Concordia Institute for Information System Engineering (CIISE)
Concordia University

INSE 6140 Malware Defenses and Application Security

Project Report:

A Survey on Crypto-Mining Malware and Methods of Detecting Cryptojacking

Submitted to:

Professor Dr. Makan Pourzandi

Submitted By:

Student Name	Student ID
Dhruv Haribhakti	40172725
Mahima Shukla	40206690
Aashika Lakhani	40198282

Date
21/04/2023

1. INTRODUCTION

In recent years, cryptocurrencies have become a more widely used method of online payment. Cryptocurrencies are the trendiest development in the field of digital payments as the world economy transitions to a digital era. Cryptocurrencies, in contrast to traditional money, are decentralized, meaning that no single government entity issues them, and they are created expressly for the exchange of digital information. Due to the absence of a third party, this gives users peace of mind and a sense of security when doing transactions. People choose to utilize cryptocurrencies because they are a reliable and secure type of digital currency and because they use encryption for security.

However, with the growing popularity of cryptocurrencies, the usage of crypto mining malware, also known as crypto jacking, has grown along. Once the value of the stake is known, attackers target cryptocurrencies. Hacking the target's computer or mobile phone for the purpose of mining cryptocurrencies against their will is known as crypto jacking. There have been a number of attacks used, such as double spending, transaction malleability, netsplit, networking attacks, and attacks on individual miners and mining pools. It causes systems to slow down, can increase energy costs, and can cause potential harm to the hardware. Due to these security issues and flaws, cryptocurrencies are not used with the same level of trust as traditional forms of money. Therefore, it is essential to identify and stop crypto mining malware in order to protect user confidentiality and security.

The virus that is used for cryptocurrency mining is still a constant threat to people and businesses today. Malware actors utilize a variety of methods, such as phishing, social engineering, and exploiting software flaws, to infect devices with mining malware. They frequently target computers that have inadequate security measures in place, such as obsolete software or weak passwords. According to a Kaspersky analysis, the total amount of potential crypto mining exploits increased by 23% during the first half of 2021 over the same timeframe in 2020. This shows that hackers are still actively attempting to deploy malware that mines cryptocurrency for money.

Cryptocurrency malware can harm victims in a variety of ways. As the malware uses up system resources, it can first result in system slowdowns or crashes. As a result, productivity may suffer or costly hardware changes may be required. The infection can also increase electricity use, which would raise electricity costs. Furthermore, malware that mines for data can jeopardize the compromised system's security. The malware may also install other software, such as spyware or ransomware, which can interrupt system operations or steal sensitive data.

Hence, malware that facilitates cryptocurrency mining has major ethical and legal ramifications. Legally speaking, utilizing another person's computing resources without that person's permission is typically forbidden and may result in both criminal and civil penalties. Malware that uses cryptocurrency to mine is theft from an ethical standpoint. To gain money, the attackers are essentially taking the victim's processing power. Furthermore, mining malware can be used to mine coins with a bad environmental impact, like Bitcoin, which has come under attention for its high energy usage.

To stop and identify cryptojacking, a few techniques have been developed. Antivirus software use, monitoring of networks, browser extensions, and routine programs updates are a few of these techniques. This survey offers a thorough analysis of cryptomining malware and cryptojacking detection techniques. It discusses many varieties of cryptomining malware and how they behave, such as file-based and browser-based miners. The numerous preventative and detection techniques like signature-based detection, behavior-based detection and machine learning-based detection are also covered, along with their advantages and disadvantages. Overall, this report intends to help people and organizations secure their systems and networks from this new threat by fostering a better awareness of cryptomining malware and cryptojacking detection techniques.

2. PAPER CLASSIFICATION

A. Background

Papers [1], [2], [3] and [10] give a brief idea about the background of crypto mining, blockchain and various malware types and how it is spread.

Blockchain is a distributed ledger that uses cryptography to produce immutable records. Verifying and adding transactions to a blockchain ledger is a process known as crypto mining, often referred to as cryptocurrency mining. This is often accomplished by employing specialised computer hardware to solve difficult mathematical equations. Blockchain networks employ the consensus algorithms PoW (Proof of Work) and PoS (Proof of Stake) to verify transactions and uphold the blockchain's integrity. PoS uses the idea of "staking" or retaining cryptocurrency in a wallet as a means of verifying transactions and adding them to the blockchain, as opposed to PoW, which uses computational work to be done.

The lifecycle of cryptojacking malware, which exploits computers to mine cryptocurrency without the user's consent, includes script preparation, injection, and attack phases. It is often divided into two categories: host-based cryptojacking and in-browser cryptojacking. Malware techniques which include in-browser mining scripts, malware, social engineering, malicious ads and browser extensions, and drive-by download are ways and tactics used by crypto mining malware to infect target computers and mine cryptocurrency.

B. Detection and Prevention Methods

Papers [4] through [9] explain about the various preventive measures to be taken as well as the detection methods for cryptojacking malware.

Utilizing ad blockers and anti-malware software, updating software and browser extensions, and being aware of fraudulent emails, links, and downloads are some preventative ways to avoid cryptomining malware. Monitoring CPU utilization and device performance on a regular basis may assist in identifying and stopping unauthorized cryptocurrency mining.

The various detection methods include:

a) Miner Behavior Graph:
It includes maintaining a watch on a network's cryptocurrency miners to look for unusual activities. Anomalies like unexpected increases in mining activity can be found and evaluated as possible cryptojacking malware by setting a baseline of expected behaviour and comparing it to current activity.

b) Network metadata:
It examines network traffic to spot trends and indicators connected to cryptocurrency mining, like connections to mining pools, well-known mining programs, or C2 servers. This strategy can assist in finding and preventing crypto mining malware before it reaches target devices.

c) CPU usage metrics:
It includes observing a device's CPU utilization for any unexpected spikes or extended periods of high consumption that can point to cryptocurrency mining activity.

d) Machine learning models:
Some commonly used models that can detect mining malware by analyzing various features of the system or network traffic are:

1) **Logistic Regression:** It is a statistical model that analyses cryptojacking malware traits and forecasts the risk of infection to estimate the probability of a binary outcome.

2) **C4.5:** An approach for building decision trees that uses entropy-based splitting criteria by training on known malware behaviors and applying the resulting model to fresh data.
3) **CART (Classification and Regression Trees):** It is a different decision tree algorithm that may be applied to regression and classification. It can recognize crucial characteristics and categorize mining malware according to those characteristics.
4) **Random forest:** It classifies data using numerous decision trees, and by training on a large dataset of network and system activity and applying the resulting model to categorize new data as either malware or not.

e) **Deep learning models:** It uses neural networks to analyze huge datasets of features related to cryptomining malware to construct the below mentioned models:
1) **LSTM:** Long Short-Term Memory. A sort of neural network with recurrent features that can be applied to the detection of malware by looking at sequential data, like network activity or log files, to find patterns and abnormalities connected to cryptojacking malware.
2) **Att-LSTM:** Attention based LSTM. By weighing the significance of various features and concentrating on the most pertinent features for classification, it is an LSTM model with an attention mechanism.
3) **CNN:** Convolutional Neural Network. A particular kind of neural network that looks at image-based information, like screenshots of malware activity, to find patterns and features connected to the malware.
4) **FCNN:** Fully Connected Neural Network. Studies a huge dataset of features tied to malware, and then applies the learned model to categorize fresh data as either cryptojacking malware or not.

C. Case study

References [18], [19] and [20] were used to present a case study on the recent attacks on cryptomining malware and cryptojacking.

a) **Medical Technology Company Targeted by Monero Cryptominer Concealed in WAV Files:** A medical technology business was the target of an attack in June 2022 that used well-obfuscated malware to infect Windows 7-based PCs and spread throughout the network. The attack used a Monero cryptominer that was hidden inside WAV files. When Guardicore Laboratories and their MSSP Blue Bastion were contacted for incident response, they were able to stop the malicious processes and remove the malware by deleting the binary payloads using their Centra platform, registry dumps, forensics images, and network service logs.

b) **LemonDuck Cryptomining Botnet Targeting Docker on Linux Platforms:** LemonDuck, a well-known botnet that targets Docker on Linux platforms, operates infected containers through an accessible Docker API using a modified ENTRYPOINT, and it avoids detection by employing a crypto mining proxy pool and seeking for SSH keys rather than scanning IP ranges. leveraging signed images, avoiding mining software in built images, leveraging authentication for Docker APIs, and keeping an eye out for rogue containers and high CPU usage are some mitigation techniques.

D. Impact of Crypto mining malware and future trends:

Papers [11] through [16] have been useful in knowing more about the impacts of cryptomining malware, how ransomeware is related to cryptojacking, what are the different kinds of crypto ransomeware attacks and what are the future trends in cryptomining malware.

Reduced device performance, higher electricity costs, weakened device security, and potential hardware damage are all effects of crypto mining malware. Because some ransomware attacks incorporate crypto mining software as an additional payload to make cash while the victim's files are encrypted, crypto mining malware and ransomware are connected[13]. Both kinds of malware have the

potential to seriously harm a victim's device and data, and attackers may additionally demand payment for the release of critical information, adding another level of complexity to the attack. Protection against all forms of malware, including ransomware and crypto mining malware, is therefore crucial.
The two upcoming trends—smart contracts and quantum computing—could influence the creation and dissemination of crypto mining malware. Smart contracts may have security flaws that hackers might leverage to run harmful code, whereas quantum computing may be exploited to create more sophisticated malware that is more difficult to stop. As a result, it's crucial for consumers and businesses to keep informed about these trends and take precautions to shield their devices and networks from malware of all kinds, including malware that mines cryptocurrency.

3. SYNTHESIS/ DISCUSSION

A. Background

Through a decentralized network called the blockchain, cryptocurrencies are digital assets that use encryption to offer a secure channel for transactions. Blockchain is a distributed ledger that creates immutable records with cryptography. Blockchain's decentralized structure makes it very secure and resistant to change. Because of their quick block times, blockchains have high transaction speeds, which leads to quicker transactions. On the other hand, cryptomining is the process of adding new transactions to the blockchain by employing specialized computer gear to solve challenging mathematical problems. As a compensation for validating and adding transactions to the blockchain, this process is often referred to as "mining" because it entails the generation of new bitcoin units.
To mine cryptocurrencies, there are two methods: joining a mining pool and solo mining. To boost their chances of effectively mining cryptocurrencies and earning rewards, miners form mining pools to pool their processing resources. To solve a mathematical puzzle and add a new block to the blockchain when mining alone, a miner must compete with other miners. However, each participant that joins a mining pool gives the pool a piece of their processing power. After a block has been successfully mined, the rewards are divided up among the pool's participants based on their contributions. In this manner, miners can still share in the reward depending on their contribution to the pool even if their processing power is insufficient to solve the puzzle and mine a block. Joining a mining pool has several advantages, including a steadier income stream, a smaller chance of not receiving any rewards owing to bad luck, and access to superior tools and knowledge. The necessity to have faith in the pool operator to distribute the profits properly and increased fees are a few drawbacks[3].

PoW (Proof of Work)

To stop system misuse, cryptocurrency systems employ the notion of proof-of-work (PoW). The system needs the computer requesting the service to perform computational effort, often in the form of processing time. PoW, which was developed by Cynthia and Moni in 1993, is distinguished by an imbalance between the computing effort itself and its validation. Similar to a CAPTCHA[1], PoW is made for people to solve rather than machines. Some of the pros and cons of PoW are:

Pros:

- Provides a high level of security since validating a block involves a significant amount of computing work.
- Miners are encouraged to engage and maintain the network since they will be compensated for their efforts.
- Has a long history of successful implementation, and Bitcoin and other significant cryptocurrencies use it as their consensus mechanism.

Cons:

- Requires a lot of energy and computing power, which can be expensive and have a bad effect on the environment.
- Can result in the concentration of mining power due to the advantages enjoyed by larger and better-equipped miners over smaller ones.
- It is possible for one miner or a small group of miners to control a majority of the network's mining power in a 51% attack.

PoS (Proof of Stake)

In contrast to the proof-of-work (PoW) system, which chooses the owner of the next block based only on the amount of computational work they complete, the proof-of-stake (PoS) system chooses the owner based on an amalgamation of selection at random and their stake in the system. PoW is still used even though PoS is thought to be more energy efficient than PoW because it offers a better consensus on which computer should build the next block. Most well-known cryptocurrencies either employ PoW or a hybrid PoW/PoS mechanism[10]. The advantages and disadvantages are listed below:

Pros:

- More energy efficient than PoW, as it does not require extensive computational work.
- Prevents mining power from being centralized because it does not compensate miners according to their computational ability.
- Increases the difficulty of a single entity controlling the network, which lowers the likelihood of 51% exploits.

Cons:

- Because it depends more on participant wealth than on the quantity of computational labor done, PoS can be less secure than PoW.
- Are vulnerable to "nothing-at-stake" attacks, in which validators are motivated to validate several chains at once.
- Can result in a concentration of wealth among participants because those with the largest stakes benefit from the network.

Given that both PoW and PoS have advantages and disadvantages, it is difficult to declare with certainty which is preferable. The ideal consensus mechanism ultimately depends on the objectives and needs of the network in question. To combine the advantages of PoW and PoS, several cryptocurrencies have even begun to utilize a hybrid strategy.

Cyber Kill Chain for a basic Cryptomining malware

The cyber kill chain is a framework for describing the several phases of a cyberattack, from the first stage of data exfiltration to the last stage of initial reconnaissance.

The attacker first conducts reconnaissance to learn more about the network and systems of the target. The next step is to develop a payload containing the crypto mining virus and distribute it to the target through phishing emails or software exploits. The virus then installs itself and starts mining cryptocurrency using the target system's resources after finding security holes in the target's systems to get access.

By connecting to the malware through a C2 server, the attacker can manipulate and keep an eye on it from a distance. To continue mining cryptocurrency, the software is made to stay on the target system despite removal attempts.

When the attacker succeeds in mining cryptocurrencies, they may keep using the virus to acquire more money or move on to a different target.

Several methods and tools, including network traffic analysis, endpoint detection and response (EDR) solutions, and behavioral analysis, must be used to find crypto mining malware. Security experts can put methods in place to recognize and stop crypto mining malware assaults by knowing the stages of the Cyber Kill Chain[17].

Organizations can better understand the many stages of an attack and learn how to prevent or lessen the effects of such attacks on their systems by applying the Cyber Kill Chain paradigm to cryptomining malware. It deconstructs the many phases of an attack and provides knowledge of how the malware is supplied, executed, and maintained, and can assist in identifying and stopping the spread of such malware.

Malware Types

For every type of cryptojacking malware, the script preparation and attack phases of its lifecycle are the same. In contrast, the script injection phase involves either locally embedding the malware into other apps or injecting the malicious script onto the websites[2]. As a result, we divide the cryptojacking virus into two groups:

1) **In-browser Cryptojacking:** It happens when a website secretly mines cryptocurrency in the victim's web browser by running a script. In most cases, this kind of attack is carried out by inserting JavaScript code into a webpage, which then runs in the background as the user browses the website.

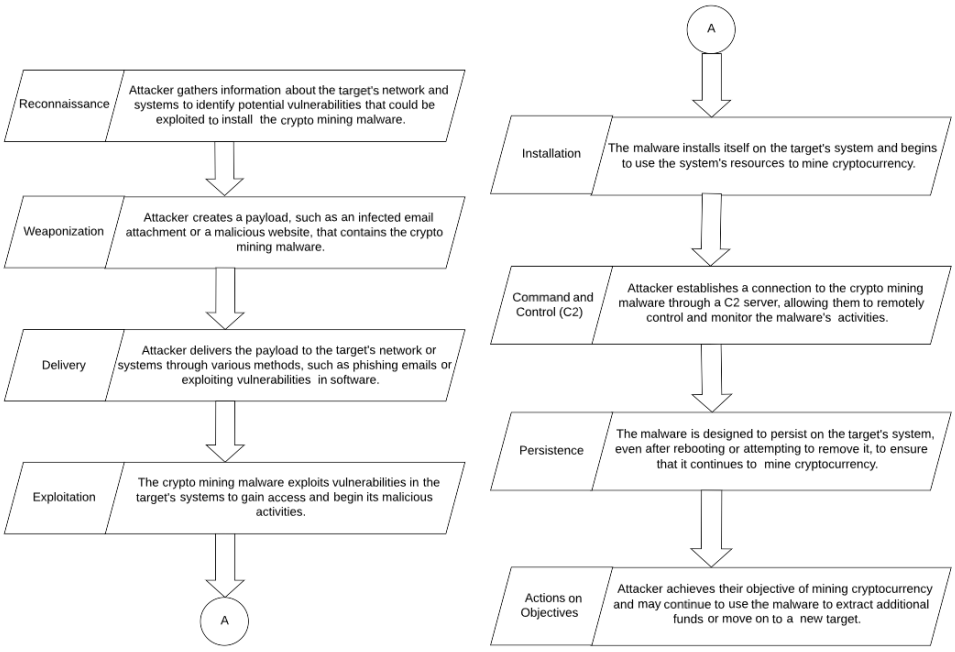


Fig 1. Cyber Kill Chain for a basic crypto mining malware

2) **Host-based Cryptojacking:** Host-based cryptojacking installs malware on the victim's computer or server to mine cryptocurrency.

The main differences between these two malware types are:

1) ***Execution Method:*** While host-based cryptojacking requires malware to be installed on the victim's computer or device, in-browser cryptojacking is carried out through a script that runs on a website.
2) ***Impact:*** In contrast to host-based cryptojacking, which can result in more serious hardware damage and higher electricity costs, in-browser cryptojacking often has less of an impact on the victim's device performance and energy usage.
3) ***Detection:*** Because the consumer can observe the unusually high CPU utilization or hear their device's fan running more frequently, in-browser cryptojacking is simpler to identify. Because malware may be made to conceal itself and elude antivirus programs, host-based cryptojacking is more challenging to identify.
4) ***Persistence:*** When a user navigates away from a website or closes it, in-browser cryptojacking comes to an end. On the other hand, host-based cryptojacking can go on mining bitcoin even if the victim's device is not in use or their browser is closed.
5) ***Mitigation:*** While host-based cryptojacking requires the removal of the virus, which can be challenging and time-consuming, in-browser cryptojacking can be halted by simply closing the infected page.

Hence, users should take care to avoid both types of cryptojacking malware such as utilizing antivirus software and staying away from fraudulent websites and downloads, to prevent them.

Cryptojacking Malware Techniques

The various techniques used the cryptojacking malware are listed below[2]:

1) **Malvertising:** Online ads that contain hidden code to mine cryptocurrency on the victim's device without their knowledge or consent are known as malicious ads. The victim's computer's processing power is used to run the code when they click on these adverts, which makes their system slower. Attackers can easily and swiftly spread crypto mining malware to a large user base by using malicious advertising.

2) **Phishing emails:** Cryptojacking is frequently distributed using phishing emails. Attackers persuade the victim to click on a link or download an attachment that contains the virus by sending fake emails that look to be from reliable sources. The malware mines cryptocurrency for the attacker using the victim's device's processing power after it has been installed. Phishing emails are typically quite successful because they can deceive people into willingly installing malware, frequently without realizing it.
3) **Social engineering:** Cryptojacking is distributed using the social engineering technique, which deceives victims into installing the virus on their devices. Attackers may use a variety of strategies, including impersonating a reliable person or organization, promising fictitious prizes or incentives, or employing fear tactics, to persuade the victim to download and install the malware. Because it relies on preying on human emotions and behavior, social engineering-based cryptojacking can be very difficult for users to recognize and avoid.
4) **Drive-by download:** Drive-by download is a method that infects victims' devices via a compromised website or web application. The virus is automatically downloaded and placed on the victim's device without their knowledge or agreement when they access the website or use the application. Drive-by download-based cryptojacking can be quite efficient because it can quickly and efficiently infect a huge number of users, frequently without requiring any user interaction or download.
5) **Malicious browser extensions:** Malicious extensions are installed in victims' web browsers as part of a tactic to spread cryptojacking malware. After being installed, the extension runs in the background and mines cryptocurrency for the attacker using the device's processing power. Malicious browser extensions can be spread through several techniques, such as social engineering tricks or by taking advantage of weaknesses in authorized extensions. This method can be very successful because extensions are simple to install and allow access to a lot of data on the victim's device.
6) **Watering holes:** A method known as a "watering hole" involves infecting a victim's device with cryptojacking malware through a compromised website that the victim frequently visits. By inserting malicious code into a website that the victim is likely to visit, the attacker compromises it. Watering hole-based cryptojacking can be quite successful since it targets particular people or groups and can rapidly and easily infect many users.
7) **IoT Botnets:** By infecting the devices with malware and setting up a network of remote-controllable bots, the attacker takes control of the machines. Each device in the botnet adds its processing power to the mining operation, which is subsequently utilized to mine cryptocurrency. Because it may infect a huge number of devices and utilize them to create sizable sums of cryptocurrency, botnet-based cryptojacking can be quite efficient.

B. Detection and Prevention Methods

Detecting web-based and host-based crypto mining malware can be challenging, since the malware is designed to run silently in the background without the victim's knowledge. However, there are a few detection methods that can be used:

1) **Miner Behavior Graph:** It uses a graph-based methodology to examine miner behavior, locate communication patterns, and produce a graph that depicts the interaction between miners and mining pools[4].
2) **Network Metadata:** Based on an examination of network traffic produced by the malware, this detection technique is used[9]. It comprises gathering and analyzing a range of network data, including NetFlow, DNS logs, HTTP logs, and other metadata that can be used to identify the presence of malware that mines cryptocurrency.
3) **CPU Usage Metrics:** Monitoring a system's CPU utilization to look for any unusual spikes or persistently high consumption patterns that can point to the presence of malware that mines cryptocurrency is known as detection with CPU usage metrics[6].

All three methods of detecting crypto mining have their own strengths and weaknesses. Here is a comparison among them:

	Advantages	Disadvantages
Miner Behavior Graph (MBG)	• Can detect web-based and binary-based malware. • Can detect new variants. • Can identify multiple components like C&C. • Generates graphical representation for easy interpretation.	• Requires sufficient amount of data for training. • May produce false positives or false negatives depending on the training dataset.
Network Metadata	• Can detect different types of propagation methods. • Can detect connections to known mining pools or C&C. • Can be used to stop further propagation.	• Require specialized tools to monitor the Network traffic. • Limited to network-based detection. • Cannot detect malware with obfuscating techniques.
CPU Usage Metrics	• Can be effective for the web-based malware. • Can be used to find new variants. • Real-time detection.	• Can have many false positives when a system uses high CPU usage for other purpose.

Table 1. Comparison between MBG, Network metadata and CPU usage metrics

Other than these three detection methods, machine learning and deep learning models can also be used to detect mining malware.

Machine learning models: These models are used to detect malware by analyzing various features of the system or network traffic[7].

	Advantages	Disadvantages
Logistic Regression	• Straightforward and easy to understand. • Rapid prediction and training. • Effectively manages massive volumes of information.	• Possibly not effective with large data sets. • It could be difficult to handle changeable relationships that are not linear[5]. • May be ill-fitting or excessively ill-fitting.
C4.5	• Handles both continuous and categorical information. • Simple to comprehend and apply. • Capable of handling missing data.	• May produce a lot of rules and overfit the data. • Possibly less effective with unbalanced data. • The data may not handle noise efficiently.
CART	• More rapid than C4.5 • Able to manage a lot of data. • Can process both continuous and categorical data	• May produce a lot of rules and overfit the data. • Possibly less effective with unbalanced data. • Possible poor handling of missing data.
	• Greater precision and less risk of	• High computational costs

Random Forest	overfitting compared to individual decision trees. • Can handle both continuous and categorical data. • Capable of handling missing data.	• Possibly need further data to train the model. • Is sometimes more challenging to interpret than other models.

Table 2. Comparison between different machine learning models

Deep learning models: These models are used to detect malware in network traffic[8].

	Advantages	**Disadvantages**
LSTM	• Capable of handling consecutive data. • Able to identify long-term dependencies. • Ability to handle input sequences of varying length. • Can benefit from information both present and future.	• Can be computationally expensive and poor to train. • It can need additional data to train. • It might experience disappearing or expanding gradients when training.
Att-LSTM	• Capable of handling consecutive data. • Able to identify long-term dependencies. • Can concentrate on pertinent elements of the input sequence. • Ability to handle input sequences of varying length.	• Can be computationally expensive and poor to train. • It can need additional data to train. • It might experience disappearing or expanding gradients when training.
CNN	• Capable of handling spatial data. • Can handle enormous amounts of data, • Can automatically extract features, • Can be computationally effective	• Sequential data might not be handled correctly. • Possibly misses long-term dependencies. • Possibly sensitive to the incoming data's size and orientation.
FCNN	• Can handle both continuous and categorical data. • Can handle data with high dimensions. • Possibly computationally effective • It might be simple to deploy and train	• Maybe incapable of handling spatial or sequential data • Long-term dependencies or spatial connections might not be captured. • Possibly need further data to train the model

Table 3. Comparison between different deep learning models

C. Case Study

This case study presents two of the recent attacks on cryptomining malware and cryptojacking.

1) Medical Technology Company Targeted by Monero Cryptominer Concealed in WAV Files

A well-obfuscated malware attack that concealed a Monero cryptominer inside WAV files was launched against a medium-sized medical technology company in June 2022. The hacker used the infamous EternalBlue vulnerability to travel laterally via the company's network and infect

computers running Windows 7. To investigate and stop the attack, Guardicore Laboratories provided incident response solutions[18].

Detection: On October 14, BSODs were discovered on several Windows workstations, which prompted the company to approach Guardicore Laboratories and their MSSP Blue Bastion for an investigation. Kernel memory dumps, which would have been helpful for forensic investigation, could not have been saved by the machines' configuration. But in addition to those resources, the investigation also used the Guardicore Centra platform, registry dumps, forensics pictures, and network service logs and discovered that one of the computers had run a prolonged command line that accessed suspicious data in a registry key.

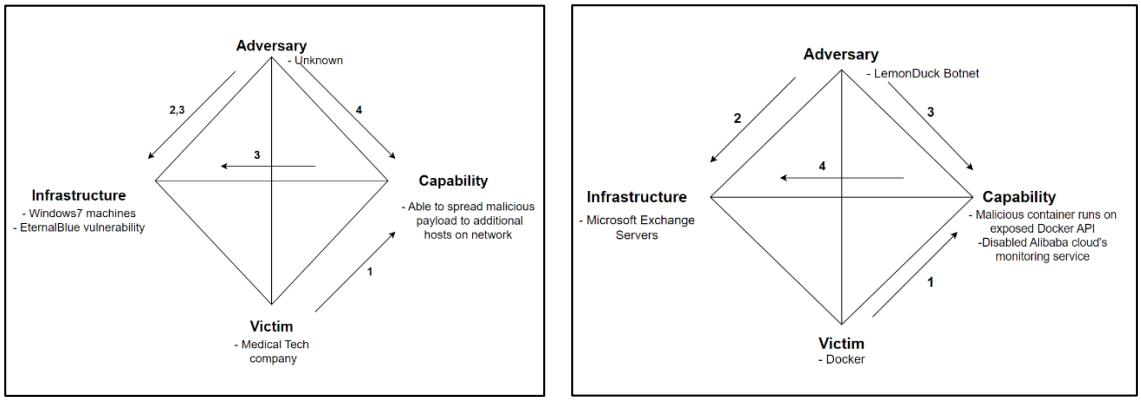
Further, it was found that the attackers had exploited EternalBlue to spread laterally via the network and had run subnet scans on port 445 to disseminate the malicious payload to more hosts. The malware payload was reverse engineered by Guardicore Laboratories, who discovered a multi-layered executable file.

Mitigation: The malware was eliminated, the malicious processes were stopped, and the registry keys containing the binary payloads were deleted to end the attack.

Here is a diamond model for intrusion analysis for this attack:

I. The victim had the capability to find the multilayered executable file. This file was found by Guardicore Laboratories by reverse engineering the malware payload.
II. The adversary ran subnet scans on port 445 to spread malicious payload to the infrastructure.
III. The adversary used EternalBlue vulnerability to spread laterally through the network.
IV. The adversary was able to spread malicious payload to additional hosts on the network

.



(a) (b)

Fig 2. Diamond Model for Intrusion Analysis

2) LemonDuck Cryptomining Botnet Targeting Docker on Linux Platforms

The CrowdStrike Cloud Threat Research[20] team identified LemonDuck as a well-known bitcoin mining botnet that targets Docker on Linux platforms in early 2021. In addition, the botnet is well-known for attacking Microsoft Exchange servers using ProxyLogon and exploiting flaws like EternalBlue and BlueKeep to mine cryptocurrencies, get elevated privileges, and move laterally within infected networks. LemonDuck seeks to make money off its work by running several campaigns at once and mining different cryptocurrencies like Monero.

Attack Method: While LemonDuck utilises a modified ENTRYPOINT to download and operate infected containers via an exposed Docker API, Docker APIs help automation. By using a crypto mining proxy pool to conceal its wallet address, it avoids discovery by looking for SSH keys rather than scanning IP ranges. It executes scripts using discovered SSH keys to access servers. Additionally, it avoids discovery by targeting and deactivating Alibaba Cloud's monitoring service.

Mitigation: The following actions are advised to stop LemonDuck and related botnets from penetrating cloud environments: Use only signed images from reputable registries, steer away from adding mining software or SSH keys in built images, utilise authentication for Docker APIs, and keep an eye out for rogue containers and high CPU consumption[19].
Here is a diamond model for intrusion analysis for this attack:

i. The victim has the capability to identify the malware.
ii. The attacker targets Microsoft Exchange Servers via ProxyLogon.
iii. The attacker has the capability to make money off its operations by running several active mining operations for cryptocurrencies.
iv. Multiple campaigns are running on multiple C2 servers targeting Linux and Windows.

D. Impact of cryptomining malware and future trends

Because cryptocurrencies are anonymous, cybercriminals target them, leading professionals to create defences against such attacks. Malware that mines cryptocurrency can significantly affect how well a system uses its resources. This is because the malware mines cryptocurrencies using the device's computing power, which can suck up a lot of resources[12]. As a result, the system may operate much more slowly, resulting in delays and maybe crashing some programs. In addition, excessive processing power utilization might lead to overheating and hardware damage, which could be expensive to fix. Additionally, because the device requires more power to operate, the victim may incur greater electricity costs because of the increased resource utilization. The malware may also be used by the attacker to steal confidential data from the victim's network or device[11]. These kinds of attacks offer serious risks to users of cryptocurrencies, both personally and professionally, because they can lead to financial losses, data breaches, and reputational harm. Because of the rising use of cryptocurrencies and the relative simplicity of executing these attacks, cybercriminals have found them to be lucrative and appealing. As a result, crypto-mining malware can have a negative impact on how much system resources are used, thus it's crucial to take precautions against infection and eliminate the malware as soon as it's found[14].

Future Trends: These are the possibilities that can happen in the near future.

1) ***Smart Contracts:*** Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. They can be used to facilitate the implementation of agreements, enhancing the security and efficiency of transactions. But they are vulnerable to security flaws because attackers can leverage these smart contracts by injecting harmful code within their code to distribute cryptomining malware. Then, without the victim's knowledge or cooperation, they can remotely control the infected devices and mine cryptocurrencies using their processing power.
2) ***Cryptovirology:*** Cryptovirology is the study of how harmful software, such as crypto-mining programmes and ransomware attacks, uses cryptography[15]. These exploits have the potential to decrease system performance, utilise more energy, and harm hardware. Recent developments have produced sophisticated tactics and equipment that enable attackers to execute more harmful operations. To identify and stop these attacks, researchers are creating new defences and instruments, like machine learning algorithms and blockchain-based solutions. To keep one step ahead of the attackers, however, ongoing research and development are required due to the continually developing nature of these threats.
3) ***Quantum Computing:*** A type of computing known as quantum computing manipulates data using quantum-mechanical phenomena like superposition and entanglement. Compared to conventional computers, quantum computers have the capacity to solve difficult mathematical problems more quickly, making them potentially useful for breaking encryption schemes and jeopardizing the security of cryptocurrencies. In order to get access to and steal the digital currencies kept in cryptocurrency wallets, it can also be used to make private keys for those wallets. Attackers may employ quantum computing to create new, more advanced crypto

mining malware that is more difficult to identify and protect against if it becomes more generally available[16].

4. CONCLUSION

As a trustworthy and secure form of digital money, cryptocurrencies have grown in popularity. However, their use has also led to an increase in crypto mining malware, also known as cryptojacking, which is a persistent threat to consumers and businesses. Malware actors employ a variety of techniques to infect devices with mining malware, degrading the victim's system performance, consuming excessive amounts of electricity, and possibly jeopardizing their security. To safeguard user privacy and security, it is crucial to recognize and slow down these virus attacks. Thus, to assist people and organizations in securing their systems and networks against this new threat, this report offers an analysis of various cryptomining malware and cryptojacking detection techniques, including signature-based detection, behavior-based detection, and machine learning-based detection.

5. CONTRIBUTION TABLE

Name	Tasks
Dhruv Haribhakti	Cryptomining (theory), Types of malware Evaluations of current solutions New approaches or solution for prevention
Mahima Shukla	Methods of implementation Effects of cryptojacking New approaches or solution for prevention
Aashika Lakhani	Old methods of detection Problems faced New approaches or solution for prevention

6. REFERENCES

[1] Navamani, T. M. 'A Review on Cryptocurrencies Security'. Journal of Applied Security Research, vol. 18, no. 1, Jan. 2023, pp. 49–69. Taylor and Francis+NEJM, https://doi.org/10.1080/19361610.2021.1933322.

[2] Tekiner, Ege, et al. 'SoK: Cryptojacking Malware'. 2021 IEEE European Symposium on Security and Privacy (EuroS&P), 2021, pp. 120–39. IEEE Xplore, https://doi.org/10.1109/EuroSP51992.2021.00019.

[3] Pastrana, Sergio, and Guillermo Suarez-Tangil. A First Look at the Crypto-Mining Malware Ecosystem: A Decade of Unrestricted Wealth. 2019. DOI.org (Datacite), https://doi.org/10.48550/ARXIV.1901.00846.

[4] Zheng, Rui, et al. 'Cryptocurrency Mining Malware Detection Based on Behavior Pattern and Graph Neural Network'. Security and Communication Networks, edited by Chunhua Su, vol. 2022, Mar. 2022, pp. 1–8. DOI.org (Crossref), https://doi.org/10.1155/2022/9453797.

[5] Alqahtani, Abdullah, and Frederick T. Sheldon. 'A Survey of Crypto Ransomware Attack Detection Methodologies: An Evolving Outlook'. Sensors, vol. 22, no. 5, Feb. 2022, p. 1837. DOI.org (Crossref), https://doi.org/10.3390/s22051837.

[6] Gomes, Fabio, and Miguel Correia. 'Cryptojacking Detection with CPU Usage Metrics'. 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA), IEEE, 2020, pp. 1–10. DOI.org (Crossref), https://doi.org/10.1109/NCA51143.2020.9306696.

[7] Pastor, Antonio, et al. 'Detection of Encrypted Cryptomining Malware Connections With Machine and Deep Learning'. IEEE Access, vol. 8, 2020, pp. 158036–55. DOI.org (Crossref), https://doi.org/10.1109/ACCESS.2020.3019658.

[8] Darabian, Hamid, et al. 'Detecting Cryptomining Malware: A Deep Learning Approach for Static and Dynamic Analysis'. Journal of Grid Computing, vol. 18, no. 2, June 2020, pp. 293–303. Springer Link, https://doi.org/10.1007/s10723-020-09510-6.

[9] Detection of Illicit Cryptomining Using Network Metadata. 1 July 2021, https://doi.org/10.21203/rs.3.rs-607598/v1.

[10] Hajri, Haitham Hilal Al, et al. 'Crypto Jacking a Technique to Leverage Technology to Mine Crypto Currency'. International Journal of Academic Research in Business and Social Sciences, vol. 9, no. 3, Mar. 2019, pp. 1220–31. hrmars.com, https://hrmars.com/index.php/IJARBSS/article/view/5791/Crypto-Jacking-a-Technique-to-Leverage-Technology-to-Mine-Crypto-Currency.

[11] Zimba, Aaron, et al. 'Crypto Mining Attacks in Information Systems: An Emerging Threat to Cyber Security'. Journal of Computer Information Systems, vol. 60, no. 4, July 2020, pp. 297–308. Taylor and Francis+NEJM, https://doi.org/10.1080/08874417.2018.1477076.

[12] Kulandei, Berlin, and Dhenakaran S.S, 'Impact of Crypto-Mining Malware on System Resource Utilization'. INTERNATIONAL JOURNAL OF COMPUTER SCIENCES AND ENGINEERING, Feb. 2019

[13] Wecksten, Mattias, et al. ‘A Novel Method for Recovery from Crypto Ransomware Infections’. 2016 2nd IEEE International Conference on Computer and Communications (ICCC), IEEE, 2016, pp. 1354–58. DOI.org (Crossref), https://doi.org/10.1109/CompComm.2016.7924925.
[14] Badawi, Emad, and Guy-Vincent Jourdan. “Cryptocurrencies Emerging Threats and Defensive Mechanisms: A Systematic Literature Review.” IEEE Access, vol. 8, 2020, pp. 200021–37. DOI.org (Crossref), https://doi.org/10.1109/ACCESS.2020.3034816.
[15] Zimba, Aaron, et al. ‘Recent Advances in Cryptovirology: State-of-the-Art Crypto Mining and Crypto Ransomware Attacks’. KSII Transactions on Internet and Information Systems, vol. 13, no. 6, June 2019, pp. 3258–79. itiis.org, https://itiis.org/digital-library/manuscript/2420.
[16] Kappert, Noah, et al. Quantum Computing – The Impending End for the Blockchain? Article in Collected Edition, Pacific Asia Conference on Information Systems (PACIS), 2021.
[17] Dargahi, Tooska, et al. ‘A Cyber-Kill-Chain Based Taxonomy of Crypto-Ransomware Features’. Journal of Computer Virology and Hacking Techniques, vol. 15, no. 4, Dec. 2019, pp. 277–305. DOI.org (Crossref), https://doi.org/10.1007/s11416-019-00338-7.
[18] Guardicore Labs Team. “A Medical Technology Company Targeted by Monero Cryptominer Concealed in WAV Files.” Threats Making WAVs - Incident Response to a Cryptomining Attack, 2021, https://www.akamai.com/blog/security/threats-making-wavs-incident-reponse-cryptomining-attack.
[19] Pereira, Brian. “LemonDuck Cryptomining Botnet Targeting Docker on Linux Platforms.” LemonDuck Malware Evolves Into Major Cryptomining Botnet, 22 Apr. 2022, https://www.bankinfosecurity.com/lemonduck-malware-evolves-into-major-cryptomining-botnet-a-18947.
[20] Ahuje, Manoj. “LemonDuck Cryptomining Botnet Targeting Docker on Linux Platforms.” LemonDuck Targets Docker for Cryptomining Operations, 21 Apr. 2022, https://www.crowdstrike.com/blog/lemonduck-botnet-targets-docker-for-cryptomining-operations/.