A Survey of Attack Instances of Cryptojacking Targeting Cloud Infrastructure

Keshani Jayasinghe
University of Westminster
No 115, New Cavendish Street,
London, UK
+94 (0) 77 1925654
w1628078@my.westminster.ac.uk

Guhanathan Poravi
Informatics Institute of Technology
No 57, Ramakrishna Road,
Colombo 6, Sri Lanka
+94 (0) 77 342330
guhanathan.p@iit.ac.lk

ABSTRACT

Cryptojacking is the act of using an individual's or an organization's computational power in order to mine cryptocurrency. In some scenarios, this can be considered as a monetization strategy, very much similar to advertisements. But to do so without the explicit consent of the computer owners is considered illegitimate. During previous years, attackers' focus was heavily laid on browser-based cryptojacking. However, it was noted that the attackers are now shifting their attention to more robust, more superior targets, such as cloud servers and cloud infrastructure. This paper analyses 11 forms of practical scenarios of cryptojacking attacks that are targeted towards cloud infrastructure. We carefully look at their similarities and properties, comparing those features with the limitations of existing literature regarding the detection systems. In this paper, we survey the attack forms, and we also survey the limitations of existing literature as an attempt to outline the research gap between the practical scenarios and existing work.

CCS Concepts

• Security and privacy → Intrusion/anomaly detection and malware mitigation • Security and privacy → Malware and its mitigation

Keywords

Cryptojacking; Cryptocurrency; Monero; Mining; Cloud Security; Malware Detection

1. INTRODUCTION

The concept of thievery has existed since the existence of civilization itself. As society became increasingly complex and sophisticated, so did theft and attacks. The introduction of network and technology has not decreased crime and threats, but only moved the criminals to a newer platform for their crimes [25]. Cybercriminals' complex attack models are powered by a range of inventions and technologies. These tools and technologies allow them anonymity, shielding and means of profits. While these technologies have not been developed with the intention of cybercrime, criminal misuse is widespread and unswerving. Cryptocurrencies have grown to be a massive financial field, with the USD market capitalization of $225B currently [8]. That, combined with the potential growth and complete anonymity offered, has caught the attention of many malicious players, with cryptojacking being one of the more up and coming illicit methods of accumulating cryptocurrency at the expense of its victims.

Cryptojacking can be roughly defined as the *"unauthorized use of victim computing resources to mine and exfiltrate cryptocurrencies"* [25]. It can be considered as a form of malware, which is a harmful piece of software designed specifically to infect or cause damage to computers, servers and networks. In order to mine cryptocurrency effectively so as to earn a profit, dedicated hardware such as GPUs (Graphics Processing Units) and ASICs (Application Specific Integration Circuits) are required. Some of those who are not willing to acquire said hardware reach out for other illegitimate methods of obtaining computational resources to mine cryptocurrency for themselves, as given as below [8, 24]:

- Browser-based cryptojacking
- Malicious browser extensions
- Cryptojacking via Android apps
- ISP and public router hijacks
- Compromised third-party libraries
- Botnet based cryptojacking
- Cryptojacking the Internet of Things
- Compromised cloud servers, breaches, and injections

Browser-based cryptojacking became massively popular with malicious actors in the years 2017 and 2018, with services such as Coinhive providing straightforward means to monetize visitor's computational resources via mining [23]. While this service was expected to be used legitimately, attackers were quick to deploy Coinhive miners without user consent, thus illegally exhausting the victim's resources for personal gain [8]. Browser-based cryptojacking surged to unprecedented levels in December 2017, where Symantec claims to have blocked 8 million cryptojacking events and TrendMicro Annual Report for 2017 [29] showing more than 45,000,000 cryptocurrency mining events. A recent RedLock report states that around 25% of the organizations experienced cryptojacking in their cloud servers during 2018 [7, 12, 27]. With the shutdown of Coinhive and the price drop of Monero, cryptojacking attacks have slightly diminished [24], although the attacks and attack variants remain still at large. With small mining operations, such as browser-based and android

APIT 2020, January 17–19, 2020, Bali Island, Indonesia
© 2020 Association for Computing Machinery.
ACM ISBN 978-1-4503-7685-3/20/01…$15.00
DOI: https://doi.org/10.1145/3379310.3379323

based cryptojacking, being relatively unprofitable, attackers have begun to explore more complex and sophisticated forms of attack, seeking larger payoff with lesser time. One of the more prevailing cryptojacking methods that were observed to be growing was through targeting cloud infrastructure. Cloud servers and infrastructure, often found under-protected and comprising of vulnerabilities, are posing as extremely appealing targets for any attacker searching for robust and unrestrained CPU power. For cryptojacking attackers, the cloud is a goldmine [9, 12, 18, 22]. Mentioned below are several effects that follow attackers and victims of cryptojacking specifically targeting cloud servers and infrastructure.

Benefits of Cryptojacking in Cloud for Attackers

- Considerably greater CPU resources for a bigger payoff
- Larger attack surface
- Spreading capabilities within the network
- Accessing data and credentials in cloud servers
- Ability to backdoor the server and leave it more vulnerable for future attacks
- More reliable than depending on a network of browsers

Adverse Effects of Cryptojacking in Cloud for Victims

- Substantial damage to the servers
- Large resource consumption bills
- Device performance, degradation, and malfunction
- High priority organizational tasks and real processes cease to operate or lowered in priority

This paper produces a comprehensive analysis in which different features and properties of practical attack forms are summarized. We also present a review of existing literature and a form of comparison between the existing work with the attack details in order to outline the research gap.

2. ATTACK INSTANCES TARGETING CLOUD SERVERS AND INFRASTRUCTURE

2.1 Attack Instances

Table 1 lists down a set of cryptojacking attacks that have occurred targeting cloud servers and infrastructure and their properties.

2.1.1 Smominru

As a malware that propagates via EternalBlue exploit, Smominru has infected over 90,000 devices within August 2019, from countries including China, Taiwan, Russia, Brazil and U.S. It was observed that Smominru downloads a malicious payload once it has completed successful infection of a device, and this payload downloads a valid NVDIA CUDA library. This library helps the miner to take full advantage of the parallel processing abilities of the GPU and mine at full capacity to maximize payoff. It was detected that Smominru included modules for other malicious activities such as spying, data exfiltration and theft of credentials. It was specifically noted that this attack infrastructure is distributed widely, with complex architecture and very high flexibility, all characteristics making it a challenging task to detect or dismantle [20, 26].

2.1.2 CryptoSink

CryptoSink is another attack instance that utilizes XMRig, an open source mining algorithm, to mine for Monero. By focusing on both Windows and Linux platforms, this miner has exploited an Elasticsearch system vulnerability (CVE-2014-3120) in order to target Elasticsearch systems. It infects victim devices by sending malicious HTTP requests, and once a target device is found, it either downloads an executable directly (Windows) or uses '*curl*' and '*wget*' to download a bash script, which then downloads a binary file that includes the miner, a malware to backdoor the server, a service to redefine the system's '*rm*' command and a watchdog functionality for the attackers' purposes. The '*rm*' command was rendered powerless as it was overwritten to re-download the malware file each time the command was run. It was discovered by the F5 network researchers that this malware uses a unique technique of terminating existing or competing miners on the system by redirecting them to the localhost [6, 35].

2.1.3 Zealot

Researchers at F5 Labs, a company focused on researching security and threats, considers Zealot to be a very sophisticated and a highly obfuscated attack [3]. Zealot was found to be using the exploits EternalBlue and EternalSynergy to spread across networks. It leverages Apache Struts Jakarta Multi-parser vulnerability (CVE-2017-5638) and DotNetNuke Content Management System vulnerability (CVE-2017-9822) in order to propagate within the internal networks by sending HTTP requests. Zealot, like most malicious miners, was seen to be mining Monero with an algorithm dubbed 'mule', by specifically targeting vulnerable Apache Struts servers. For Windows, it uses an obfuscated PowerShell agent, and for Linux based systems, a Python agent is used, and both seem to be based on EmpireProject post-exploitation framework. This attack was noted for its complexity and its multi-staged execution.

2.1.4 Adylkuzz

Very much similar to Smominru and Zealot, this malware also spreads from victim to victim by using the EternalBlue exploit. It targets Windows based corporate LANs (Local Area Networks), servers and wireless networks, specifically in Russia, Ukraine, Taiwan, Brazil and India to mine for Monero in large scale. A noticeable feature in this malware form is its ability to shut down the SMB (Server Message Block) network in order to stop further malware infection on the device [15].

2.1.5 WannaMine

First reported in October 2017, this mining malware was leveraging the Oracle WebLogic Server Remote Vulnerability (CVE-2017-10271) along with Eternal- Blue. At the time of discovery, the miner has attacked more than 75,00 devices including domain controllers and endpoints. WannaMine was observed to be utilizing live-off-the-land technologies such as Windows Management Instrumentation (WMI) and PowerShell for propagation and execution. Ping- Castle scanner is also used to map the network and find best possible potential target device. [32]

Table 1. Summary of Attack Instances Targeting Cloud Servers And Infrastructure

Attack Instance/Name	Discovered Date	Platform	Currency /Amount	Vulnerability / Exploit	Victim	Tools/ Technology
Smominru	January 2018	Windows Server 2003, 2008, 2012 & Windows XP & 7	Monero (Amount: $1.5m)	EternalBlue exploit	Almost 90,000 devices	NVIDIA CUDA API,
CryptoSink	March 2019	Windows/ Linux	Monero (Amount: $4,500)	Elasticsearch system vulnerability	Elasticsearch Systems	XMRig Miner, Windows CertUtil, '*curl*' & '*wget*' commands
Zealot	March 2017	Windows/ Linux	Monero (Amount: $8,500)	-	Vulnerable Apache Struts servers	Mule cryptomining malware, '*Nohup*', '*curl*' & '*wget*' commands, TCP for communication, PowerShell, EmpireProject
Adylkuzz	May 2017	Windows	Monero (Amount: $22,000)	EternalBlue	Corporate LANs, servers and wireless networks	DoublePulsar
WannaMine	October 2017	Windows	Monero	EternalBlue exploit, Oracle WebLogic Server Remote Vulnerability	More than 75,000 devices since 2017	WMI, Powershell, PingCastle
RubyMiner	January 2018	Windows/ Linux	Monero	Multiple vulnerabilities in HTTP web servers	Web servers - Almost 700 servers worldwide (PHP servers, IIS servers, Ruby on Rails servers)	XMRig Miner
Tesla Attack	February 2018	AWS hosted Kubernetes server	-	Lack of password protection	Tesla's Kubernetes Console	CloudFlare
JenkinsMiner	February 2018	Windows/ Linux	Monero (Amount: $3M)	Jenkins Serialized Object vulnerability	Jenkins CI server	XMRig Miner, PowerShell, Remote Access Trojan
Coinreg Monero	March 2018	Windows	Monero	-	South American offices of an auto maker	Coinreg Monero, Mimikatz, Powershel, XOR encryption
Norman	August 2019	Windows	Monero	-	Servers and workstations of the attacked network	UPX obfuscated XMRig Miner, DuckDNS, NSIS compilation, Agile Obfuscator
Graboid	October 2019	Containers in Docker Engine	Monero	Unsecured Docker daemon & endpoint protection software limitations	More than 2000 unsecured Docker hosts	XMRig algorithm

2.1.6 RubyMiner

Almost 700 web servers worldwide, including PHP servers, IIS servers and Ruby on Rails servers, were attacked by the RubyMiner, which made use of the victims' resources to mine for Monero. RubyMiner attack uses the XMRig Miner algorithm, which the attacker injects to the victim devices by exploiting multiple HTTP web server vulnerabilities.

2.1.7 Tesla Attack

A cyber-attack that became famous recently was the cryptojacking attack on Tesla's Kubernetes Console, which was hosted on an AWS server. The primary reason for this attack was identified as the Kubernetes console not being password protected. In order to evade detection, the attackers have avoided using well known mining algorithms. Attackers also avoided directing the network to a mining pool, and instead opted for installing mining pool software which then collected to a semi-public endpoint. CloudFlare was used by the attackers to hide the real IP address of the mining pool. Attackers have also kept the CPU usage moderate, in order to avoid detection. It was observed that apart from mining, the attacker also gained access to credentials for other environments including an Amazon S3 bucket, while the Kubernetes Console was compromised. [5, 12, 13]

2.1.8 Jenkins Miner

Dubbed as one of the biggest cryptojacking operations by CheckPoint [10], the attackers of this cryptojacking malware have used a combination of Remote Access Trojan (RAT) and XMRig Miner to attack Jenkins CI servers running Windows or Linux platforms. It was found that over $3 million were mined through this cryptojacking attack form. Jenkins Miner exposed the Jenkins Java Serialized Object vulnerability (CVE-2017-1000353) in order to get the victim devices to accept the requests. [5]

2.1.9 Coinreg Monero

Coinreg Monero miner and Mimikatz was used on a 2 wave attack that utilized living- off-the-land tools in order to propagate the network. Encoded PowerShell scripts were used to introduce malicious payload to victim devices. Mimikatz was mainly used to gather credentials which will be useful later in order to read and write encrypted payloads to the registry keys of the victim network. It was also found that the attacker was uploading stolen data, possibly credentials, to a public cloud storage provider. [20]

2.1.10 Norman

This cryptojacking attack was discovered by the Varonis Security Research team. Norman was found to be using the XMRig Miner to attack at a large scale by targeting all servers and workstations of the infected network. Miner relies on DuckDNS for communication purposes and the mal- ware archive was compiled using NSIS (Nullsoft Scriptable Install System). This archive consisted of a DLL file, payload information and NSIS modules. The DLL file was built with .NET and was found to be triple obfuscated using Agile .NET Obfuscator. Layers of obfuscation has provided this malware added protection against detection. [30]

2.1.11 Graboid

This was a cryptojacking attack targeting Docker Engine Containers. Unit 42 of Palo Alto Networks found that this malware has attacked more than 2000 Docker hosts by compromising unsecured Docker Daemons. It was noted that traditional endpoint protection tools do not inspect activities nor data within containers, which was a key security limitation. This cryptojacking malware propagates by downloading the payload as well as a list of potential targets, from which 3 are picked at random while executing the cryptomining algorithm, XMRig Miner. [4]

2.2 Overview of the Attack Instances

As stated above, 11 large scale, harmful cryptojacking attacks targeting cloud infrastructure and servers were analyzed comprehensively. It was found that these attacks share many similarities and common elements. It was observed that the majority of the attacks were done targeting Windows Platform, as depicted by Figure 1.

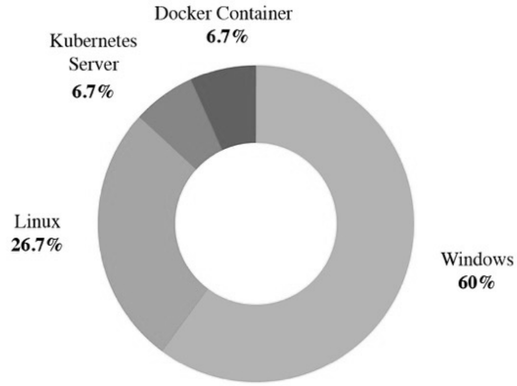

Figure 1. Categorization of Target Platforms

2.2.1 XMRig Miner

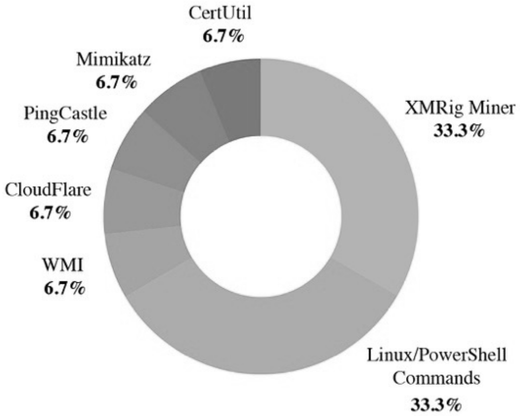

Figure 2. Categorization of Tools Used

While examining the attack details, as categorized in Figure 2, it was clearly noted that the majority of the attacks have made use of the Monero CPU miner, XMRig, which is available free and open source [34]. Symantec has categorized this miner as a "potentially unwanted application" [16]. Although its targeted for Windows operating system, the attackers have modified the application to be run on Linux platforms at times. It also redirects 5% of the payoff made to the original developer's XMR wallet ID. However, this is optional and can be disabled through the source code.

2.2.2 Living-off-the-land Tools and Techniques

The concept of Living off the Land techniques is the usage of tools that are already installed on the target devices by attackers to serve their malicious purposes. This can be observed on the analyzed cryptojacking attacks. Threat actors are using legitimate system tools, such as PowerShell and Windows Management Instrumentation (WMI), which are whitelisted and helps the attackers to avoid detection. A categorization of legitimate tools utilized by the analyzed attack instances is depicted by Figure 2. These tools are mainly used in order to administrate the network, monitor the system behavior and communicate with command and control (CC). Fileless attacks (discussed later) are also considered as a subcategory of Living off the land attacks. [1, 27]

2.2.3 Fileless Technique

Fileless infection technique is an attack form in which the malware is not written to the disk. Instead it will reside within the volatile memory. Above mentioned cryptojacking attacks were not seen to directly write an executable to victim's device. In its place, the payload will acquire the mining script from the CC using PowerShell in most instances. These downloaded scripts and executables will reside in the memory, and will perform an in-memory execution. [14, 27]

2.2.4 EternalBlue Exploit

EternalBlue is an exploit that was developed by NSA and leaked by The Shadow Brokers group. This exploitation is based on multiple vulnerabilities, including the Server Message Block (SMB) protocol. SMB is a network communication protocol in Windows OS. This exploit allows attackers to remotely execute code and gain access to a network. This exploit was famously utilized in WannaCry attacks, as well as a multitude of cryptojacking attacks that were previously analyzed in this paper. [17, 19]

2.2.5 Additional Damage

It must be noted that while analyzing the above attacks, majority of the them were aiming to not only mine cryptocurrency from the victim devices but also to establish backdoors, install spyware, data exfiltration and mainly, to steal credentials. Such instances, it was found that the attackers will gather sensitive credentials which will be uploaded to cloud servers for further usage.

3. EXISTING APPROACHES OF DETECTION

While there are plenty of anti-virus and malware detection solutions that exist in a product level, those failed to detect complex and organized attacks. By analyzing the above instances, it is apparent that the attackers have gone through levels of obfuscation and sophistication to achieve their malicious goals with no discovery. With the increase of complexity of their attack models, security scholars have identified this as opportunity to research and develop better, more resilient and accurate detection systems of cryptojacking. Laid out below is a brief analysis of the existing work that has been recognized to detect malicious threat actors cryptojacking cloud infrastructure.

Table 2. Summary of RADS: Real-Time Anomaly Detection System for Cloud Infrastructures

Research	**RADS: Real-Time Anomaly Detection System for Cloud Infrastructures [2]**
Introduction	Anomaly detection system for DDoS (Distributed Denial of Service) and cryptojacking attacks in real- time. This research solution is categorized into 2 phases: • Using OCC (One Class Classification) algorithm to learn the "normal" CPU and network traffic patterns • Combines Window Based Time Series Analysis to lower the false positive rate. Authors justifies the use of OCC for anomaly detection by pointing out the lack of data for the "negative" class or the anomalous class. Lays heavy emphasis over detection while experiencing short momentary workload "spikes" in the server. The authors try to detect both DDoS and cryptojacking attacks in the same intensity with no separation of parameters or detection notifications.
Algorithm/ Technique	One Class classification algorithm, Window Based Time series analysis with average and standard deviation of data.
Technologies	Java for the module, Apache Common Maths and Weka libraries
Limitations	• Classifies both DDoS and cryptojacking as an anomaly, and does not differentiate between the two. • High CPU utilization is used to detect crypto- jacking while high network traffic is used to detect DDoS attacks. Network traffic impacts on cryptojacking is not considered. • Negative class data used for the training model are generated by simulating an attack with a CPU stress tool. • Processing time of the detection system in- creases exponentially with increasing number of virtual machines. • Additional damage (such as spyware, back- doors, data and credential theft) are not considered as a part of the detection.
Assumptions	Assumes that the cryptojacking attacks will consume significant CPU power in a constant manner, and simulates the attack by running a CPU stress tool at 100%.

The Table 2 gives a summary of the work done by Barbhuiya et al. [2]. The authors aim to detect both DDoS and cryptojacking attacks by analyzing network traffic and CPU utilization respectively. The largest drawback of this detection system is that the author does not try to differentiate and classify DDoS and cryptojacking attacks, nor are the datasets and the classification models for the attacks separately. This ignores the obvious observation of how accurate it is to detect DDoS attacks solely based on network traffic while detecting cryptojacking exclusively based on CPU utilization. The authors have used One Class Classification to build the classification model, and due to the lack of negative data, the authors develop artificial negative data. This artificial negative data is gathered by emulating cryptojacking attacks using a CPU stress tool at 100%. CPU stress tool is a workload generator. It is unrealistic to assume that cryptojacking attacks behave in similarity to a workload generator that is configured at 100%, especially since sophisticated cryptojacking attacks are throttling resource utilization levels. No network traffic parameters were noted as a feature. Additionally, other damages such as installed spyware, data and credential theft, backdoors are not considered to be a part of the detection system, and hence will not be detected nor accounted for. Performance of this technique mentioned as lightweight by the author. However, with a high number of virtual machines, the training time will increase exponentially.

Table 3. Summary of Mining On Someone Else's Dime: Mitigating Covert Mining Operations in Clouds and Enterprises

Research	**Mining on Someone Else's Dime: Mitigating Covert Mining Operations in Clouds and Enterprises [28]**
Introduction	Hardware based behavioral monitoring tool that detects cryptojacking with micro-architectural execution patterns – namely, Hardware Performance Counters (HPC). This solution is divided into 3 components: • Profiler – Analyses virtual machines and polls HPC every 2 seconds • Detection Agent – Runs HPC values against the trained classifier and receives the detection status • Mitigation Agent – Suspects the virtual machine if cryptojacking detection is positive Utilizes a range of mining and non-mining signatures as features to train the model, while accounting for the noise generated from virtualization. The authors express that profiling has a higher accuracy when taking the algorithm and algorithm behavior into account rather than the syntax. The authors also discover that mining algorithms run a set of computations repeatedly in a consistent manner, and that various mining coins have overlapping behavior signatures. Evaluated using precision, recall and F- score.
Algorithm/ Technique	Tests against K-Nearest Neighbor, Multi-Class Decision Trees and Random Forest Algorithms. Elects Multi-Class Random Forest algorithm with 50 Decision Trees.
Technologies	C++ for the module, Python and Bash, Perf/Perf-KVM and '*nvprof*' for CPU/GPU monitoring
Limitations	• Additional damage (such as spyware, back- doors, data and credential theft) are not considered as a part of the detection. • Attackers maintain a throttle level to avoid detection, which was not considered. • It is possible to artificially manipulate HPC to avoid detection • Can be avoided by even slightly changing cache probing patterns of the algorithm [28]

As represented by Table 3, Tahir et al. [28] introduces this detection mechanism based on Hardware Performance Counters (HPC), which records low-level micro-architectural events. However, mentioned below are several limitations and drawbacks in using HPC with machine learning to detect malware:

- Gathering HPC in virtual machines are unreliable, since HPC counters are already in motion in virtual machines, so that trying to extract the counters utilizes HPC itself [36].
- Using measured HPC traces from the same program for both training and testing datasets is unrealistic since polymorphic malware constantly changes.

Apart from the limitations that are imposed with HPC analysis, attackers can also avoid detection with:

- Strong code obfuscation
- Artificially manipulating HPC levels
- Introducing a reasonable throttle level [28]

The most prominent drawback noticed on this detection system is the lack of including Monero as a cryptocurrency that is frequently being mined. Monero, being one of the most untraceable coins, is being used for cryptojacking in a notable scale, as observed above. While it is unsure whether the algorithm that majority of the analyzed attackers have used (XMRig Miner) will be detected with the single use of HPC in virtual machines, author's heavy focus lies on the general cryptocurrencies such as Bitcoin. It must be understood that Bitcoin miners and Monero miners work differently. Additionally, as same as [28], this system does not recognize further damage to the system, which may include spyware, backdoors, and credential theft, as a part of the detection, and thus, will not provide a method to detect or validate these.

4. EXPLORATION OF RESEARCH GAP

It can be understood that cryptojacking is a different form of malware attack in which the attackers will steal the victim's computational resources in order to run a mining algorithm that will mine Monero on behalf of the attacker. This attack form should not be taken lightly since it has caused considerable amount of damage including hardware degradation, loss of credentials, backdoors and rather large electricity and resource consumption bills. Cryptojacking, as mentioned above in this paper, is known to use successful and complicated evasion techniques in order to circumvent security measures. Thereafter, existing literature was also studied, in which 2 robust detection systems were identified that, to the best of our knowledge, dealt with cryptojacking attacks specifically targeting cloud infrastructure. However, there is a gap that was noticed between the academic literature and practical indications.

Firstly, it should be mentioned that code obfuscation is a simple yet quite effective technique utilized by the attackers. This prevents reverse engineering, keyword based detection techniques and pattern matching tools as noted by [21]. Apart from that, dead-code injection is another technique used to attain similar results as [11] states. In this paper, it was observed that some of the cryptojacking malware attacks delivered obfuscated payloads and scripts. Normal and Zealot attacks predominantly stands out in this regard, as they were both perceived to be using layers of obfuscation.

Similarly, attackers also employee proxies and URL randomization in order to bypass blacklisting. Blacklisting is a classic robust detection system employed by virus guards. While this technique has proven itself, there are various techniques to bypass blacklist based systems as mentioned above. [11, 31]

One of the most noticeable characteristics of a cryptominer is the CPU utilization it affects. Although the miners find it profitable to use all 100% of their available resources, this tends to raise alarms and detection systems, which is why most miners have employed a throttle level. XMRig Miner specifically can be customized to use a preferred number of cores, maximum CPU usage and CPU priority. With these configurations, an attacker can mine Monero without making much noise in the background.

While surveying the practical attack scenarios, we observed that the usage of living-off-the-land techniques and fileless attacks were common. These techniques are considered to be stealthy, as they are using whitelisted system tools to hide their malicious behavior under the routine system behavior.

These system tools and command line alterations will not be detected by automated sensors, and hence provides a shield for the attackers against detection systems. This also includes having no conspicuous binaries written to the victim's disks and executing remote scripts. Wueest and Anand [33] mention in a Symantec Internet Security Threat Report that this form of technique may even evade signature detection systems if the attacks were to obfuscate scripts. Hence, we can presume that traditional static detection solutions are unreliable in identifying to such attacks. Likewise, there are a few limitations observed in the reviewed literature, as drafted in more detail above. In [2], heavy weightage of the detection system lays on CPU metrics. This can be thwarted with CPU throttling, which can be adjusted through the XMRig configurations. Similarly, [28] proposed solution of using Hardware Performance Counters is unreliable, given that fact that Tahir et al. assumes that cryptojacking takes place with CPU and GPU capacities being pushed to their limit. In that case, we can consider that CPU metrics is a core factor.

Based on the above conclusions, we presume that techniques such as blacklisting and CPU based classification to be inefficient in detecting cryptojacking accurately, as sophisticated attacks are under the protection of the above mentioned evasion approaches. Hence, with the survey of attacks and the review of literature, it can be concluded that the reviewed literature is not adequate, since the adoption of whitelisted system administration tools and remote code executions were not considered in the said literature.

It is evident that this sophisticated evasion technique should be considered when seeking for further detection models for cryptojacking. It can be concluded that further research is required that takes fileless malware and living-off-the- land techniques into account in detecting cryptojacking for cloud servers and infrastructure. We plan to further investigate this problem by researching more deeply into dynamic, behavioral based detection systems and particularly focusing on the drawbacks of the current approaches.

5. LIMITATIONS OF THE SURVEY

Several limitations of this survey should be mentioned. A total of 11 cryptojacking attack instances were surveyed. These attack instances were selected based on their threat level and the level of information available. The literature that were reviewed were the only literature that were found upon our research that concerns the detection of cryptojacking in a cloud infrastructural level. Other works may have exceeded our scope or was not included due to the lack of information available. Furthermore, product level detection solutions were not considered as a part of this survey.

6. CONCLUSION

Cryptojacking, a form of malware that steals victims' computational resources, is targeting servers and cloud infrastructure. This paper presents this dilemma in 4 components: introduction to the domain, analysis of attack instances, a survey of existing literature and a review of research gaps. All 11 recent attack instances were carefully analyzed in the aspects of the target platforms, vulnerabilities exploited and tools utilized. Findings of the analysis were proven useful in identifying common elements between the attacks, which might further be of help to researches who continue to work on this predicament in the future. Furthermore, existing literature were evaluated in terms of their techniques, technologies and limitations. Thereafter, a comprehensive review of research gaps concerning this problem was outlined.

The future work on this research will be to research the development of a cryptojacking detection system particularly focusing on cloud infrastructure and environment. The main idea is to utilize behavioral analysis techniques to monitor system behavior at a hypervisor level. The behavioral analysis techniques will be particularly oriented towards fileless malware behaviors and living-off-the-land attack behaviors.

7. REFERENCES

[1] Alzuri, A. et al. The Growth of Fileless Malware. 5.

[2] Barbhuiya, S. et al. 2018. RADS: Real-time Anomaly Detection System for Cloud Data Centres. *arXiv:1811.04481 [cs]*. (Nov. 2018).

[3] Beware of Attackers Stealing Your Computing Power for their Cryptomining Operations: 2018. https://www.f5.com/labs/articles/threat-intelligence/beware-of-attackers-stealing-your-computing-power-for-their-cryptomining-operations.html. Accessed: 2019-11-17.

[4] Chen, J. 2019. Graboid: First-Ever Cryptojacking Worm Found in Images on Docker Hub. *Unit42*.

[5] Cryptojacking and Crypto Mining - Tesla, Kubernetes, and Jenkins Exploits: 2018. *https://neuvector.com/container-security/cryptojacking-crypto-mining-tesla-kubernetes-jenkins-exploits/*. Accessed: 2019-11-16.

[6] "CryptoSink" Campaign Deploys a New Miner Malware: 2019. https://www.f5.com/labs/articles/threat-intelligence/-cryptosink--campaign-deploys-a-new-miner-malware.html. Accessed: 2019-11-05.

[7] ESET 2019. *Cybersecurity Trends: 2019*.

[8] Eskandari, S. et al. 2018. A First Look at Browser-Based Cryptojacking. *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (London, Apr. 2018), 58–66.

[9] IBM 2019. IBM X-Force Threat Intelligence Index 2019. (2019), 36.

[10] Jenkins Miner: One of the Biggest Mining Operations Ever Discovered: 2018. https://research.checkpoint.com/jenkins-miner-one-biggest-mining-operations-ever-discovered/. Accessed: 2019-11-17.

[11] Konoth, R.K. et al. 2018. MineSweeper: An In-depth Look into Drive-by Cryptocurrency Mining and Its Defense. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security - CCS '18* (Toronto, Canada, 2018), 1714–1730.

[12] Lessons from the Cryptojacking Attack at Tesla: 2018. https://redlock.io/blog/cryptojacking-tesla. Accessed: 2019-10-17.

[13] Making it Rain - Cryptocurrency Mining Attacks in the Cloud: https://www.alienvault.com/blogs/labs-research/making-it-rain-cryptocurrency-mining-attacks-in-the-cloud. Accessed: 2019-11-07.

[14] Mansfield-Devine, S. 2017. Fileless attacks: compromising targets without malware. *Network Security*. 2017, 4 (Apr. 2017), 7–11. DOI:https://doi.org/10.1016/S1353-4858(17)30037-5.

[15] Meet Adylkuzz: Cryptocurrency-mining malware spreading using the same exploit as WannaCry: 2017. https://blog.avast.com/meet-adylkuzz-cryptocurrency-mining-malware-spreading-using-the-same-exploit-as-wannacry. Accessed: 2019-11-17.

[16] Miner.Xmrig | Symantec: https://www.symantec.com/security-center/writeup/2018-061105-4627-99. Accessed: 2019-11-18.

[17] MS-ISAC 2019. *EternalBlue*. Technical Report #SP2019-0101. MS-ISAC.

[18] Nahmias, D. et al. 2019. TrustSign: Trusted Malware Signature Generation in Private Clouds Using Deep Feature Transfer Learning. *2019 International Joint Conference on Neural Networks (IJCNN)* (Budapest, Hungary, Jul. 2019), 1–8.

[19] Nakashima, E. and Timberg, C. NSA officials worried about the day its potent hacking tool would get loose. Then it did. 5.

[20] O'Gorman, B. 2018. *Cryptojacking: A Modern Cash Cow*. Symantec.

[21] Papadopoulos, P. et al. 2018. Truth in Web Mining: Measuring the Profitability and Cost of Cryptominers as a Web Monetization Model. *arXiv:1806.01994 [cs]*. (Jun. 2018).

[22] 'RubyMiner' Cryptominer Affects 30% of WW Networks: 2018. https://research.checkpoint.com/rubyminer-cryptominer-affects-30-ww-networks/. Accessed: 2019-11-17.

[23] Rüth, J. et al. 2018. Digging into Browser-based Crypto Mining. *Proceedings of the Internet Measurement Conference 2018 on - IMC '18*. (2018), 70–76. DOI:https://doi.org/10.1145/3278532.3278539.

[24] Saad, M. et al. 2018. End-to-End Analysis of In-Browser Cryptojacking. *arXiv:1809.02152 [cs]*. (Sep. 2018).

[25] Schneier, B. 2015. *Secrets and lies: digital security in a* networked *world*. John Wiley & Sons, Inc.

[26] Smominru botnet infects 4,700 new PCs daily: 2019. https://www.kaspersky.com/blog/smominru-botnet-eternalblue/28862/. Accessed: 2019-11-16.

[27] Symantec 2018. *Symantec Internet Security Threat Report 2018*. Symantec.

[28] Tahir, R. et al. 2017. Mining on Someone Else's Dime: Mitigating Covert Mining Operations in Clouds and Enterprises. *Research in Attacks, Intrusions, and Defenses*. M. Dacier et al., eds. Springer International Publishing. 287–310.

[29] Trend Micro 2017. *2017 Annual Security Roundup: The* Paradox *of Cyberthreats*. Trend Micro.

[30] Varonis Uncovers New Malware Strains and a Mysterious Web Shell During a Monero Cryptojacking Investigation: 2019. https://www.varonis.com/blog/monero-cryptominer/. Accessed: 2019-11-17.

[31] Wang, W. et al. 2018. SEISMIC: SEcure In-lined Script Monitors for Interrupting Cryptojacks. *Computer Security*. J. Lopez et al., eds. Springer International Publishing. 122–142.

[32] Wannamine cryptominer that uses EternalBlue still active: 2018. https://www.cybereason.com/blog/wannamine-cryptominer-eternalblue-wannacry. Accessed: 2019-11-16.

[33] Wueest, C. and Anand, H. 2017. Living off the land and fileless attack techniques. (2017), 30.

[34] xmrig 2019. *xmrig/xmrig*.

[35] XMRig Miner Now Targeting Oracle WebLogic and Jenkins Servers to Mine Monero: 2018. https://www.f5.com/labs/articles/threat-intelligence/xmrig-miner-now-targeting-oracle-weblogic-and-jenkins-servers-to-mine-monero.html. Accessed: 2019-11-07.

[36] Zhou, B. et al. Can We Reliably Detect Malware Using Hardware Performance Counters? 2.