaeed, Mahdi & Khan, Khaled & Al-Ali, Muhammed & Al-Mohammed, Hasan & Alamro, Zaid. (2020). Highlight on Cryptocurrencies Mining with CPUs and GPUs and their Benefits Based on Their Characteristics. Highlight on Cryptocurrencies Mining with CPUs and GPUs and ...10.1109/ICSET51301.2020.9265386.

[14] . M. Arora, "The Architecture and Evolution of CPU-GPU Systems for General Purpose Computing," pp. 1–12, 2012, doi: 10.1.1.353.231.

[15] AMD Close to the Metal (CTM). http://www.amd.com/.

[16] D. Tanana and G. Tanana, "Advanced Behavior-Based Technique for Cryptojacking Malware Detection," *2020 14th International Conference on Signal Processing and Communication Systems (ICSPCS)*, 2020, pp. 1-4, doi: 10.1109/ICSPCS50536.2020.9310048.

[17] Cryptojacking: How the crypto boom is driving malware infections(Cryptojacking: How the crypto boom is...)

[18] Vanlioglu, Bilal Gonen, Murat Ozer, Mehmet F. Bastug, "IS CRYPTOJACKING DEAD AFTER COINHIVE SHUTDOWN?", 3rd International Conference on Information and Computer Technologies (ICICT), 14 May 2020.

[19] R. Tahir, S. Durrani, F. Ahmed, H. Saeed, F. Zaffar, and S. Ilyas, "The browsers strike back: Countering cryptojacking and parasitic miners on the web," in IEEE Conference on Computer Communications, INFOCOM, Paris, France, April 2019, pp. 703–711.doi: 10.1109/eCrime47957.2019.9037576.

[20] M. Saad, A. Khormali and A. Mohaisen, "Dine and Dash: Static, Dynamic, and Economic Analysis of In-Browser Cryptojacking," 2019 APWG Symposium on Electronic Crime Research (eCrime), 2019, pp. 1-12, doi: 10.1109/eCrime47957.2019.9037576.

[21] Tom Olzak, "How to Fight Cryptojacking Attacks With Machine Learning | Toolbox It Security"

[22] P. Haridas, G. Chennupati, N. Santhi, P. Romero and S. Eidenbenz, "Code Characterization With Graph Convolutions and Capsule," in *IEEE Access*, vol. 8, pp. 136307-136315, 2020, doi: 10.1109/ACCESS.2020.3011909.