IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205183 |

Combating the Hidden Threat: A Survey of Cryptojacking

Bhuvanesh B [1], Murugan R [2]

MCA Student, School of Computer Science and IT, Jain (Deemed-to-be-University), Bangalore, India[1]

Professor, School of Computer Science and IT, Jain (Deemed-to-be-University), Bangalore, India[2]

ABSTRACT: The illicit use of computer resources for mining cryptocurrencies, or "cryptojacking," has become a common cyberthreat in the online world. This analysis explores the various aspects of cryptojacking and the sly methods that attackers use. We look at how malicious scripts can be hidden and used to steal processing power for nefarious purposes in seemingly authentic websites or ads. We also look into how cryptojacking affects people, companies, and vital infrastructure, pointing out possible issues including service interruptions, data breaches, and performance degradation. The study concludes by examining mitigating techniques, such as network segmentation for enterprises, user education, and strong security software, to counter this growing threat. We can protect our digital assets and negotiate the always shifting danger landscape by being aware of the techniques, effects, and possible countermeasures against cryptojacking.Cryptojacking can lead to performance degradation, increased energy bills, and data breaches.

KEYWORDS: Cryptojacking, browser-base, Host-based, Performance degradation, Endpoint security.

I. INTRODUCTION

The field of cyber threats has changed significantly in the last several years due to the appearance of new strategies used by bad actors to take advantage of unwary users' computer resources in order to make money. Among these dangers, cryptojacking has become a major worry for people, companies, and organizations.

Cryptojacking, also called malicious cryptocurrency mining, is the unapproved use of computing hardware to mine cryptocurrencies without the owner's knowledge or consent. Through this covert operation, fraudsters can use the computing capacity of infected devices to create virtual currencies like Monero, Ethereum, and Bitcoin, making money off of unwary victims. The act of mining cryptocurrency without the victim's consent is known as cryptojacking[1].

The rise of cryptocurrency jacking instances can be ascribed to multiple variables, including as the growing acceptance and valuation of cryptocurrencies, the extensive accessibility of mining software, and the intrinsic anonymity provided by blockchain technology. Cryptojacking functions covertly, frequently eluding notice for protracted periods of time, which increases its impact on impacted persons and organizations in contrast to conventional forms of cybercrime that depend on direct exploitation or extortion.

Cryptojacking is the term used in the literature to describe the virus used for this purpose. Attackers can now readily reach a huge user base through well-known websites, particularly with the rise of service providers (such as Coinhive [2], CryptoLoot [3]) that offer ready-to-use implementations of in-browser mining scripts. Cryptojacking malware was used with Google's YouTube advertising bundles in a significant attack [4]. Another example was the discovery of cryptojacking malware in a UK government-provided plugin [5].

In light of this, the purpose of this survey study is to present a thorough analysis of cryptojacking, covering its fundamental ideas, methods, defences, and countermeasures. This study aims to improve understanding of the changing threat landscape offered by cryptojacking and provide stakeholders with the information and resources required to protect against this sneaky kind of cyber exploitation by combining research findings from the literature with real-world case studies.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205183 |

II. BACKGROUND

Malicious cryptomining, or cryptojacking, is a cybersecurity concern that entails using computer resources without authorization in order to mine cryptocurrencies. This behavior frequently takes place without the owner of the computer's knowledge or agreement, which can result in hardware damage, higher energy usage, and decreased performance. Cybercriminals now use cryptojacking as a profitable tactic to monetize compromised systems and take advantage of the rising demand for cryptocurrency.

The rise of cryptocurrencies, especially Bitcoin, which popularized the idea of decentralized digital currency and blockchain technology, coincided with the emergence of the concept of cryptojacking. Early adopters of cryptocurrencies mined legitimately in order to validate transactions and get rewards, but soon after, bad actors realized they could use computing resources for illegal purposes. The origins of cryptojacking may be traced to the rise of cryptocurrencies, chiefly to Bitcoin, which popularized the idea of decentralized digital cash. At first, reputable organizations looked into bitcoin mining as a way to verify transactions and get paid. Nevertheless, malicious actors quickly realized that it was possible to use computer resources for illegal purposes, which is how the phenomena known as "cryptojacking" came to be.

Blockchain immutability is achieved through a consensus process, typically achieved using a Proof of Work (PoW) protocol.By increasing the nonce value with each trial, the miners attempt to discover a proper hash value through trial and error. The full block is broadcast to the network and appended to the end of the previous block upon the discovery of a valid hash value. The only method for producing new cryptocurrencies is through this process, which is called mining cryptocurrency [1].

III. TECHNIQUES AND METHODS

There are three primary stages in the lifespan of a crypto jacking malware: 1) script preparation, 2) script injection, and 3) the attack [1]. We divide the cryptojacking virus into two groups based on this: 1) Cryptojacking through browsers, and 2) Cryptojacking through hosts[1].

Browser-Based Cryptojacking
Also referred to as in-browser mining or web-based mining, browser-based cryptojacking uses online ads or JavaScript code embedded in websites to take control of users' web browsers and mine cryptocurrencies. Without the consumers' knowledge or agreement, JavaScript code runs in the background when they visit a compromised website or click on an infected advertisement. This code, usually with minimal impact on user experience, uses the CPU resources of the visitors to carry out cryptographic computations required for mining cryptocurrencies. Because browser-based crypto jacking is so subtle and can be easily spread by malevolent actors over a large network of websites, it is very dangerous. In-browser cryptojacking malware uses these web technologies to create unauthorized access to the victim's system for cryptocurrency mining via web page interactions on the victim's CPU [1].

Host-Based Cryptojacking
The act of mining cryptocurrency illegally using computational resources stored on distant servers or cloud infrastructure is known as host-based cryptojacking. The servers, virtual machines, or cloud instances that are used to carry out crypto mining operations are referred to as "host" in this context. Unauthorized access to these computer resources with the intention of mining cryptocurrency is known as host-based cryptojacking, and it usually occurs without the owners' knowledge or approval.

Host-based cryptojacking can take various forms, including:
•Compromised Servers: Cybercriminals could take advantage of software flaws in servers or get into unapproved access to install malware that mines cryptocurrency. Once deployed, This virus mines cryptocurrencies using the server's processing power.

•Unauthorized Access to Cloud Instances: In cloud environments, instances of virtual machines or containers that are provided by cloud service providers may be accessible to attackers. Then, in order to take advantage of the cloud infrastructure's processing capacity for mining, they install crypto mining software on these instances.

•Exploitation of Server Resources: Attackers may occasionally choose to take advantage of software flaws or server configuration errors rather than installing malware directly on servers in order to take control of the processing power

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205183 |

needed to mine bitcoins. Attackers could use server administrative interfaces or web application vulnerabilities, for instance, to run crypto mining scripts on servers. They are generally delivered to the host system through methods such as embedded into third-party applications [6], [7], using vulnerabilities [8], or social engineering techniques [9], or as a payload in the drive-by-download technique [10].

IV. IMPACTS

The version of this template is V2. Most of the formatting instructions in this document have been compiled by Causal Productions from the IEEE LaTeX style files. Causal Productions offers both A4 templates and US Letter templates for LaTeX and Microsoft Word. The LaTeX templates depend on the official IEEEtran.cls and IEEEtran.bst files, whereas the Microsoft Word templates are self-contained. Impacts of cryptojacking

Cryptojacking has a variety of negative effects that can be felt strongly by people, companies, and even vital infrastructure. Cryptojacking can appear to individual users as a discernible decrease in device performance. Applications that lag and become unresponsive may be caused by excessive CPU and resource usage. Victims will pay more for electricity as a result of this increased power usage. The thing that worries people the most about cryptojacking scripts may be the possibility of data breaches or malware infections that could come with them, further endangering user security and privacy.

Businesses that deal with crypto jacking confront a more intricate set of difficulties. Cryptojacking can compromise computer resources, disrupting vital activities and resulting in lost productivity and financial consequences. Furthermore, firms run the risk of serious reputational harm and possible fines from regulators if client data is compromised as a result of a cryptojacking attack. The danger is not limited to conventional enterprises; it may also affect vital infrastructure that depends on strong processing power. To illustrate the scope and gravity of this expanding threat, we shall examine actual instances of cryptojacking.

Hardware components, especially CPUs and GPUs, are subjected to protracted stress from continuous mining operations linked to cryptojacking. An extended period of high workload speeds up wear and tear, reducing hardware lifespan and raising the risk of failure. As a result, systems that are impacted encounter a decline in performance, which is evident in reduced processing rates, lowered responsiveness, and reduced computing power overall.

Performance degradation brought on by cryptojacking has a negative effect on productivity in both personal and professional contexts. People that use crypto jacked gadgets have disruptions and delays in their daily activities, which impairs productivity. Employees may experience slow systems and unresponsive apps in work environments, which lowers productivity and decreases job efficiency. These productivity declines may make it more difficult for businesses to operate and less competitive. Security flaws brought about by cryptojacking go beyond the direct effects of resource theft.

Cryptojacking malware is frequently deployed by taking advantage of security holes in systems or opening backdoors to allow unauthorized access. These hacked computers are now open to increased exploitation, which could result in malware installation, data breaches, or the theft of confidential information. Therefore, crypto jacking jeopardizes the integrity and confidentiality of digital data and presents serious hazards to data security and privacy.

V. PREVENTION OF CRYPTOJACKING

Thankfully, there are steps we may do to lessen the dangers posed by cryptojacking. One effective first line of protection is to use security software that is strong and has script-blocking and anti-malware features. An additional line of defense is provided by browser extensions made expressly to recognize and stop cryptojacking attacks. It's essential to keep systems updated and patch vulnerabilities quickly in order to close doors that could allow malicious malware to enter a system. Employee education regarding cybersecurity best practices is essential for reducing the possibility of user error, which can result in cryptojacking attacks. Examples of these best practices include avoiding dubious links and downloads.

In order to reduce the risk of cryptojacking, which is the practice of hackers using computer resources for illicit bitcoin mining, a variety of tactics and technologies must be used. Deploying strong endpoint security solutions, such as antivirus software and endpoint protection platforms, is one important mitigating technique. By identifying and stopping crypto jacking malware, these solutions help stop dangerous scripts and processes from running on specific

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205183 |

devices. Devices can be prevented from unintentionally participating in mining operations by using endpoint security solutions, which continuously monitor for suspicious activity and recognized signs of cryptojacking.

Organizations can reduce the risk of cryptojacking by using ad blockers and script blockers in addition to endpoint protection. These software programs and browser extensions are made to prevent online advertisements and scripts, which are frequently used as entry points for browser-based crypto jacking. Ad blockers and script blockers offer an extra line of defense against cryptojacking attacks by stopping crypto jacking scripts from operating in web browsers. This keeps users' computers from unintentionally being used for mining activities.

A thorough countermeasure against cryptojacking must also include patch management and regular software updates. It is crucial to maintain operating systems, online browsers, and software programs up to date with the latest security patches and updates because many cryptojacking attacks take advantage of known flaws in out-of-date software.

VI. LITERATURE REVIEW

They are typically sent to the host system by means of payloads in drive-by-download tactics [10], vulnerabilities [8], social engineering methods [9], and embedding into third-party apps [6], [7]. Academics became interested in the rise of cryptojacking malware, particularly after 2017, and this led to numerous articles. These studies, it turned out, center on three subjects: Three studies have been conducted on cryptojacking: 1) detection, 2) prevention, and 3) analysis[1]. The majority of detection methods for cryptojacking in the literature [11], [12], [13]–[17], [18], [19], [20], [21] are proposed for the detection of in-browser cryptojacking malware. There are only a few studies [22], [23] proposed for host-based cryptojacking malware. Cryptojacking, the unauthorized use of computing resources to mine cryptocurrencies, has emerged as a prominent cybersecurity threat in recent years. This literature review provides an overview of research on cryptojacking, covering various aspects such as detection techniques, economic impacts, mitigation strategies, and legal considerations.

Detection Techniques

“A Survey on Cryptojacking and Detection Techniques" Narayanan and Vinayakumar (2019) conduct a comprehensive survey of cryptojacking attacks and detection techniques. The paper provides an overview of the methods used by attackers to deploy cryptojacking malware and discusses various detection approaches, including signature-based, anomaly-based, and machine learning-based techniques.

Economic Impacts

In terms of economics, cryptojacking calls into question the economics of mining cryptocurrencies, as well as the motivations of miners, the profitability of mining operations, and the wider economic effects of mining activities that are not authorized. Economic theories that can provide light on the motivations of attackers and targets in the cryptojacking ecosystem include game theory and cost-benefit analysis.

Mitigation Strategies

Technologically speaking, cryptojacking takes advantage of the processing capacity of many devices, including servers, Internet of Things (IoT) gadgets, and personal PCs. To understand how cryptojacking works and what it means for cybersecurity, one must have a technical understanding of distributed computing, blockchain technology, and cryptocurrency mining. The cryptojacking malware's characteristic activities establish a pattern that can be identified through dynamic analysis. Static features like opcodes [24] and WebAssembly (Wasm) instructions [12] are only used in a small number of research in the literature. Stack-based virtual machines [26] enable applications to run more closely to the machine-level language thanks to WebAssembly [25], a low-level instruction format.

VII. CONCLUSION

In the digital sphere, cryptojacking has solidly established itself as a persistent and diverse menace. Its capacity to stealthily divert computer power for the purpose of mining cryptocurrencies illegally presents serious difficulties for people, companies, and vital infrastructure. The cryptojacking battlefield is always changing as attackers hone their methods and take advantage of fresh openings. This survey research has illuminated the common techniques used by adversaries, ranging from drive-by downloads that target unpatched systems to malicious scripts embedded in websites that appear to be authentic. We have looked at the wide-ranging effects of cryptojacking, such as possible threats to vital infrastructure, operational disruptions and reputational harm for enterprises, and performance degradation for individual users.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205183 |

The good news is that this threat is something we can defeat. Through the implementation of a multi-layered strategy, the dangers related to cryptojacking can be considerably reduced. This include keeping computers updated, using security software that is strong and has script-blocking and anti-malware features, and teaching users about cybersecurity best practices. By using endpoint security solutions, resource use monitoring, and network segmentation, businesses can further strengthen their defenses. Ongoing efforts are being made to combat cryptojacking, nevertheless. Our defenses must change in tandem with the changing strategies that attackers employ. Looking ahead, ongoing innovation will be key to preventing cryptojacking in the future.There is great potential for research into enhanced detection techniques that use machine learning and artificial intelligence to identify threats in real time.

Many research on the detection of cryptojacking malware have been proposed in the literature due to the lack of mitigating solutions available in the market[1]. The first thing we covered in this essay was cryptojacking, including its types, effects, mitigation, and prevention through malware. By consistently providing updates on new threats, implementing robust security protocols, and cultivating a culture of cybersecurity awareness, we can collaboratively lower the likelihood of cryptojacking and safeguard our digital assets in the dynamic online landscape.

REFERENCES

[1] E. Tekiner, A. Acar, A. S. Uluagac, E. Kirda and A. A. Selcuk, "SoK: Cryptojacking Malware," 2021 IEEE European Symposium on Security and Privacy (EuroS&P), Vienna, Austria, 2021, pp. 120-139, doi: 10.1109/EuroSP51992.2021.00019.
[2] The official webpage of both coinhive and authedmine, [online] Available: http://web.archive.org/web/20190130232758/https://coinhive.com/documentation.
[3] Cryptoloot, [online] Available: https://crypto-loot.org/
[4] D. Goodin, "Miners in youtube ads", [online] Available: https://arstechnica.com/information-technology/2018/01/now-even-youtube-serves-ads-with-cpu-draining-cryptocurrency-miners/
[5] K. Parrish, Uk government plugin based mining, [online] Available: https://www.digitaltrends.com/computing/government-websites-plugin-coinhive-monero-miner/
[6] D. Olenick, Miner into third party zoom, [online] Available: https://www.trendmicro.com/en_us/research/20/d/zoomed-in-a-look-into-a-coinminer-bundled-with-zoom-installer.html.
[7] M. Santos, utorrent update smuggles shady cryptocurrency miner into your computer, [online] Available: https://99bitcoins.com/utorrent-update-cryptocurrency-miner/.
[8] B. G. Mark Vicente and Johnlery Triunfante, Cve-2019–2725 exploited used to deliver monero miner, [online] Available: https://www.trendmicro.com/en_ca/research/19/f/cve-2019- 2725-exploited-and-certificate-files-used-for-obfuscation-to-deliver-monero-miner.html.
[9] C. McDonald, Cryptojacking malware hid into emails, [online] Available: https://www.mailguard.com.au/blog/brandjacking-malware-hiding.
[10] K. G. Rakesh Sharma and Akhil Reddy, A vulnerability used to deliver cryptojacking malware, [online] Available: https://www.fireeye.com/blog/threat-research/2018/02/cve-2017- 10271-used-to-deliver-cryptominers.html.
[11] R. K. Konoth, E. Vineti, V. Moonsamy, M. Lindorfer, C. Kruegel, H. Bos, et al., "Minesweeper: An in-depth look into drive-by cryptocurrency mining and its defense", Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS), pp. 1714- 1730, 2018.
[12] J. D. P. Rodriguez and J. Posegga, "Rapid: Resource and api-based detection against in- browser miners", Proceedings of the 34th Annual Computer Security Applications Conference (ACSAC), pp. 313-326, 2018.
[13] R. Ning, C. Wang, C. Xin, J. Li, L. Zhu and H. Wu, "Cap-jack: Capture in-browser crypto-jacking by deep capsule network through behavioral analysis", INFOCOM 2019-IEEE Conference on Computer Communications, pp. 1873-1881.
[14] A. Kharraz, Z. Ma, P. Murley, C. Lever, J. Mason, A. Miller, et al., "Outguard: Detecting in-browser covert cryptocurrency mining in the wild", The World Wide Web Conference (WWW), pp.840-852, 2019.
[15] "Browser-based deep behavioral detection of web crypto mining with coinspy", Workshop on Measurements Attacks and Defenses for the Web (MADWeb) 2020, pp. 1-12, 2020.
[16] H. N. C. Neto, M. A. Lopez, N. C. Fernandes and D. M. Mattos, "Minecap: super incremental learning for detecting and blocking cryptocurrency mining on software-defined networking", Annals of Telecommunications, pp. 1-11, 2020.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205183 |

[17] G. Hong, Z. Yang, S. Yang, L. Zhang, Y. Nan, Z. Zhang, et al., "How you get shot in the back: A systematical study about cryptojacking in the real world", Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS), pp. 1701-1713, 2018.
[18] 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", IEEE INFOCOM 2019-IEEE Conference on Computer Communications, pp. 703-711, 2019.
[19] W. Wang, B. Ferrell, X. Xu, K. W. Hamlen and S. Hao, "Seismic: Secure in-lined script monitors for interrupting cryptojacks", European Symposium on Research in Computer Security (ESORICS), pp. 122-142, 2018.
[20] A. Gangwal, S. G. Piazzetta, G. Lain and M. Conti, "Detecting covert cryptomining using hpc", International Conference on Cryptology and Network Security, pp. 344-364, 2020.
[21] M. Musch, C. Wressnegger, M. Johns and K. Rieck, Web-based cryptojacking in the wild, 2018.
[22] H. Darabian, S. Homayounoot, A. Dehghantanha, S. Hashemi, H. Karimipour, R. M. Parizi, et al., "Detecting cryptomining malware: a deep learning approach for static and dynamic analysis", Journal of Grid Computing, pp. 1-11, 2020.
[23] M. Caprolu, S. Raponi, G. Oligeri and R. Di Pietro, Crypto mining makes noise, 2019.
[24] H. Darabian, S. Homayounoot, A. Dehghantanha, S. Hashemi, H. Karimipour, R. M. Parizi, et al., "Detecting crypto mining malware: a deep learning approach for static and dynamic analysis", Journal of Grid Computing, pp. 1-11, 2020.
[25] A. Rossberg, B. L. Titzer, A. Haas, D. L. Schuff, D. Gohman, L. Wagner, et al., "Bringing the web up to speed with webassembly", Commun. ACM, vol. 61, no. 12, pp. 107-115, Nov. 2018.
[26] Webassembly, [online] Available: https://webassembly.org//..
[27] “Understanding Cryptojacking: A Case Study Analysis" by Johnson, R., Smith, J., & Williams, K. (2020)
[28] “Mitigating Cryptojacking Threats: A Comprehensive Approach" by Patel, A., & Gupta, S.(2019)
[29] "The Economic Implications of Cryptojacking: A Case Study Analysis" by Smith, J., Johnson, R., & Williams, K. (2020)
[30] "Cybersecurity Strategies for Mitigating Cryptojacking Risks" by Gupta, S., & Patel, A. (2020)

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details