Cryptojacking: Detection and Prevention Techniques

Ashtha Goyal
Department of computer science & Engineering
Graphic Era Deemed to be University
Graphic Era Hill University
Dehradun, India
goyal.official.21@gmail.com

Priya Matta[*]
Department of Computer Science & Engineering
Tula's Institute
Dehradun, India
mattapriya21@gmail.com
[*]*Corresponding Author*

2023 9th International Conference on Smart Computing and Communications (ICSCC) | 979-8-3503-1409-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICSCC59169.2023.10334975

***Abstract*— Cryptojacking has emerged as a significant cyber security threat in recent years, fuelled by the rise in popularity and value of cryptocurrencies. It refers to the unauthorized use of computing resources to mine cryptocurrencies, such as Bitcoin or Monero, without the knowledge or consent of the device owner. This illicit activity is typically facilitated by injecting malicious code into websites, ads, or software applications, allowing the code to silently run in the background and exploit the device's processing power and energy resources for mining purposes. Cryptojacking can have detrimental effects, including decreased device performance, increased power consumption, and potential financial losses for victims. As a result, researchers and security experts have focused on developing effective detection and prevention techniques to mitigate the risks associated with cryptojacking. These techniques encompass various approaches, such as machine learning algorithms, behavior analysis, network monitoring, and user education. Collaboration among stakeholders, including industry, academia, and policymakers, is also crucial in addressing this evolving threat. Inclusive, understanding, and combating cryptojacking is essential to safeguard computing resources, protect individuals and organizations from financial losses, and ensure a secure digital environment in the face of an ever-changing cyber security landscape.**

Keywords*— *Cryptocurrency Mining, Malware, Coinhive, Browser-based Cryptojacking, Unauthorized Mining.

I. INTRODUCTION

The blockchain-based cryptocurrencies have gained increased attention outside of specialized industries like the banking and business sectors since the 2009 introduction of Bitcoin. Since the majority of financial institutions already recognize cryptocurrencies as a valid form of payment, doing business with them is both easy and commonplace for any end user. With over 2000 active cryptocurrencies and a near to $1 trillion market cap, interest in cryptocurrencies grew significantly in 2017 [1]. According to a recent Kaspersky survey, 19% of people globally have acquired Bitcoin in the past. The act of mining cryptocurrencies with the victim's processing power without their consent is known as cryptojacking. This illegal mining operation significantly reduces the computing efficiency of the victim host and increases electricity consumption at a substantial cost. This unlawful processing power is then converted into cryptocurrency by the attacker. The word used in the literature to characterize the virus employed for this purpose is "cryptojacking."

Due to the availability of ready-to-use in-browser mining script implementations from service providers like CoinHive and CryptoLoot, attackers can easily gain access to a sizeable user base through popular websites.

In a big attack, YouTube combined Google's ad packages with cryptojacking malware [2]. As long as visitors persisted on the appropriate page, the malicious ad package created by their host engaged in unauthorized mining. YouTube and other media content providers are excellent targets for attackers due to their relatively high user engagement, acceptance, and regular time spent on such websites. Another illustration was the finding of cryptojacking malware in a plugin that the UK government made available [3]. This plugin was being used by a large number of legitimate governmental and legitimate non-governmental websites at the time.

There have also been numerous instances when attackers have disseminated cryptojacking software using cutting-edge methods. For instance, during one incident, the experience botnet Vollgar targeted all MySQL data servers globally in order to compromise the admin accounts and insert cryptocurrency miners into those systems [4]. When the Covid-19 epidemic was at its worst, an alternate current occurrence using the Zoom video conferencing platform was recorded. In this case, the attackers merged the Zoom software with a cryptojacking [5] script and disseminated it over a number of file-sharing networks. In other cases, similar to this, hackers implanted and spread cryptojacking software through gaming consoles like the Nintendo Switch [6] and websites like Steam. In addition, according to recent investigations, 1.4 million MikroTik routers were vulnerable to a firmware flaw that could be exploited to inject crypto-mining code into every outgoing web connection [7]. The paper is organized into seven sections. Section I announces cryptojacking malware. In Section II we have a glimpse of the background and motivation behind this work. Section III is related to the associated research work in which we have described all processes that happened in cryptojacking. In Section IV and Section V, we analyze the detection and prevention techniques with associated tools. Section VI has an open research direction based on the recent research work and In Section VII we have concluded the work by portraying the future scope.

II. BACKGROUND AND MOTIVATION

A wider variety of more advanced in-browser miners are emerging. One of the most widely used crypto-mining algorithms, CryptoNight, includes more than 9 variations that were derived from 3 variants. Cryptominers are also written in a wider variety of languages [8]. In-browser cryptominers no longer have to use WebAssembly as their only option. JavaScript (and asm.js) based cryptominers have more chances now that PoW (Proof-of-Work) algorithms are being developed that require less processing. In fact, WebAssembly and JavaScript are already used by miners. Additionally,

979-8-3503-1409-0/23/$31.00 ©2023 IEEE

cryptominers strive to blend into the background by keeping moderate workloads. This is partly due to the severe resource use of earlier iterations of cryptominers, which made consumers aware of them and swiftly delete them. The computing resources are not being forcefully taken over by recent cryptominers [9]. This study briefly describes the blockchain idea and how Bitcoin is mined in blockchain networks in this section. Keep in mind that mining cryptocurrencies are a legal activity that can be profitable [10]. This work first describes how this mechanism functions so that we can see how cryptojacking malware makes use of it.

III. LITERATURE SURVEY

With the surge in cryptocurrency values and the emergence of the Coinhive cryptomining script in 2017, researchers have increasingly focused their attention on cryptomining and cryptojacking. The rise in popularity of these practices has prompted the need for effective detection and prevention methods to halt unauthorized mining activities that exploit computational resources without the users' awareness or consent [11]. Detecting cryptojacking presents a unique challenge compared to traditional malware due to its distinctive characteristics. Unlike conventional malware, cryptojacking operations do not aim to cause harm or gain control over the victim's system; instead, they capitalize on the victim's computational power.

The detection of cryptojacking malware poses unique challenges for traditional malware detection systems. Typically, these systems categorize cryptojacking malware as resource-intensive applications, overlooking their malicious intent. Unlike traditional malware that seeks to cause harm, cryptojacking malware simply exploits computing resources and transmits the resulting hash values to the attacker [12]. Additionally, the integration of cryptojacking scripts into reputable websites further complicates their identification, as users generally trust these sites and do not anticipate unauthorized mining activities on their machines. This adds an element of stealth to cryptojacking attacks, making them harder to detect. Unlike other types of malware that aim to steal sensitive data or disrupt systems, the primary objective of cryptojacking malware is to maintain a covert presence on the infected system to maximize the attacker's profits. The longer the malware goes undetected, the greater the potential revenue for the attacker [13]. These factors significantly contribute to the distinct nature of cryptojacking malware.

A. Blockchain

It is a centralized distributed digital ledger system that stores P2P (peer-to-peer) transactions based on P2P network system participants in an unchangeable manner. A chain of blocks makes up the blockchain framework. Each block in Bitcoin [14] contains two components: the block header and the transactions. Listed below is the content of a block header:

1) *The previous block's hash*
2) *Version*
3) *Timestamp*
4) *Difficulty Target*
5) *Nonce, and the root of a Merkle tree*

Every block is theoretically connected to the one before it to the inclusion of the previous block's hash. It is impossible to update any block's data to this binding. On the other hand, a group of independently confirmed transactions are included in each block's second section. Many studies have examined how Blockchain can be utilized to solve the problems associated with using traditional transactional methods. In order to give a unique means to safeguard data privacy, CrowdBC [15] is an example effort that employs smart contracts to build a reward/penalty system and explores the idea of abstracting a user's real-world identity. In the context of IoT and sensor networks, operates similarly to proposed security techniques based on Blockchain to ensure the validity and integrity of cryptographic authentication data.

B. Cryptocurrency Mining

Cryptocurrency mining refers to the process of validating and verifying transactions on a blockchain network and adding them to the public ledger (the blockchain) by solving complex mathematical problems. Miners use computational power to perform these calculations and, in return, are rewarded with newly minted cryptocurrency tokens [16]. An agreement mechanism, which is typically accomplished through a "Proof of Work" (PoW) protocol, ensures the immutability of a blockchain. The chain of block structure maintains the immutability with each block as well as the immutability with the entire blockchain. In PoW, certain network nodes solve a hashing challenge to produce a distinct hash value, which is then broadcast to all other nodes. The block reward and transaction fees go to the first node to broadcast a valid hash value. In various Proof of Work (PoW) implementations, a crucial step involves checking if a calculated hash value meets a specific difficulty target. If the hash value satisfies the target, it is considered valid and accepted by all participating nodes. The node responsible for discovering the valid hash value is rewarded for its contribution. It's important to note that different PoW systems employ diverse techniques to determine the difficulty target, depending on their specific implementation [17].

C. Target Cryptocurrencies

1) Monero: Monero initially used the CryptoNight algorithm, which was specifically designed to be ASIC (Application Specific Integrated Circuits)-resistant and promote more decentralized mining. However, in 2020, Monero transitioned to the RandomX algorithm [18], which is optimized for CPU (Central Processing Unit) mining and further enhances the network's resistance to specialized mining hardware. Monero offers characteristics that render an attacker undetectable through cryptographic ring signatures [19]. Due to these characteristics of Monero, hackers frequently use their in-browser cryptojacking malware to mine Monero.

2) Bitcoin: It is a public ledger, which allows anyone to view transaction history and balances. All transactions are recorded transparently and permanently on the blockchain, promoting accountability and trust within the network. The immense attention that Bitcoin mining has received in recent years has caused the difficulty goal to rise sharply. The mining structure of Bitcoin allows for the construction and use of specific mining hardware, which is far more powerful and profitable than CPUs and GPUs (Graphics Processing Units). The increasing difficulty target plus the drawbacks of the CPU rendered CPU mining unprofitable [20]. Attackers who conduct in-browser cryptojacking attacks, therefore, do not favor Bitcoin mining.

3) Other Cryptocurrencies: Attackers find cryptojacking appealing because cryptomining can be parallelized across numerous victims. As a result, distributed cryptomining may be supported by cryptocurrency. As a consensus technique, PoW is used by both Monero and Bitcoin. Other cryptocurrencies (as shown in Table I), like Proof of Stake (PoS) and Proof of Masternode (PoM), use various consensus models instead of PoW [21].

TABLE I. ANALYSIS OF TARGETED CRYPTOCURRENCIES FOR MINING

Cryptocurrency	Algorithm	Maximum Supply	Mining Reward	Popular Mining Hardware
Ethereum (ETH)	Ethash (Proof of Stake)	No Maximum supply	Varies(block by block)	GPUs
Bitcoin (BTC)	SHA-256	21 million	Halves every 210,000 blocks	ASICs
Litecoin (LTC)	Scrypt	84 million	Halves every 840,000 blocks	ASICs, GPUs
Monero (XMR)	RandomX	No maximum supply	Varies(block by block)	CPUs, GPUs
Zcash (ZEC)	Equihash	21 million	Varies(block by block)	ASICs, GPUs
Dash (DASH)	X11	18.9 million	Decreases over time	ASICs, GPUs
Ravencoin (RVN)	KawPow	21 billion	Fixed (5,000 RVN) per block	GPUs
Dogecoin (DOGE)	Scrypt	No maximum supply	Varies(block by block)	ASICs, GPUs

D. Cryptojacking Malware Types

To generate Bitcoins and reap rewards, malicious software known as cryptojacking, or cryptocurrency mining malware, exploits the computational resources of victims' devices, including PCs and mobile devices. The life cycle of cryptojacking malware comprises three primary stages: script preparation, script injection, and the actual attack. The script creation and attack phases remain consistent across all variants of cryptojacking malware. However, the script injection phase diverges, involving either local embedding of the script into various applications or injecting the malicious script into both legitimate and illicit websites. Based on this distinction, we categorize cryptojacking malware into two groups: host-based cryptojacking and in-browser cryptojacking. The subsequent subsections provide a detailed breakdown of the life cycles associated with both types of cryptojacking malware [22].

1) In-browser Cryptojacking Malware: Interactive web content can now access the victim's device's CPU and other computing resources thanks to widely used web technologies like JavaScript (JS) and WebAssembly (Wasm). In-browser cryptojacking malware essentially uses these web technologies to access a victim's computer without authorization and mine cryptocurrencies using the victim's CPU and processing capacity [23]. Figure 1 illustrates the script preparation and injection stages involved in in-browser cryptojacking malware. Upon registration (Step 1), the script owner receives pre-configured mining scripts from the service provider, streamlining the process of getting started. The service provider then distributes mining tasks among its customers and later divides the earnings from the mining pool among them (Step 2). Once equipped with the necessary service credentials, the script owner proceeds to incorporate the malicious cryptojacking script into the HTML source code of the targeted website (Step 3). In the subsequent sections, we delve into further elaboration on this approach, as well as explore alternative methods employed in cryptojacking infections [23].

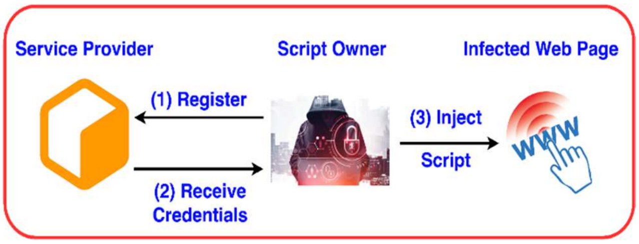

Fig. 1. In-browser cryptojacking malware

Figure 2 outlines the sequential steps involved in a cryptojacking malware attack. Initially, victims access the website source code through their devices (Steps 1 and 2). Subsequently, the web browser loads the website, triggering the immediate execution of the mining script for cryptojacking (Step 3). Once the script runs, it requests mining work from the service provider (Step 4), who then forwards the task request to the mining pool (Step 5). The mining pool assigns the mining duty (Step 6), which is then given back to the mining script by the service provider (Step 7). The victim's computer receives the new mining assignment from the script, prompting the victim's device to commence the mining operation (Step 8). The mining script continues to mine on the victim's computer (Step 9), periodically sending the mining results directly to the service provider as long as there is an active internet connection between the script and the provider (Step 10). The service provider consolidates data from various sources and conveys the findings to the mining pool (Step 11).

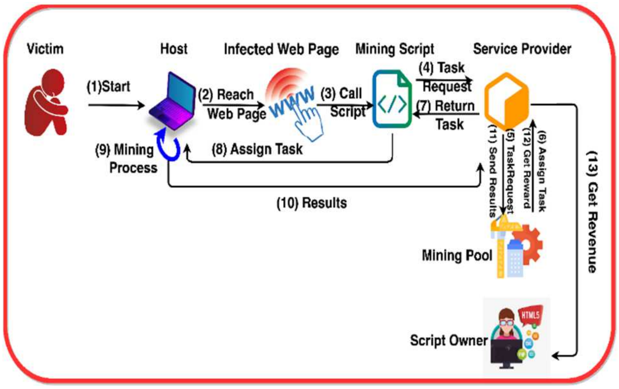

Fig. 2. The life cycle of the In-browser cryptojacking malware

Ultimately, the mining pool distributes the mined funds back to the service provider as payment. After the service provider deducts its service fee, the script owner receives their share from the provider using their service credentials. In this context, the victims [24] do not receive compensation or benefit from any party; instead, the attackers exploit the victims' CPU power.

2) Host-based Cryptojacking Malware: The Hackers employ a surreptitious form of malware known as host-based cryptojacking to exploit a user's host resources, effectively transforming it into a controlled zombie computer under the malware owner's command. Unlike in-browser cryptojacking malware, host-based malware necessitates installation on the victim's machine to gain access to its computational capabilities. These types of malware are commonly delivered to the host system through various means, such as being embedded within third-party applications [25], exploiting system vulnerabilities, or employing social engineering tactics, often concealed as payloads in drive-by downloads.

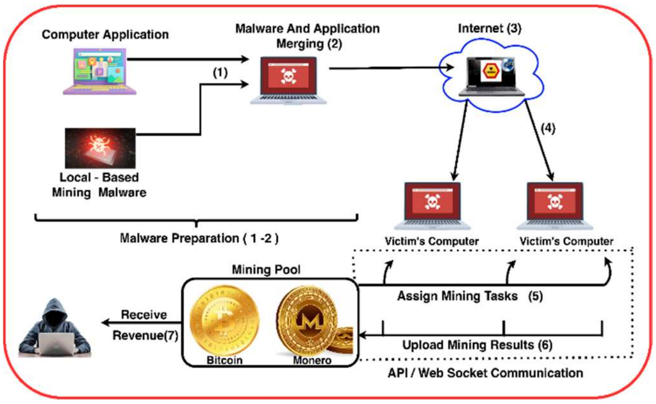
Computer Application
Malware And Application Merging (2)
Internet (3)
(1)
(4)
Local - Based Mining Malware
Malware Preparation (1 -2)
Victim's Computer
Victim's Computer
Mining Pool
Assign Mining Tasks (5)
Receive Revenue(7)
Bitcoin
Monero
Upload Mining Results (6)
API / Web Socket Communication

Fig. 3. Host-based cryptojacking malware

The lifecycle of host-based cryptojacking malware is illustrated in Figure 3. Initially, the unauthorized Bitcoin mining malware is created as part of the script preparation phase (Step 1). To deceive the victim, the attacker merges this malware with a trusted application (Step 2). The injection process begins with the dissemination of the malicious application through online data-sharing platforms like torrents or public clouds (Step 3). The injection phase concludes when the victim downloads and installs any of the infected applications onto their host computers, which could be personal computers, IoT devices, or servers (Step 4). During the attack phase, the host-based cryptojacking malware receives tasks to solve hash puzzles from the mining pool through a web socket or API connection (Step 5). It then sends the computed hash values back to the mining pool (Step 6). Ultimately, the attacker retains the entire profit without expending any energy (Step 7), leaving the victim empty-handed [26]. Upon receiving the cryptocurrency revenue from the service provider, the attacker has three options for utilizing their earnings:

a) Using exchanges or peer-to-peer transactions to convert it to fiat cash;

b) Utilizing it as a service cryptocurrency; or

c) Employing services for blending cryptocurrencies to cover its trail.

The scope of this study does not include additional endwise investigation of the cryptojacking economy and the currency, but similar studies have been done on ransomware [27].

IV. CRYPTOJACKING DETECTION TECHNIQUES AND TOOLS

Detecting cryptojacking activities requires monitoring and analysis of various indicators to identify unauthorized use of computing resources for cryptocurrency mining. Here are some common techniques and tools used in cryptojacking detection as shown in Table II:

TABLE II. DETECTION TECHNIQUES ASSOCIATED WITH TOOLS

Detection Technique	Description	Tools/Approaches
Network Traffic Analysis	Monitoring network traffic for communication with mining pools	Wireshark, Zeek (formerly Bro), Suricata
Endpoint Behavior Analysis	Analyzing processes, system logs, and resource utilization patterns on endpoints to detect suspicious activities related to cryptojacking	Sysmon, OSSEC, Endpoint Protection Software
Unauthorized Mining Scripts	Regular scanning and monitoring of website source code, files, and browser extensions for the presence of unauthorized mining scripts injected into websites or applications	Malwarebytes, NoScript, Chrome/Firefox Dev Tools

V. CRYPTOJACKING PREVENTION TECHNIQUES AND TOOLS

Cryptojacking prevention refers to the measures and strategies implemented to protect against cryptojacking attacks. Cryptojacking prevention aims to safeguard computing resources, such as devices, networks, and websites, from unauthorized use for cryptocurrency mining without the consent or knowledge of the owner [28]. Here are some common techniques and tools used in cryptojacking prevention as shown in Table III:

TABLE III. PREVENTION TECHNIQUES ASSOCIATED WITH TOOLS

Prevention Technique	Description	Tools/Approaches
Regular Software Updates	Keeping all software, including operating systems, web browsers, and plugins, up to date with the latest security patches and updates	Automatic update features, patch management tools
Browser Extensions and Add-ons	Installing reputable browser extensions or add-ons specifically designed to block cryptojacking scripts	MinerBlcok, No Coin, uBlock Origin
Network Traffic Monitoring	Implementing network monitoring solutions to detect and block connections to known cryptojacking domains or IP addresses	Intrusion Detection System (IDS), Security Management and Event Management (SMEM) systems

VI. OPEN RESEARCH DIRECTIONS

By developing more sophisticated and accurate detection methods to identify cryptojacking malware. This could involve the use of machine learning, deep learning, and behavioral analysis techniques to detect malicious patterns and activities associated with cryptojacking. Explore the impact of cryptojacking on Internet of Things (IoT) devices and mobile devices. Investigate the unique challenges and vulnerabilities posed by cryptojacking in these environments and develop effective mitigation strategies. Investigate the usage of zero-day exploits in cryptojacking attacks. Study the techniques used by attackers to discover and exploit new vulnerabilities for mining purposes, and explore ways to detect and prevent zero-day cryptojacking attacks. Explore the potential of utilizing blockchain technology to detect and prevent cryptojacking. Investigate how blockchain can enhance security, transparency, and accountability in detecting and mitigating cryptojacking attacks. Investigate effective strategies for raising user awareness about cryptojacking and promoting safe online behaviours. Study the effectiveness of educational campaigns, training programs, and awareness materials in preventing cryptojacking incidents.

VII. CONCLUSION

Cryptojacking represents a significant and growing threat in the cyber security landscape. It involves the unauthorized use of computing resources to mine cryptocurrencies, resulting in decreased device performance, increased power consumption, and potential financial losses for victims. To combat this threat, researchers and security experts are actively working on detection and prevention techniques, including machine learning algorithms, behavior analysis, and user education. Prevention measures such as regular software updates, anti-malware tools, ad-blockers, and user awareness play a vital role in mitigating the risk of cryptojacking. Collaboration between industry, academia, and policymakers is essential to establish legal frameworks, share threat intelligence, and promote international cooperation. By implementing proactive security practices and staying informed about emerging threats, individuals and organizations can better protect their computing resources and contribute to a safer digital environment for all. It is crucial to remain vigilant and prioritize cybersecurity measures to effectively combat the evolving landscape of cryptojacking attacks.

REFERENCES

[1] A. Marshall, “Combined crypto market capitalization races past $800 bln,” https://cointelegraph.com/news/combined-crypto-mar ket-capitalization-races-past-800-bln, accessed: 2022-07-02.

[2] D. Goodin, “Miners in youtube ads,” https://arstechnica.com/in formation-technology/2018/01/now-even-youtube-serves-ads-wit h-cpu-draining-cryptocurrency-miners/, accessed: 2022-06-13.

[3] Sundaram, B. B., Maurya, S., Karthika, P., & Saraswathi, P. V. (2021, January). Enhanced the Data Hiding in Geometrical image using stego-Crypto techniques with machine laerning. In 2021 6th International Conference on Inventive Computation Technologies (ICICT) (pp. 1141-1144). IEEE.

[4] C. Cimpanu, “A crypto-mining botnet has been hijacking mssql servers for almost two years,” https://www.zdnet.com/article/a-cr ypto-mining-botnet-has-been-hijacking-mssql-servers-for-almo st-two-years/, accessed: 2022-07-02.

[5] Fezzey, T., Batchelor, J. H., Burch, G. F., & Reid, R. (2023). Cybersecurity Continuity Risks: Lessons Learned from the COVID-19 Pandemic. Journal of Cybersecurity Education, Research and Practice, 2022(2), 4.

[6] T. Smith, “Miner found at nintendo switch console,” https://bitc oinist.com/nintendo-switch-game-pulled-over-cryptojacking-co ncerns/, accessed: 2022-07-02.

[7] Hong, G., Yang, Z., Yang, S., Zhang, L., Nan, Y., Zhang, Z., ... & Duan, H. (2018, October). How you get shot in the back: A systematical study about cryptojacking in the real world. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 1701-1713).

[8] Romano, Alan, Yunhui Zheng, and Weihang Wang. "Minerray: Semantics-aware analysis for ever-evolving cryptojacking detection." In 2020 35th IEEE/ACM International Conference on Automated Software Engineering (ASE), pp. 1129-1140. IEEE, 2020.

[9] Jayasinghe, K., & Poravi, G. (2020, January). A survey of attack instances of cryptojacking targeting cloud infrastructure. In Proceedings of the 2020 2nd Asia pacific information technology conference (pp. 100-107).

[10] Xu, G., Dong, W., Xing, J., Lei, W., Liu, J., Gong, L., ... & Liu, S. (2022). Delay-CJ: A novel cryptojacking covert attack method based on delayed strategy and its detection. Digital Communications and Networks.

[11] Tekiner, Ege, Abbas Acar, A. Selcuk Uluagac, Engin Kirda, and Ali Aydin Selcuk. "SoK: cryptojacking malware." In *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 120-139. IEEE, 2021.

[12] Lachtar, N., Elkhail, A. A., Bacha, A., & Malik, H. (2021, June). An application agnostic defense against the dark arts of cryptojacking. In 2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) (pp. 314-325). IEEE.

[13] Ege Tekiner1, Abbas Acar1, A. Selcuk Uluagac1, Engin Kirda2, and Ali Aydin Selcuk3 “cryptojacking malware” https://www.arxiv-vanity.com/papers/2103.03851/.

[14] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system.” 2008.

[15] M. Li et al., “CrowdBC: A Blockchain-Based Decentralized Framework for Crowdsourcing,” IEEE Transactions on Parallel and Distributed Systems, 2019, vol. 30, pp. 1251-1266.

[16] Basha, M., Kethan, M., Karumuri, V., Guha, S. K., Gehlot, A., & Gangodkar, D. (2022, December). Revolutions of Blockchain Technology in the Field of Cryptocurrencies. In 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART) (pp. 761-764). IEEE.

[17] Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y. ACM SIGMETRICS Performance Evaluation Review, 42(3), 34-37.

[18] Sovbetov, Y. (2018). Factors influencing cryptocurrency prices: Evidence from bitcoin, ethereum, dash, litcoin, and monero. Journal of Economics and Financial Analysis, 2(2), 1-27.

[19] M. Mo¨ser, K. Soska, E. Heilman, K. Lee, H. Heffan, S. Srivastava, K. Hogan, J. Hennessey, A. Miller, A. Narayanan et al., “An empirical analysis of traceability in the monero blockchain,” Proceedings on Privacy Enhancing Technologies (PETS), vol. 2018, no. 3, pp. 143–163, 2018.

[20] Dhyani, B., Sharma, S., & Kumar, M. (2022). predictive modelling of select cryptocurrencies and identifying the best suitable model-with reference to arima and anns. Annals of'Constantin Brancusi'University of Targu-Jiu. Economy Series, (6).

[21] H. Darabian, S. Homayounoot, A. Dehghantanha, S. Hashemi, H. Karimipour, R. M. Parizi, and K.-K. R. Choo, “Detecting cryptomining malware: a deep learning approach for static and dynamic analysis,” Journal of Grid Computing, pp. 1–11, 2020.

[22] A. Acar, L. Lu, A. S. Uluagac, and E. Kirda, “An analysis of malware trends in enterprise networks,” in Information Security, Z. Lin, C. Papamanthou, and M. Polychronakis, Eds. Cham: Springer International Publishing, 2019, pp. 360–380.

[23] Eskandari, S., Leoutsarakos, A., Mursch, T., & Clark, J. (2018, April). A first look at browser-based cryptojacking. In 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 58-66). IEEE.

[24] Saad, M., Khormali, A., & Mohaisen, A. (2018). End-to-end analysis of in-browser cryptojacking. arXiv preprint arXiv:1809.02152.

[25] D. Y. Huang, M. M. Aliapoulios, V. G. Li, L. Invernizzi, E. Bursztein, K. McRoberts, J. Levin, K. Levchenko, A. C. Snoeren, and D. McCoy, “Tracking ransomware end-to-end,” in 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018, pp. 618–631.

[26] Hu, X., Shu, Z., Song, X., Cheng, G., & Gong, J. (2021, December). Detecting cryptojacking traffic based on network behavior features. In 2021 IEEE Global Communications Conference (GLOBECOM) (pp. 01-06). IEEE.

[27] “Nocoin: Block lists to prevent javascript miners,” https://github.com/hoshsadiq/adblock-nocoin-list, accessed: 2022-07-02.

[28] Xu, G., Dong, W., Xing, J., Lei, W., Liu, J., Gong, L. & Liu, S. (2022). Delay-CJ: A novel cryptojacking covert attack method based on delayed strategy and its detection. Digital Communications and Networks.