Dissertation Proposal

Analyzing Cryptojacking and Security Issues in Cryptocurrency and Metaverse in the Public Cloud

Ayodeji Adeniran

Date: April 28, 2024

Department of Modeling and Simulation
University of Central Florida
Orlando, FL 32816

Doctoral Committee:
Dr. David Mohaisen (Chair)
Dr. Changchun Zou
Dr. Mary Jean Amon
Dr. Yao Li
Dr. Sung Choi Yoo

Ayodeji Adeniran
Department of Modeling and Simulation, University of Central Florida (UCF)
4000 Central Florida Blvd., Orlando, FL 32816-2362 USA

EDUCATION

PH.D. IN MODELING AND SIMULATION (2019 – CURRENT)
University of Central Florida

M.SC. IN SYSTEMS ENGINEERING AND MANAGEMENT (2010 – 2011)
St Mary's University of San Antonio, Texas
CGPA: 3.98

B.ENG. IN ELECTRICAL AND ELECTRONIC ENGINEERING (1999 – 2003)
Federal University of Technology, Akure
CGPA: 3.45

PEER-REVIEWED PUBLICATIONS

1. **Ayodeji Adeniran**, and David Mohaisen, *Measuring Cryptocurrency Mining in Public Cloud Services: A Security Perspective*. The 11th International Conference on Computational Data and Social Networks (CSoNet), 2022.
2. **Ayodeji Adeniran**, Mohammed Alkinoon, and David Mohaisen, *Understanding the Utilization of Cryptocurrency in the Metaverse and Security Implications*. The 12th International Conference on Computational Data and Social Networks (CSoNet), 2023.

UNPUBLISHED PUBLICATION

1. **Ayodeji Adeniran**, Kieran Human, and David Mohaisen, *Security Analysis of Cryptojacking Infrastructure: A Comprehensive Study on Threats and Vulnerabilities*.

Contents

Abstract

Cryptocurrency has become a crucial component of the global financial system. However, this rise in popularity has also led to an increased risk of cyberattacks targeting the cryptocurrency ecosystem. Security and immutability are inherent requirements in the blockchain system, but malicious actors have introduced harmful content into various aspects of the cryptocurrency network and its interconnected systems. The existing work was on CPU usage for hardware and web-based mining; the work focused on websites without considering their underlying infrastructure, whether hosted on-prem or in the cloud. This dissertation addresses the gap by exploring the interplay between the cryptocurrency mining pools, the public cloud, and the metaverse in cryptocurrency.

First, we investigate the intersection between the cryptocurrency mining pool and the public clouds better to understand the role of public clouds in mining cryptocurrency. The study offers valuable insights into the prevalence of public cloud usage in the cryptocurrency mining sector. We conducted a passive DNS trace to detect cryptocurrency-related activities. Our results showed that 24 public cloud providers had components of cryptocurrency-related content. We scanned websites for vulnerabilities in public cloud services and found that the top clouds have strong links to mining pools. They exhibit heavy-tailed characteristics. We also identified countries with high mining pool distribution. We discovered that the mining pools in our dataset are primarily used for mining metaverse currencies.

Furthermore, we investigated the utilization of cryptocurrency within the metaverse and acquired metaverse coins with a minimum capitalization of 25 million USD. Using Whois to extract domain information, we scanned metaverse coin websites for malicious cryptocurrency content. We got the metaverse coin websites, used WHOIS for domain info, and scanned network traffic for suspicious activity. We also analyzed the domains to investigate their hosting history and determine their involvement in any past malicious activities. We scrutinized the cryptocurrency content on these domains to ascertain if they contained any phishing links, malware, or other malicious content. Our scan aimed to assess the security risks associated with cryptocurrency-related content on these IP addresses and domains. We discovered many files associated with the metaverse domains have a malicious presence.

Finally, we investigate the infrastructure used for cryptojacking by analyzing 887 malicious websites that are identified to have cryptojacking related maliciousness. The dataset was collected four years ago, and the websites were recently rescanned to ensure accuracy. The results revealed that out of the original 887 malicious websites, 517 were identified as malicious, while 370 were deemed clean. This valuable information provides insight into the dynamic landscape of website security. We found the presence of cryptojacking malware in the malicious websites. We identified the top countries of origin for most of these websites based on their geographical distribution.

1 Introduction

Cryptocurrency has become an integral part of the global financial system, with an estimated market capitalization of over a trillion dollars. Cryptocurrencies operate on decentralized networks based on blockchain technology. There are several popular cryptocurrencies such as Bitcoin (BTC), Ethereum (ETH), Ripple (XRP), and Litecoin (LTC), and they are all based on the blockchain technology. Cryptocurrency operates on a decentralized network, where every transaction needs to be validated before being added to the blockchain. The responsibility of validating cryptocurrency transactions lies with the cryptocurrency miners. They perform a complex algorithm to validate the transactions, and once successful, they are rewarded for their work.

Cryptocurrency mining requires a significant amount of energy and processing power to complete a transaction. Miners are motivated by the prospects of financial gain, which can prompt them to seek out more cost-effective and lucrative alternatives. As a result, there has been a trend towards cloud-based cryptocurrency mining, as it allows miners to access a wealth of resources. Our current investigation focuses on cryptocurrency miners' activities in the public cloud. We are specifically interested in understanding the distribution of public cloud infrastructure and how it impacts the formation of cryptocurrency mining pools. Additionally, we seek to identify any malicious activities resulting from these mining activities in the public cloud. Our goal is to understand the relationship between public cloud infrastructure and the cryptocurrency mining industry, as well as any security risks associated with these activities.

The Metaverse presents a virtual world where individuals can engage with each other and digital objects in real-time by leveraging immersive technologies like virtual (VR) and augmented reality (AR). Within the Metaverse, users can also conduct transactions utilizing cryptocurrency, a type of digital payment [16]. We aim to explore the impact of cryptocurrency as a payment method in the metaverse. Specifically, we are interested in examining the potential risks and negative consequences associated with the use of cryptocurrency, such as its potential facilitation of malicious activities in the metaverse. We will investigate the different malicious contents and their distribution in the top market capitalized metaverse domains we identified in our study. We have identified the top market-capitalized metaverse domains. Our next step is to conduct an in-depth investigation into the distribution of various malicious contents within these domains. We aim to identify and analyze the types of malicious content, such as phishing scams, malware, and other fraudulent activities, and their distribution channels within these domains.

The rise of cryptocurrency mining and the desire to maximize profits has led to a phenomenon known as crypto-jacking. Crypto-jacking occurs when cryptocurrency miners take control of other people's resources without their permission to mine cryptocurrency. These resources are referred to as infrastructures and can be cloud-based, web-based, or router-based. The goal is to take control of the infrastructure in order to use its resources for mining cryptocurrency. To gain a better understanding of crypto-jacking and its impact on infrastructures, we have analyzed a dataset collected a few years ago and are interested in performing a detailed website analysis. Our area of interest is investigating the security challenges prevalent in the cryptocurrency space. This includes a comprehensive analysis of the interacting components associated with the metaverse, public cloud, and infrastructure in crypto-jacking. We aim to identify the potential risks and vulnerabilities associated with the components above.

1.1 Statement of Research

In this dissertation, our primary focus is to investigate the security and vulnerabilities in cryptocurrency. We have examined the potential security issues arising from cryptocurrency mining by exploring the relationship between the public and crypto mining pools. Additionally, we have studied the possible threats posed by cryptomining on online infrastructures. We will provide more details on the studies.

The analysis of cryptocurrency mining in public cloud services provides insights into the prevalence and impact of cryptocurrency mining activities conducted within cloud environments. By quantifying the extent of mining operations and identifying contributing factors, this study establishes a foundation for understanding the broader ecosystem of cryptocurrency utilization across different computing platforms.

Building upon this foundation, the study on the utilization of cryptocurrency in the metaverse explores how cryptocurrencies are integrated into virtual environments and examines the security implications of their use. By investigating the adoption patterns, transactional behaviors, and associated risks within the metaverse, this study extends the analysis of cryptocurrency utilization beyond traditional computing infrastructures, providing a nuanced understanding of the evolving landscape of digital currency usage.

Finally, the comprehensive security analysis of cryptojacking infrastructure delves into the specific threat posed by cryptojacking operations, which exploit computing resources for illicit cryptocurrency mining. By dissecting the infrastructure supporting cryptojacking activities and identifying vulnerabilities and exploit vectors, this study contributes to the broader understanding of cybersecurity risks associated with cryptocurrency utilization. Moreover, it offers actionable insights and countermeasures for mitigating the threats posed by cryptojacking, thus closing the loop on the security implications identified in the previous studies.

In summary, these three studies collectively contribute to a holistic understanding of cryptocurrency utilization, spanning from its prevalence in cloud environments to its integration into virtual worlds and the associated cybersecurity risks. By building upon previous work and addressing distinct aspects of the cryptocurrency ecosystem, they provide valuable insights for policymakers, industry practitioners, and researchers seeking to navigate the complex challenges and opportunities presented by digital currencies.

Measuring Cryptocurrency Mining in Public Cloud Services: A Security Perspective (§ 3). In the past, cryptocurrency mining was largely reliant on hardware miners. However, with the advent of public clouds, the focus has shifted towards utilizing cloud-hosted servers. This is because of the public cloud's exceptional scalability, ease of deployment, high availability, and cost-effectiveness, all of which make it a far more appealing option for mining. We thoroughly analyzed various public clouds and known cryptocurrency mining pools to explore the relationship between them. Our study revealed that several crypto mining pools are being hosted on public clouds, and there is evidence of illegal use of these cloud computing resources, including malicious content.

Understanding the Utilization of Cryptocurrency in the Metaverse and Security Implications. Metaverse is an online digital platform and one of the emerging technologies and it is getting a widespread popularity and acceptance. Metaverse platforms involve buying and selling goods with both fiat currency and cryptocurrency. Our investigation is focused on cryptocurrency transactions within the metaverse and the associated security concerns.Our analysis centered on the top metaverse coins with a market capitalization of no less than twenty-five million dollars. Our objective was to uncover any potentially harmful behavior within the metaverse. We meticulously examined metaverse domains and found malicious content in the associated files in the metaverse. Additionally, we investigated fiat currency and cryptocurrency's role in the metaverse. Our findings revealed the presence of malicious activity within the metaverse domains.

CryptoJacking Infrastructure Analysis in Cryptocurrency (§ 5). For cryptocurrency transactions to be added to the blockchain, they must first undergo a validation process known as mining. Unfortunately, this process can be costly due to the required CPU power and energy. Consequently, some individuals turn to the unauthorized use of others' infrastructure, such as websites, networks, and routers, to mine for cryptocurrencies. This particular study delves into the realm of web-based cryptojacking infrastructure. Conducting an analysis of websites previously linked to cryptojacking is a valuable practice in determining whether they still contain such material or have since severed ties with it. Our objective is to scrutinize the prevalence and types of harmful content present on these websites, while also examining their geographic distribution to identify any clustering and investigate potential explanations.

2 Related Work

2.1 Cryptocurrency Mining in Public Cloud

This work is broadly associated with a body of work on crypto mining (irrespective of the tools used for that mining). Tahir *et al*. [44] studied the abuse of virtual machines in cloud services for mining digital currencies, which is the most related work to ours. Huang *et al*. [20] were among the first to notice the illegal use of CPU cycles for malware-induced mining. The initial work on web-based crypto mining was presented by Saad *et al*. [41] and Ruth *et al*. [37], who measured the prevalence of cryptojacking among websites (i.e., utilizing mining on visitors' machines). To do that, Ruth *et al*. [37] obtained blacklisted URLs using the no coin web extension, mapped them on a large corpus of websites obtained from the Alexa Top 1M list, and identified 1491 suspect websites involved in cryptojacking. In a concurrent work, Saad *et al*. [41] conducted a similar study, but on a larger number of websites; 5703 sites in total. Concurrently, Eskandari *et al*. [15] examined the prevalence of cryptojacking among websites and the use of *Coinhive* as the most popular platform for cryptojacking. All of these studies highlight the issue of cryptojacking through measurements and the emerging use of cryptojacking as an alternative to online ads. Saad *et al*. [41] goes further by conducting code analysis toward detecting cryptojacking codes and their economic impact. Bertino and Nayeem [6] highlighted worms in IoT devices that hijacked them for mining purposes, pointing to the infamous *Linux.Darlloz* worm that hijacked devices running Linux on Intelx86 chip architecture for mining [5]. Krishnan *et al*. [25] studied a series of computer malware, such as *TrojanRansom.Win32.Linkup* and *HKTL_BITCOINMINE*, that turned host machines into mining pools. Sari and Kilik [43] used Open Source Intelligence (OSINT) to study vulnerabilities in mining pools with Mirai botnet as a case study.

2.2 Cryptocurrency in Metaverse

Several papers explored the security of the metaverse. Di Pietro and Cresci [14] explored the security and privacy concerns surrounding the metaverse by focusing on the security risks that metaverse users may face and how it could affect their privacy. Zhao *et al*. [52] also conducted a study on security in the metaverse, discussing the common security issues and how they can impact the metaverse. Choi *et al*. [13] examined the future of the metaverse, tackled similar security issues as the previous ones, and discussed the technology and structural frameworks associated with the realization of solutions.

Kurtunluoglu *et al*. [29] explored authentication in virtual reality and the metaverse, focusing on security and privacy concerns related to authentication methods. Aks *et al*. [3] also conducted a study on metaverse security, covering metaverse infrastructure, human interactions, and other interconnected virtual worlds aspects [21].

Tariq *et al*. [45] explored the security implications of deepfakes in the metaverse, the security challenges, authentication issues, and impersonation problems. Oosthoek *et al*. [33] researched the security threats to cryptocurrencies, particularly to Bitcoin exchanges—Bitcoin is one of the major cryptocurrencies used in the metaverse. Zaghloul *et al*. [51] also examined the security and privacy issues with Bitcoin and blockchain relevant to the metaverse. Giechaskiel *et al*. [18] examined Bitcoin security challenges and their impact when there is a security breach or exposure.

Rosenberg *et al*. [35] conducted a study on marketing in the metaverse and consumer protection. The study explained the trend in increasing marketing in the metaverse due to increased market capitalization and consideration of the security of the consumers in the metaverse. Rosenberg *et al*. [36] also studied marketing in the metaverse and the associated risks. Kshetri *et al*. [26] studied the economics of the metaverse and its impact on the global economy.

2.3 Cryptojacking of Infrastructure

This work is related to the body of works on cryptojacking. There are quite a number of study on cryptojacking but the most related to our work are Jayasinghe *et al*. [22] which explore cryptojacking in the public cloud infrastructure and Saad *et al*. [40] that analyzes the end-end in-browser crytpojacking.

Burgess *et al*. [10] MANiC (Multi-step Assessment for Crypto-miners) was developed to detect cryptocurrency mining scripts and extract the parameters that could be used to detect suspicious behavior related to mining activities. Carlin *et al*. [12] conducted similar study on detecting cryptojacking websites by using opcode for detection of browser-based cryptomining scripts within our dataset can be detected by dynamic opcode analysis. Xiao *et al*. [49] study GPU cryptojacking and developed MagTracer, a novel GPU cryptojacking detection system which was used to detect GPU cryptojacking with an accuracy of 98%. Naseem *et al*. [32] proposes using MINOS, a lightweight cryptojacking detection system based on a deep learning method, to detect the presence of unwarranted WebAssembly(Wasm)–based mining activity in real-time. Tekiner *et al*. [46] proposes a method for an efficient IoT cryptojacking detection mechanism based on network traffic features, which can detect both in-browser and host-based cryptojacking.

In another work, Saad *et al*. [42] performed analysys of content, currency, and code-based categorization of cryptojacking samples, the study measure the distribution across websites, the platform affinities, and the code complexities.

3 Measuring Cryptocurrency Mining in Public Cloud Services: A Security Perspective.

3.1 Summary of Completed Work

The public cloud infrastructure has been subject to various vulnerabilities initiated by malicious actors. By examining the interplay between cryptocurrency mining activities and the public cloud, this study endeavors to contribute valuable insights into the evolving landscape of cyber threats and the associated challenges faced by cloud service providers and users alike. Our findings shows number of cryptocurrency mining pools in the cloud and discovered malicious content in these domains and the geographical distribution of the cryptomining pools in the public cloud.

3.2 Introduction

Cryptocurrency has recently been on the rise, with the top three cryptocurrencies amounting to over a trillion USD in value [38, 39]. With cryptocurrency gradually gaining acceptance, different cryptocurrencies are still emerging. Many cryptocurrencies directly apply blockchain technology, a distributed ledger over a distributed network of nodes that record transactions. The blockchain distributed system provides a much safer architecture against failure and cryptographic primitives that ensure transactions are safer from being altered. Given the importance and value of those cryptocurrencies, cybercriminals have used them to enable their criminal activities.

Cybercrimes have been evolving over the years, where cybercriminals have been continuously coming up with new ways to violate system security properties, steal information, hijack resources, and demand ransom [24]. The emergence of new attacks has been a continuous race between the attackers and the defenders. The attackers have used several platforms to launch attacks. Attackers were noticed to have changed their strategy to defeat defenses. For instance, with the emergence of blockchain-based technologies, malicious transactions are placed on the blockchain to facilitate malicious activities through the distribution of stealthy command and control channels [8]. Given the significant valuation of cryptocurrencies, cryptojacking, an intentional effort to use others' machines and resources for mining cryptocurrencies, has been on the rise [41]. Notably, the use of cloud resources has been hypothesized to be the main entry point of mining cryptocurrencies [23], although not systematically analyzed.

The focus of this paper is to understand the prevalence of public clouds for mining purposes, possibly mining with malicious intent (e.g., with compromised cloud instances). We hypothesize that utilizing cloud resources for such activities is more consistent with the general compute trends and (from a security standpoint) adversaries' incentives than ever before. For instance, launching cyber-attacks from the private server(s) that can be traced and shut down is no longer popular among attackers because, apart from the ease and flexibility of springing up resources in the cloud, they also make less return on investment compared to setting up private servers.

There are several cloud providers, from enterprise-scale to small-scale, the users and adversaries alike can move from one provider to another and set up attack fronts fast. Exploiting blockchain technology in conjunction with cloud resources, the attackers have a vast and cheap cloud to benefit from and a difficult-to-decipher blockchain technology to hide their malicious activities, mainly when those cloud resources are obtained free of charge (i.e., compromised). While security analysis is a byproduct of our analysis, it also highlights the general trend in this space.

3.3 Research Questions

In this dissertation, Our focus is on answering four formulated research questions. These questions formed the basis of our analysis, result, and discussion geared toward answering the research questions and understanding the interplay between public cloud infrastructure and cryptomining.

1. **Can DNS traces be used to track mining activities?** Previous related works on cryptomining and cryptocurrency malicious activities were code-based analyses. We decided to make use of DNS for traffic analysis between the cryptocurrency mining domain and public cloud providers; we opted to use passive DNS, which maintains DNS resolution data on a specific record, location, and time frame.

2. **What is the prevalence of cryptomining activities on public cloud infrastructure?** We want to measure and understand the prevalence, pattern, and penetration of cryptocurrency mining activities in the cloud. The analysis and result would provide insight into the extent of cryptomining activities in the cloud.

3. **What are the hosting patterns for cloud infrastructure utilized for cryptomining across mining pools?** With the gradual shift of cryptomining activity to the cloud, several cryptomining pools are hosted in the public cloud infrastructure. We want to understand the pattern of hosting these mining pools in the cloud, if hosted across several cloud providers, in different countries, and across network operators.

4. **What is the prevalence of malicious cryptomining activities in the cloud?** One of the expected results is establishing a relationship between cryptomining pools and the public cloud for malicious activities by analyzing the data from the passive DNS. We plan to establish the existence of such malicious activities and their prevalence on the public cloud.

3.4 Dataset and Preprocessing

The dataset used in this study couples an enumeration of mining pools and associations between them and cloud instances that belong to various cloud providers utilizing DNS query data. To this end, the first part of the input data used for this analysis is the mining pools and their associated addresses. The list of the mining pools was sourced by manually listing the domains from the Stelareum mining pool website. This list contains a set of mining pool addresses that are publicly available [1]. We examined the mining pools and copied the corresponding URLs for each. Subsequently, using the popular Digital Envoy IP allocation dataset[2], we enumerated the IP pools of some top public cloud providers, which formed the second input data.

To establish an association between the various cloud providers and the mining pools, we scanned over all the IPs allocated to the public providers on one side and the mining pools addresses on the other side using the passive domain name system (pDNS) dataset used in [34]. The scan utilizes the pDNS dataset to map a relationship between the mining pools and endpoints in the cloud where traffic is sent from those endpoints to the mining pools, and vice versa, at some point in time in the past. The scan output consists of the mining pool's originating IP address and the cloud providers' corresponding IP subnet.

The scan result includes the mining pool domain, pool source IP address, and public IP subnets. The IP subnets are then converted to their respective domains to get the name of the cloud providers. The data contains thousands of response lines (as there could be various pDNS entries associated with the same pair of endpoints). As such, the data was cleaned by rearranging the data in descending order and removing those with the least number of responses. To obtain the geographical distribution of the cloud providers in our data, we further augment the data with the country where the cloud provider is located.

3.5 Main Results

This section presents our main results by measuring and mapping the association landscape between cryptocurrencies and public clouds. Before we dive into our analysis, we review the main dimensions of our analysis.

3.5.1 Analysis Dimensions

This study is concerned with various dimensions that highlight the interplay between public clouds and cryptocurrencies. Namely, we are concerned with cloud providers (associated with cryptocurrencies) and their geographical affinities, pool size, mining pools, and their distribution, cloud

[1] https://www.stelareum.io/en/mining/pool.html

[2] https://www.digitalenvoy.com/

provider-specific distribution, and (potential) illicit activities. We define each of those dimensions as we present the associated results.

3.5.2 Results and Discussion

❶ **Cloud Providers and Country of Origin.** A large number of public cloud providers make up the cloud ecosystem. While the significant providers are only a few (e.g., Amazon, Google, Azure, and Cloudflare), there are more than thousands of such providers. Understanding the affinity between mining pools and those cloud providers through distribution analysis is essential for two reasons. First, such an analysis will allow us to understand the regional distribution of those providers and associated mining activities. Second, this analysis will further shed light on whether the large providers, in general, are still dominant in their use for mining. Answering this question, possibly positively, would allow us to devise effective policies to counter cryptomining threats. Moreover, insight for this analysis would draw a representative picture of the overall computing ecosystem and associated security characteristics.

Observations. Table 8 shows the cloud providers mapped to the countries of their domain registrations. Interestingly, we find that the distribution of traffic from the mining pools is vastly distributed, covering a large number of providers, and spanning several continents. Moreover, we found that the distribution of the cloud providers' representation with respect to the studied mining pools and their association is quite skewed (heavy-tailed): while there are 24 different cloud providers represented in the dataset, the top 2 (Amazon and Google) have a representation of 48%, while the next 12 providers have 42%.

By the same token, Table 8 highlights the geographical distribution of the different cloud providers, where the distribution is also heavy-tailed over 15 countries, led by the US (57%), followed by Russia (11%), South Korea (6%), and Japan (5%). The remaining 11 countries have 21% of the cloud endpoints shared among them collectively. The cloud distribution is obtained from the result of the pDNS scan.

❷ **Mining Pools and Associated Size.** In this study, we measured two major pools in terms of their presence in the cloud. The size of the pool is measured by counting the number of individual (cloud) IP addresses associated with it (i.e., issuing queries). Understanding the pool size would highlight which pool is more popular and central in the cryptocurrency ecosystem, and possibly which cryptocurrency is being mined by the pool utilizing cloud resources.

Observations. We emphasize that we conducted scans of several mining pools in our initial data gathering (i.e., all those present in our initial set), although we only got a response from two mining pools domains, `sandpool.org` and `miningetherium.net`—which means that the other mining pools did not have any association with public clouds. In our scan, we noticed that the two mining pool domains contain other subdomains which responded to the query from the pDNS. Table 2 shows the mining domain and the subdomain with the corresponding representation in

Table 1: Cloud distribution across the country with the frequency of appearance.

Cloud Provider	Country	Pool Count	Pool%
Amazon	USA	738	24%
Google	USA	737	24%
KORNET	South Korea	188	6%
Cloudflare	USA	175	6%
Asia Pacific Net	Japan	161	5%
CL-KARELIA	Russia	155	5%
SCL66-rented1	Cyprus	135	4%
MACROREGIONAL	Russia	117	4%
HIPL-SG	USA	69	2%
Corpori	Brazil	58	2%
HOSTERION-SRL	Romania	50	2%
KAZAKTELECOM	Kazakhstan	46	2%
MOTIV-DC-1	Netherlands	46	2%
MOTIV-DC-3	Netherlands	46	2%
DNAP-081217	Finland	44	1%
AOSOZVEZDIE-NET	Russia	38	1%
IPNET-DS-WBS	South Africa	33	1%
RS-KOPERNIKUS	Rep of Serbia	33	1%
PS-1_2177	Kazakhstan	32	1%
BTC-TEMP1	Bulgaria	31	1%
TR-RTNET-981210	Turkey	31	1%
CLOUDFLARENET-EU	USA	28	1%
RU-MOS-SMILE	Russia	28	1%
UK-NTLI-990527	United Kingdom	24	1%
	Total	3043	100%

terms of cloud presence. Based on these results, we narrow down the focus of this paper to the two pools and their associations with the public cloud.

Cryptocurrency mining has global acceptance with mining activities being carried out in several parts of the world. Some mining pools are rated to be in the top tier because of the amount of mining traffic recorded and associated with them. These pools are located in different countries. Most of the top-rated pools are located in China. For instance, in the general cryptocurrency ecosystem, pools like F2Pool, AntPool, BTCC, and BW account for more than 60% of all the new bitcoins. While the dataset from the DNS scan recorded most traffic to Amazon and Google cloud providers, a search on the reported top 10 mining pools using censys.io, a search engine that scans the internet for connected devices. Alibaba's cloud network recorded a higher traffic rate for the mining pools based in China, while Amazon had higher traffic for pools located in the US and other countries. The geographical location of the mining pool could be a factor in determining the

Table 2: Mining pools distribution. A heavy-tailed distribution in terms of the number of public cloud associated with the different mining pool (sub)domains.

Pools (subdomain)	Cloud Count	Cloud Percent
sandpool.org	1,470	41%
etp.sandpool.org	1,205	34%
eu.miningethereum.net	351	10%
miningethereum.net	348	10%
www.miningethereum.net	73	2%
www.sandpool.org	55	2%
ru.etp.sandpool.org	26	1%
dev.sandpool.org	20	1%
Total	3,043	100%

preferred cloud provider before selecting other available providers.

By the same token, we found that the top two subdomains (by sandpool) represent 75% of the overall cloud associations, with ETP, the second-largest association, representing 34% of the associations (1,205 cloud endpoints). Upon further exploration, we found that this pool is used mostly for mining Metaverse ETP, a cryptocurrency that powers the Metaverse blockchain-as-a-service (BAAS) platform and is located in Europe. Among those two pools, sandpool.org had 78% (or 2,750) of the cloud associations overall, while miningetherium.net had 22% (or 798) of the cloud associations in total.

Table 3: Google vs Amazon Cloud distribution between the two pools. While the general trend of heavy-tailed distribution still applies to the individual cloud shares against the subdomains of the pools, Amazon has a more skewed distribution in contrast to a more evenly distributed share of Google's cloud instances.

Pools	Google	Amazon	Google%	Amazon%
etp.sandpool.org	307	213	42%	36%
sandpool.org	186	357	25%	59%
miningethereum.net	106	9	14%	1%
eu.miningethereum.net	104	5	14%	1%
www.miningethereum.net	19	3	3%	0%
www.sandpool.org	7	9	1%	1%
ru.etp.sandpool.org	5	6	1%	1%
dev.sandpool.org	3	5	0%	1%
Total	737	607	100	100

❸ **Cloud Providers Distribution vs Pools.** The current cloud ranking by market share places Amazon with the largest share, followed by Microsoft Azure, then Google. In our measurement, we found that Amazon and Google represented almost fifty percent of the total cloud instances connected to the mining pools in our dataset, while the other different cloud providers make up the remaining half. We want to further understand the detailed distribution between the two major cloud providers to the two mining pools to characterize their similarities and differences, as depicted in Table 3.

Observations. From those results, we made two key observations. First, the per-cloud distribution follows a similar trend of heavy-tail as in the generation distribution, although less skewed in the case of Google, where cloud share is distributed more evenly on a larger number of pool domains. Second, while Azure is quite popular in the abstract, and on par with the popularity of Google Cloud, it is absent from this analysis. We still speculate that cloud popularity may have played a factor in the distribution, and the absence of Microsoft Azure cloud in the distribution would possibly point to other factors that may have influenced the selection of Amazon and Google (e.g., strict abuse policies, or the popularity of this cloud in a given country). Some smaller cloud providers also reported traffic from the pool that indicated association to the clouds that could be either randomly or selectively. The information in the dataset is not explicit enough to accurately provide the details, but we hypothesize that factors like cost, security, or restrictions for some category of users, such as in the case of Azure, could be responsible for the choice and the clear trend.

❹ **Malicious Associations.** The popularity of cloud services over the years has made them attractive for both benign and malicious use. Services and applications previously hosted on private servers are now hosted in the cloud and many public and private companies are still migrating their workloads to the cloud. It is no surprise that mining activities are shifting to the cloud, considering the cost and the flexibility offered. Setting up servers in the cloud takes a few minutes at a significantly lower cost. The flexibility of moving from one cloud provider to another could be another factor besides the cost that attracted the miners to shift their activities to using cloud resources.

Cybercriminals operate by masquerading their malicious traffic from detection using different techniques. The servers are shut down once detected, which is a big loss for cybercriminals. Cloud services provide an easy solution for cybercriminals addressing this issue. For instance, to make their activities more discreet, cybercriminals make use of blockchain technology when operating from the cloud. In case of detection, they quickly move to another cloud provider to set up their servers in a few minutes with very minimal disruption to their services and activities. They continue to operate in these cycles at a relatively small cost and manage to keep afloat for a while before being detected.

A central question in our analysis is whether some of those cloud instances used for mining cryptocurrencies are involved in malicious activities. Unfortunately, the dataset we have is limited in many ways, particularly the absence of a payload for the DNS resolution or subsequent application-layer communication, which makes it impossible to draw such a conclusion. However, utilize our knowledge of the endpoint on the cloud to frame the question into a plausibility analysis: among those IP addresses associated with the cloud providers, how many of them are associated with malicious activities?

Observations. In order to address this question, we conducted an additional scan on the IP addresses associated with the cloud instances using `virustotal.com`, which is one of the three online scanning sites we used in our analysis. The results of the scan are shown in Table 4. Among the 24 cloud providers reported in Table 8, only five cloud providers have positive scan results in `virustotal.com`, namely Amazon, Google, KORNET, Cloudflare, and CL-KARELIA. Among them, CloudFlare had the largest detection rate, with 44% of the cloud instances reported by VirusTotal as having some security issues (i.e., flagged as a source of malicious activity). The percentage is followed by Amazon (at 34.69%) and Google (29.85%). Among those cloud providers KORNET had the least positive rate, with only around 1% of the instances detected by `virustotal.com`.

While those results are inconclusive, and cannot be used to argue for intent associated with the mining activities taking place on those cloud providers for the different mining pools, or whether mining is taking place if at all, the fact that a positive detection is associated with a number of those public cloud IPs highlights the potential risk associated with those instances.

Table 4: A distribution analysis of the malicious cloud instances (IPs) in contrast to the total number of IP count associated with the given cloud provider, and the associated percentage. Notice that with the top cloud providers, a significant number of instances are shown to be associated with a malicious activity at some point in time, per `virustotal.com` scan. Cloud providers not present in this table returned negative scan results.

Cloud Provider	Count	Malicious	Percentage
Amazon	738	256	34.69 %
Google	737	220	29.85 %
KORNET	188	2	1.06 %
CloudFlare	175	77	44 %
CL-KARELIA	161	10	6.21 %

3.6 Discussion

From our analysis, we notice that more associations are reported on the Google cloud platform than on the Amazon platform. The preference for Google Cloud over Amazon by the miners could be due to various reasons. For instance, computing power and the cost of electricity are among the challenges in cryptomining. Both cloud providers have instances with computer power resources to handle the cryptomining activities, but the cost might be the main differentiating factor because the profit determines the attractiveness of mining. The two top cloud providers are known to have high reliability and availability, and provide a range of offerings that suit the applications associated with the highlighted mining activities; virtual reality. Given the expectations of those applications, the failure rate is low in these clouds and miners could run their mining system uninterrupted.

By the same token, the less popular and smaller cloud providers have fewer resource offerings and may lack the capacity required by cryptominers. Cybercriminals using blockchain for sending malicious traffic might prefer smaller cloud providers because they may be cheaper, prone to exploits, and less secure in general, while they may accommodate such activity to drive traffic on their cloud platform. There is the possibility of using popular clouds as well by exploiting the vulnerabilities in such clouds, especially by hijacking user accounts with weak credentials and hiding their malicious traffic among millions of packets originating from the cloud. Our security analysis above highlights the potential of this hypothesis, as a number of public cloud nodes (identified by their addresses) are shown to be associated with malicious activities in `virustotal.com` scan.

Security in the cloud is a shared model system whereby both the cloud provider and the customer have their responsibilities shared. While several security measures are recommended, some fail to implement the required minimum security and may have their account hijacked and used for malicious purposes, including mining cryptocurrency. Hijacking user accounts for mining activity is common because of the high computing resources required for mining and this comes with a price: using someone else account in this manner transfers the cost to the account owner while the miners earn rewards for their mining activity. These kinds of account hijacking for mining activities were reported by a number of cloud providers, especially by the top providers. For instance, 86% of the hijacked accounts in Google clouds are used for cryptomining [47]. Our results allude to a similar outcome, as many of the cloud addresses shown in our analysis are associated with malicious activities.

In this study, we noticed that the two main mining pools uncovered in our analysis are quite protective of registration information. Upon digging into the DNS records of their domains, we found that their DNS resolution and hosting are done by Cloudflare. Neither of those main pools nor their associated subdomains is detected by `virustotal.com`. To contrast this result with other major mining pools, we evaluated the top mining pools (besides those studied thus far). The results are shown in Table 5. We noticed all the top ten mining pools are hosted in the cloud as well, and mostly in Cloudflare. Out of the ten mining pools, nine are hosted on the Cloudflare cloud, highlighting a persistent trend in the utilization of cloud resources for running mining pools, perhaps for their high availability. The public cloud provides some security measures, but that does not necessarily prevent the pools from being used for malicious purposes. We then scanned all the mining pools IP addresses using `virustotal.com`. While all of them returned negative detection results (although many returned "unrated" result for the scanned addresses), indicating that they were not involved in reported malicious activities. However, two types of detection were reported: passive DNS (pDNS) replication and communication file detection.

Interestingly, none of the domain names associated with those pools have pDNS flag; pDNS is what we use for retrieving the association between clouds and mining pools. The pDNS Replication provides temporary storage for DNS queries and captures the queries on the network and stores them for later retrieval. The stored queries are in historical form, which can be analyzed later by security experts. virustotal.com explains the main idea behind passive DNS as inter-server DNS which captures messages and forwards them to a collection point for analysis and storing of the individual DNS records in a database where they are indexed and queried after the processing. Given the lack of pDNS data for those domains, it is not surprising that we could not see them in our initial association dataset. To this end, our analysis comes with a caveat: the estimated association between those cloud providers and mining pools is a lower bound, and only captures those that are explicit about their association.

The files entry in Table 5 highlights the number of files that have been determined to perform some kind of communication with the IP address of the domain under consideration. These files are not considered malicious in nature, but indicative of an association with other addresses, which highlights our hypothesis that the estimated association is a lower bound.

Table 5: Top 10 mining pools scan. IP addresses are masked for privacy.

Mining Pool	IP Address	Domain	pDNS	Files
Binance.com	13.226.**.**	Amazon	0	2
slushpool.com	104.26.**.**	Cloudflare	0	1
f2pool.com	104.18.**.**	Cloudflare	0	10+
pool.btc.com	104.18.**.**	Cloudflare	1	10+
viabtc.com	104.16.**.**	Cloudflare	0	3
v3.antpool.com	104.18.**.**	Cloudflare	0	4
poolin.com	104.22.**.**	Cloudflare	0	5
bw.com	172.66.**.**	Cloudflare	0	7
bitfury.com	104.26.**.**	Cloudflare	0	10+
v3.antpool.com	104.18.**.**	Cloudflare	0	4

Table 6: Mining Pool IP address Malicious scan.

Pool	Security Vendor	Number
v3.antpool.com	CMC Threat Intelligence	1
bitfury.com	CMC Threat Intelligence	1
poolin.com	CMC Threat Intelligence	1
v3.antpool.com	CMC Threat Intelligence	1
viabtc.com	CMC Threat Intelligence	1
pool.btc.com	CMC Threat Intelligence	1

The analysis we have conducted thus far is based on virustotal.com, which is the golden standard for evaluating security through detection against a range of scanners and antivirus vendors. We scan the pools and associated subdomains using various in-house products of threat intelligence. Interestingly, and as shown in Table 6, we found that a number of those pools are reported as involved in malicious activities (in the description, CMC threat intelligence reported that malware is hosted on the listed mining pools). While a detection that is not replicated by the other major vendors in `virustotal.com`, highlights a divide in the security industry on how mining is perceived.

3.7 Conclusion

In this paper, we initiate the systematic study between public clouds and cryptocurrencies, one of the most prominent applications of blockchain systems. Through pDNS traces, we establish the association between two mining pools and cloud providers. Unsurprisingly, we found that the major cloud providers are popular in their association with mining pools, with a heavy-tailed distribution and global presence. Upon examining the security of the associated cloud endpoints associated with mining pools, we found that a significant number of them (above 30% in three cases) are malicious by `virustotal.com` scan results. By examining the hosting patterns of mining pools, we found that they are also heavily utilizing cloud providers, and the view of those mining pools, from a security standpoint, is divided. While our study is limited by the lack of payload from which one could understand the intent of the different associations between cloud and mining pools, it calls for further actions in this direction by providing preliminary anecdotes through characterization.

4 Understanding the Utilization of Cryptocurrency in the Metaverse and Security Implications.

4.1 Summary of Completed Work

Metaverse platforms, similar to other internet-based services, exhibit a propensity for vulnerabilities. This study undertakes an examination of the vulnerabilities stemming from cryptocurrency transactions within the metaverse, alongside the susceptibility of metaverse tokens characterized by high market capitalization to such vulnerabilities. The metaverse domain exhibits a conspicuous incidence of malicious activities, serving as indicators of nefarious elements introduced into the metaverse ecosystem. Such occurrences underscore the imperative for comprehensive cybersecurity measures within the metaverse, necessitating robust strategies for threat detection, prevention, and mitigation. Furthermore, understanding the motivations and methodologies behind these malicious activities can provide valuable insights for devising proactive defenses and safeguarding the integrity and security of the metaverse landscape.

4.2 Introduction

Metaverse is a technology of the future with much anticipation and hype about its capabilities to alter the life of humans through online model values [9]. Several companies are energetically working on building the metaverse, including technology giants like Facebook and Microsoft, among others. The metaverse is still in its development phase, and the full realization of an interconnected virtual world is yet to be a reality. The metaverse holds the potential for various applications, such as entertainment, gaming, education, virtual commerce, virtual meetings, and more, and is expected to revolutionize how we socialize, work, learn, and interact with digital contents [2].

Although the metaverse is still developing, metaverse coins already amount to trillions of USD in value, and this trend is expected to persist as the technology reaches maturity [31]. However, as with any digital platform or online community [1], the possibility of malicious activities occurring in the metaverse cannot be ignored. As the metaverse concept evolves, it is essential to address potential security concerns, including detecting malicious activities within this virtual space. While the metaverse presents new opportunities for collaboration, interaction, and entertainment, it can also attract malicious actors who seek to exploit vulnerabilities or engage in harmful activities. The intent and motivation for carrying out the malicious activity could be to steal vital information or assets that can be translated into money. Since the metaverse represents the digital world, which involves buying and selling with either cryptocurrency or fiat currency, malicious activities cannot be uncommon.

This paper focuses on understanding malicious activities in the metaverse represented by various platforms and domains. The attackers are sophisticated and experienced with reported attacks on other online platforms, e.g., cryptocurrencies and social media platforms. One of the ways the cyber attackers operate is by sending malicious files to the intended targets to corrupt the system and enable them to access it. The cyber-attacks can be malware, denial-of-service (DOS) attacks, phishing, or code injections. Security analysis of the metaverse domains is the central focus of this paper, and we intend to analyze the files interacting with the domains to gain insight. We will discuss the possible security challenges and malicious activities in the metaverse.

Organization. In section 2, we present the related work, including the research gap. In section 5.3, we introduce the problem statement, including the research questions. In section 4.4 we introduce our approach. In section 5.5, we discussed the results. We discuss various aspects of our studies in section 5.6 and conclude our work in section 5.7.

4.3 Problem Statement and Research Questions

Both legal and illegal activities and transactions are expected in the metaverse. Metaverse is expected to become the digital center for gaming, entertainment, education, etc. Traffic to the metaverse will likely increase with millions of dollars in daily transactions. Security of assets, non-fungible tokens, cryptocurrency, and other technologies has become a challenge due to illegal activities associated with them in the metaverse.

To this end, this paper aims to tackle three crucial research questions related to identifying harmful behavior in the metaverse, particularly those associated with virtual tokens. Our analysis will be guided by these questions to ensure we provide accurate and self-contained answers. By scrutinizing various domains in the metaverse, we will obtain valuable insights that will aid our examination.

1. **RQ1: What are the prevalence of digital coins in the metaverse, and what are their associated threats?** We thoroughly scrutinize the correlation between the popularity and market capitalization of the metaverse and the plausible malicious threats. We analyzed the top forty metaverse coins with the highest market capitalization to accomplish this objective.

2. **RQ2: How significant are metaverse domain artifacts such as communication and referring files in determining the maliciousness of such domains?** To effectively identify malicious incursions in Metaverse domains, conducting a thorough analysis of critical artifacts is imperative. This includes communication files, referrer files, and Passive DNS artifacts, which all directly impact Metaverse domains. Therefore, a comprehensive assessment of their contribution is essential.

3. **RQ3: Is there any correlation between fiat currency to cryptocurrency and vice versa, and the maliciousness of metaverse applications?** It is imperative to recognize the immi-

nent threat posed by cyber attackers who aim to steal money and assets, especially in the metaverse, where cryptocurrency reigns supreme. Our investigation will determine whether domains incorporating fiat currency are more susceptible to malicious activities than those solely relying on cryptocurrency.

4.4 Technical Approach

This study explored the level of malicious activities in the top metaverse tokens. We analyzed 44 metaverse tokens with a market capitalization of at least 25 million USD. We hypothesize that cybercriminals are likelier to target tokens with a high market capitalization. To test this, we first divided the metaverse tokens into their respective domains and mapped them to their IP addresses. Then, we used the "whois" tool to gather information about the DNS service provider, registrar location and URL, hosting DNS IP addresses, and content delivery network (CDN). We manually inspected all the metaverse websites we studied for transactions from fiat to cryptocurrency.

We thoroughly scanned the metaverse domains and associated IP addresses using virustotal.com. During the scan, we gathered *passive DNS*, communication files, and referrer files and identified malicious detections. We then analyzed the communication and referrer files to detect any malicious activities and identified the file types to locate the source of the malicious activities. We then cross-referenced the metaverse domains with the malicious detections in the communication and referrer files to verify their presence. Additionally, we compared domains with fiat currency and cryptocurrency to domains with malicious activity. Lastly, we examined the metaverse tokens to identify patterns between the top and low tokens based on their market capitalizations.

4.4.1 Dataset and Preprocessing

Websites and Their Attributes. For this study, we collected data on metaverse coins, their corresponding domains, and their IP addresses. Our first step was to manually select metaverse coins with a market capitalization of at least 25 million USD and then map them to their respective domains. For the initial set of domains, we utilized `https://coinmarketcap.com`, a website that specializes in tracking coins, their market caps, and associated domains of application. To extract infrastructure information and address the first research question we posed in section 5.3, we used domain query tools to extract information such as the IP addresses and CDN providers and *manually* checked each webpage for the presence of fiat currency.

Security Data Attributes. We then scanned each metaverse domain and its associated IPs with `virustotal.com`. This scan provided information on Passive DNS, communication files, referrer files, and malicious detections. We further analyzed the communication files and referrer files to identify those with malicious detection and their types. The malicious detection was also categorized into different types with the number of occurrences for each type. Our primary focus was collecting data with malicious detection to explore the correlation between the different metaverse platforms, cryptocurrencies, artifacts, and associated malicious detection.

To gain a deeper understanding of file connections, especially those related to malicious activities, we thoroughly examined the interlinking between infected communication and referrer files and malware detections. Moreover, we meticulously tallied the frequency of each file type and its association with infected communication and referrer files. Our efforts to uncover malicious behavior were further amplified by our detailed analysis of every scan result and its correlation with malware detection in the scanned files and hosting metaverse platforms.

4.4.2 Analysis Dimensions

Our study explores the relationship between the metaverse domains and malicious activity and detection. We aim to identify the source and prevalence of such activity within the metaverse space. To do so, we analyzed various dimensions and provided answers to research questions. In the next section, we will focus on specific dimensions to uncover answers to our research questions in section 5.3. Namely, the dimensions we cover with our analysis are (1) communication files and referrer files activities in the metaverse domain, (2) metaverse coins market capitalization, (3) malicious activities in Metaverse coins, and (4) metaverse coins with fiat currency to cryptocurrency.

4.5 Results and Findings

Our main results, which analyze and map the relationship between malicious detections in metaverse domains and other artifacts, will be presented in this section.

4.5.1 Communication and Referrer Files in the Metaverse Domain

The popularity of online platforms is determined by the number of visitors, transactions, and overall traffic. Facebook, for instance, boasts billions of registered users and experiences a significant amount of communication and transactions. These interactions are facilitated through manual website exploration, file exchanges, and website database access. However, it is important to exercise caution as autonomous programs such as bots can also interact with these systems. They can inject messages or code, store data in databases, and even remotely manipulate and hijack systems. Therefore, it is crucial to implement proper security measures to prevent unauthorized access and protect sensitive information. In the metaverse, communication files play a significant role. We have collected communication files from all domains and are studying their relationship with malicious activities. Our analysis aims to determine if the number of communication files is linked to malicious detections and identify the types of files responsible for such detections. This information will be crucial in developing preventive policies against malicious threats in the metaverse.

Observations. The heatmap in Fig 1 displays the frequency of malicious detections in different file types across various domains in the metaverse. The Win32 EXE file type had the highest frequency of malicious detection, with 14 domains recording it. Android came in second, with 11 domains showing a malicious presence. The axieinfinity.com domain had the highest number of malicious detections at 483. Other file types with malicious activity included PDF, Javascript, Android, and MS Excel Spreadsheet. These file types were responsible for most malicious detections in the study. Additionally, Fig 2 shows the frequency of referrer files with no detection. The figure displays a heatmap indicating the frequency of infected referrer file types in the metaverse domain. The number of occurrences for each file type is indicated.

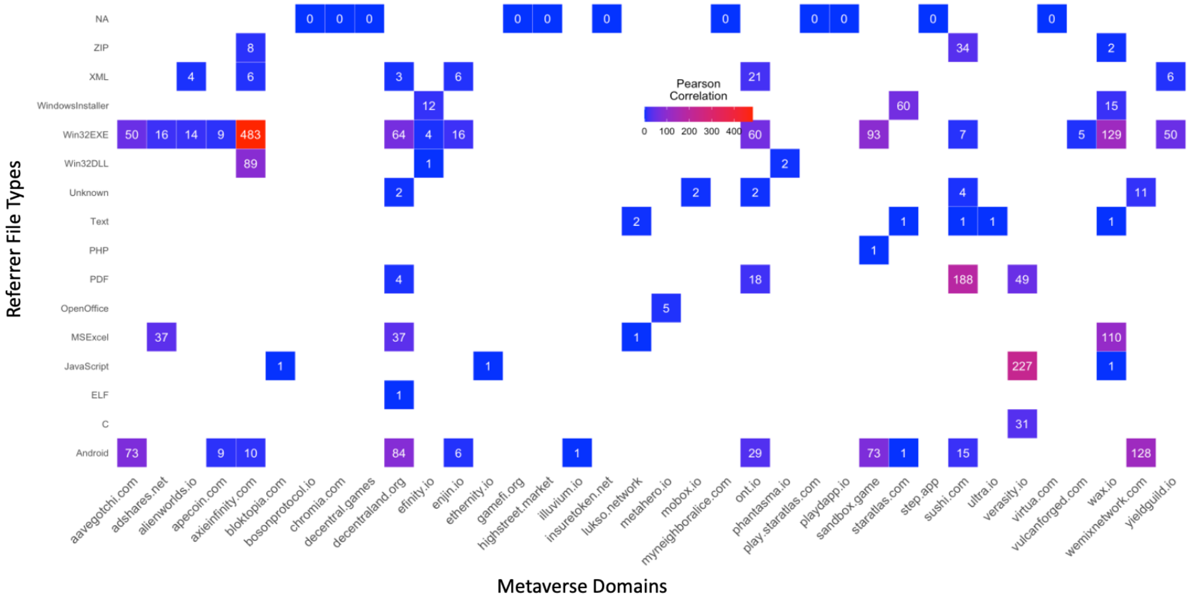

Figure 1: Metaverse Domain with Infected Referrer Files

The heatmap in Fig 3 displays a significant number of communication files with malicious detections. It was discovered that metaverse domains that had malicious detections also had communication files with malicious detections. The Win32 EXE and Android file types were more commonly found than others. The Win32 EXE file type had more detections and was present in approximately 25 out of 31 metaverse domains with malicious detections. Fig 3 provides a visualization of the total occurrences of each file type in the metaverse domains, with Android and Win32 EXE file types following the same pattern as previously observed. These two file types are dominant and contribute significantly to the detections recorded in the metaverse domains.

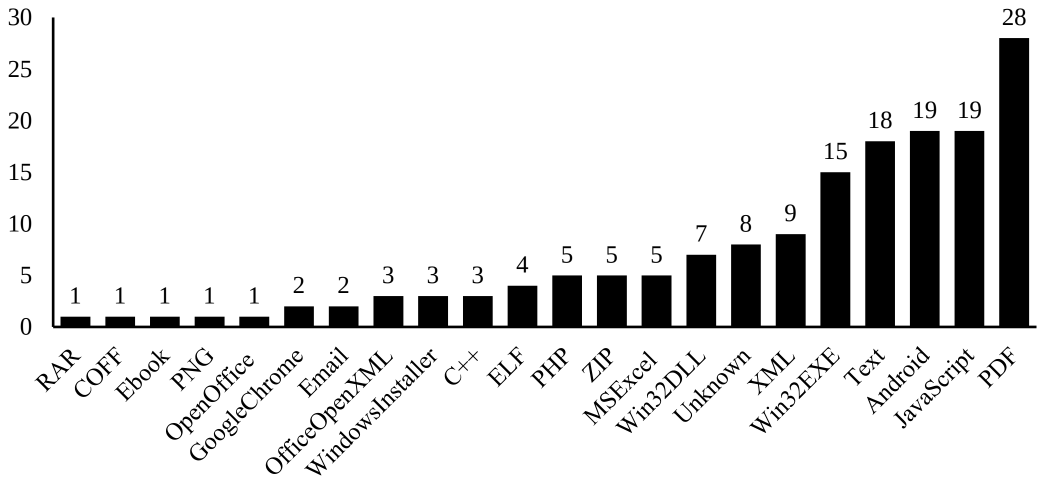

Figure 2: Number of Referrer File Types

4.5.2 Metaverse Coins Market Capitalization

The market capitalization of each metaverse token is obtained from crypto.com[3]. It is important to note that this value is subject to fluctuations, as with other markets. The data provided in this paper reflects the value at a specific point in time and may have since changed. Despite being a futuristic technology, the metaverse already boasts a trillion-dollar market capitalization. The highest-valued token is worth over a billion USD, while the lowest is approximately one thousand USD.

Table 1 shows the list of metaverse tokens in descending order based on market capitalization for the domains with at least 25 million USD capitalization.

Observations. We analyzed the top metaverse token with at least a market capitalization of about 25 million USD for vulnerability and malicious activities by performing a scan with third-party software. The scan result reveals various malicious detections in 31 out of the 44 metaverse domains, representing about 70% of the domains under consideration as shown in Figure 1 and Figure 3. The malicious detections reported are those obtained from the scan of the metaverse domains, IP addresses, communication files, and referrer files associated with the domains.

4.5.3 Malicious Activities in Metaverse Coins

Using Virustotal.com, we conduct thorough scans of files, IP addresses, and domains using many security engines, each utilizing unique algorithms to detect any sign of malicious activity. It is important to note that these engines may classify results differently, which is why we meticulously scrutinize associated components such as passive DNS, communication files, and referrer files to determine the presence of any malicious activity accurately.

[3] https://crypto.com/price/categories/metaverse

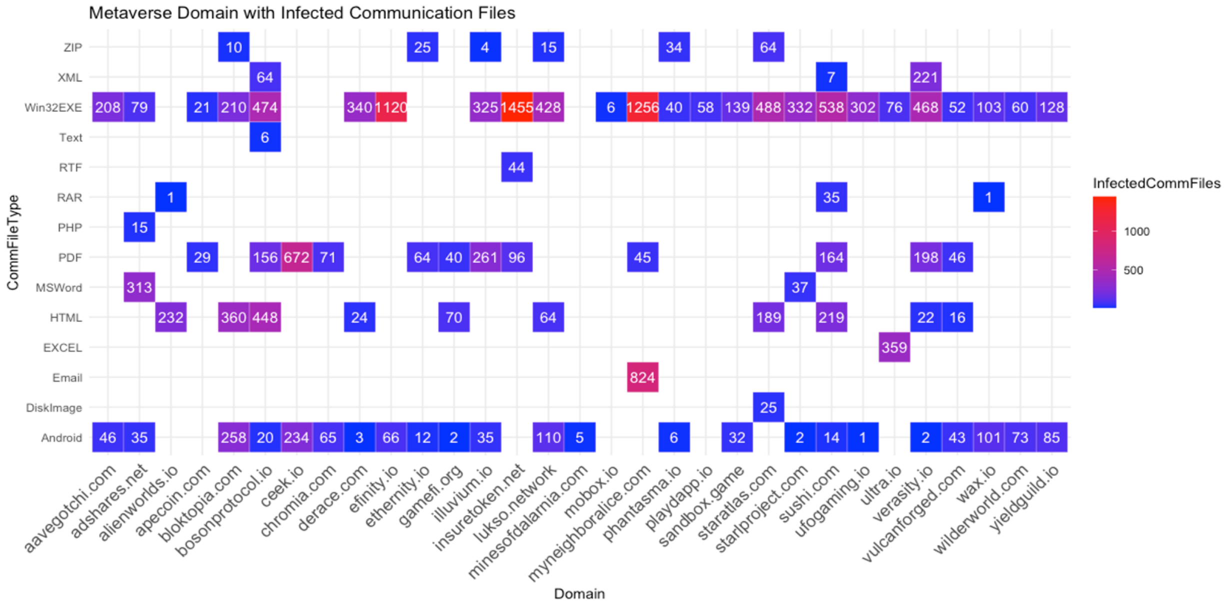

Figure 3: Infected Communication File

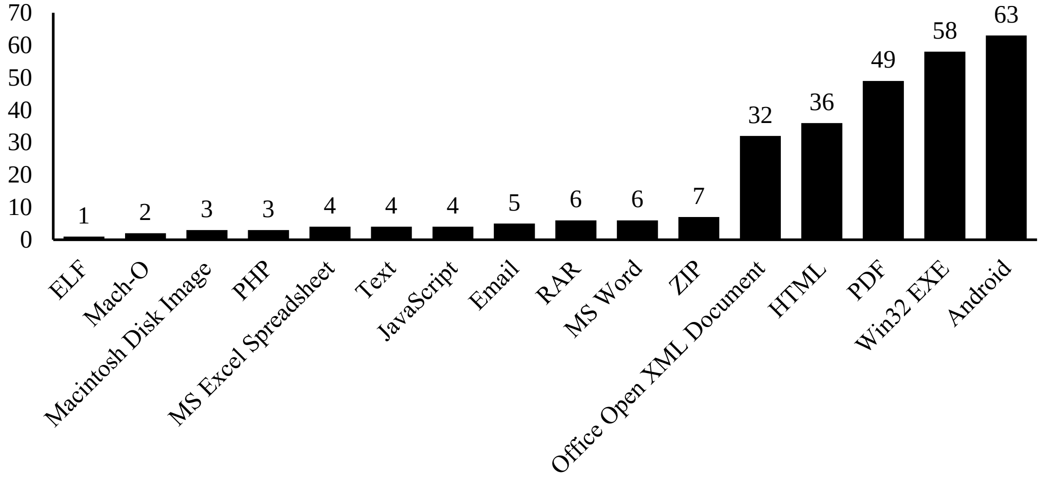

Figure 4: Infected Communication File

Table 8. displays the domains of the metaverse, their corresponding security engines, and the types of malicious detections they can identify. These findings are a result of scanning IP addresses that have been linked to their respective domains.

Observations. We found eight domains to have malicious infections when the domain IP addresses were scanned. Some domains reported more than one type of malicious detection through different security engines used by virustotal.com. The malicious types in the results are shown in Table 8. Malware, malicious, and phishing are types of files found. The CMC Threat Intelligence security engine was more prevalent, appearing eight times. The table shows the relationship between the

Domain	Security Engines	Type	# Files
playdapp.io	Abusix	Malicious	79
playdapp.io	Xcitium Verdict Cloud	Malicious	58
playdapp.io	CMC Threat Intelligence	Malware	46
bloktopia.com	CMC Threat Intelligence	Malware	210
illuvium.io	CMC Threat Intelligence	Malware	261
bloktopia.com	CMC Threat Intelligence	Malware	360
step.app	Xcitium Verdict Cloud	Malware	544
sushi.com	CMC Threat Intelligence	Malware	588
sushi.com	CMC Threat Intelligence	Malware	655
sushi.com	Criminal IP	Malicious	124
efinity.io	Xcitium Verdict Cloud	Malware	680
myneighboralice.com	Xcitium Verdict Cloud	Malware	822
myneighboralice.com	CMC Threat Intelligence	Malware	824
myneighboralice.com	Xcitium Verdict Cloud	Phishing	248
myneighboralice.com	Xcitium Verdict Cloud	Phishing	840
bosonprotocol.io	CMC Threat Intelligence	Malware	1220

Table 7: Malicious detection and types

metaverse domain and communication files. Every domain that has malicious detection records corresponding communication files. The communications files have shown to have some files with malicious detection, and these files will invariably infect the host domain with malware, phishing, and other maliciousness.

Security Engines	Malicious Type	Count of Malware
CMC Threat Intelligence	Malware	7
Xcitium Verdict Cloud	Malware	3
Xcitium Verdict Cloud	Phishing	2
Xcitium Verdict Cloud	Malicious	1
Abusix	Malicious	1
CMC Threat Intelligence	Malware	1
	Total	15

Table 8: Security engines and Malicious types

4.5.4 Metaverse coins with fiat currency to cryptocurrency

Fiat currency in the metaverse refers to using government-issued currencies, such as traditional national currencies (e.g., USD, EUR, JPY) or digital representations of those currencies within virtual worlds or virtual reality environments.

While virtual worlds primarily operate with their virtual currencies or tokens, some platforms or virtual marketplaces may support the integration of fiat currency as a means of exchange. This integration lets users purchase virtual assets or participate in economic activities using real-world currencies.

Cryptocurrency in the metaverse refers to using digital currencies, typically using blockchain technology, within virtual worlds or immersive virtual environments value [50]. Cryptocurrencies offer a decentralized and secure means of conducting transactions and can play a role in facilitating economic activities within the metaverse.

Categorizing metaverse domains into two groups is crucial for identifying which currency type is more susceptible to malicious activity. These groups include those using fiat currency and those using cryptocurrency. It is important to understand the vulnerabilities associated with each type of currency within these domains.

Observations. After analyzing 44 domains, it was found that 21 of them (48.84%) use fiat currency. Both classifications of domains showed evidence of malicious activity. It was observed that domains using fiat currency did not exhibit any distinct behavior from those using cryptocurrency, nor did it impact market capitalization. The exchange of fiat currency and cryptocurrency in the metaverse domain is considered a potential factor contributing to malicious activity, but the analysis revealed otherwise.

4.6 Discussion

Our analysis revealed several instances of malicious activity within metaverse domains. Interestingly, the location of the domains and the DNS and CDN service providers did not contribute to detecting these malicious activities. Our investigation revealed numerous communication and referrer files within the domains, many containing malware. This discovery was unsurprising, as communication and information exchange are common on metaverse web pages. Unfortunately, cyber infections within domains are quite common. Cyber criminals often select their targets based on reconnaissance activities or random selection. With ongoing cyber attacks on cryptocurrency domains and pools, we anticipate similar threats to emerge within metaverse tokens.

We have gathered communication files from 44 domains and found malicious activity in 31 of them. However, when we directly scanned the domains and their IP addresses, only 8 out of the 44 domains showed signs of malicious activity, as shown in Fig 5. This means that the number of domains with malicious activity after a direct scan using virustotal.com is much smaller than reported from the communication files and referrer files. It's possible that the large number of communication files with malicious detection does not necessarily translate to domain infections. This could be due to various reasons, such as the domains having security checkpoints, anti-malware, firewalls, or policies that prevent infections from corrupt communication files. While our study doesn't dive deeply into communication files, we can conclude that the eight domains we identi-

Domain	Fiat Currency	Domain	Fiat Currency
apecoin.com	No	minesofdalarnia.com	Yes
decentraland.org	No	myneighboralice.com	Yes
axieinfinity.com	No	efinity.io	Yes
sandbox.game	No	insuretoken.net	Yes
enjin.io	No	bloktopia.com	Yes
wemixnetwork.com	No	yieldguild.io	Yes
sushi.com	No	staratlas.com	Yes
ont.io	No	virtua.com	Yes
illuvium.io	No	aavegotchi.com	Yes
wax.io	No	ufogaming.io	Yes
lukso.network	No	adshares.net	Yes
playdapp.io	No	gamefi.org	Yes
highstreet.market	No	starlproject.com	Yes
chromia.com	No	play.staratlas.com	Yes
vulcanforged.com	No	wilderworld.com	Yes
decentral.games	No	step.app	Yes
ceek.io	No	ethernity.io	Yes
mobox.io	No	bosonprotocol.io	Yes
raca3.com	No	derace.com	Yes
ultra.io	No	metahero.io	Yes
verasity.io	No	phantasma.io	Yes
alienworlds.io	No		

Table 9: Metaverse Fiat to Cryptocurrency

fied also had communication files with malicious activity.

The website Virustotal.com has its own passive DNS service. We have noticed that the passive DNS results show many malicious detections. Passive DNS stores DNS queries for future analysis, which can help detect malicious networks or infrastructure. However, we cannot confirm if the malicious detections in passive DNS are directly linked to the malicious activities in the eight domains mentioned in Fig 5. It is worth noting that these eight domains are also present in the passive DNS malicious results, as seen in communication files.

The body of the analysis is based on several scan results from virutotal.com.

4.7 Conclusion and Future Work

Our research analyzes the top metaverse tokens with a market capitalization of at least 25 million USD. We examined the corresponding domains and IP addresses and scanned them for malicious activity using virustotal.com. We found that while many associated files had malicious activity, only 18.6% of the domains showed signs of maliciousness. Although our analysis confirms the

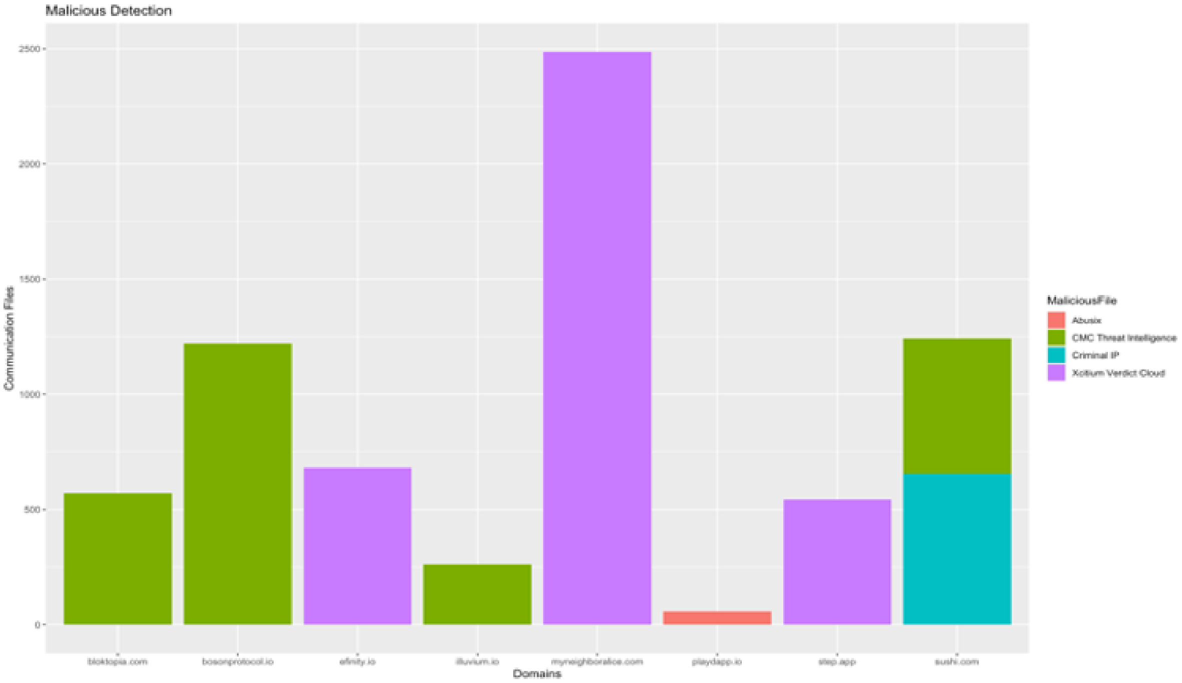

Figure 5: Metaverse Domains with Malicious Detection Types

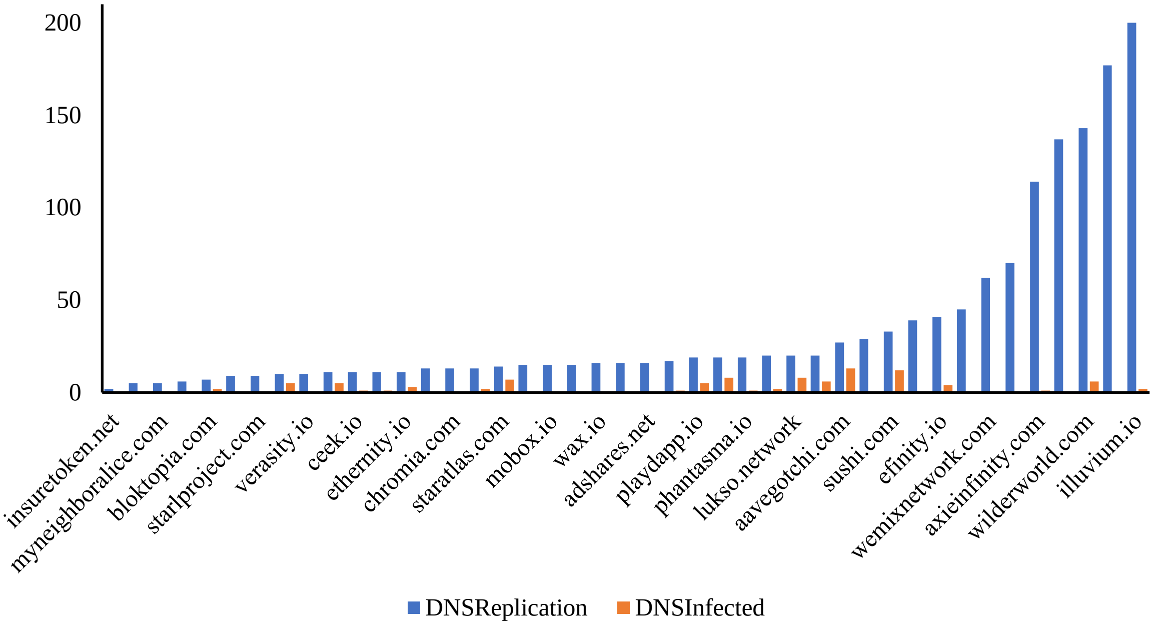

Figure 6: Metaverse Domains with Malicious Detection Types

presence of malicious activity in metaverse domains, we were unable to determine the contributing factors. Further research is necessary to identify the sources and factors that contribute to potential malicious activities in the metaverse.

The confirmation of malicious activities in metaverse domains is undeniable, according to the study. It should be noted that a high market capitalization of tokens does not necessarily indicate a lack of maliciousness. The study has identified various forms of maliciousness that must be taken seriously. In the future, we will expand the number and range of metaverse domains for our analysis, expand the study into fiat currencies and their association with the security of the metaverse, and further look into the payload (files) in the metaverse platform and their contribution to the security of such systems.

5 CryptoJacking Infrastructure Analysis in Cryptocurrency.

5.1 Summary of Completed Work

This study investigates the geographical distribution of websites containing cryptojacking malware across diverse regions and domains. It explores the correlation between malicious cryptojacking websites and internet penetration rates in developed nations. Notably, the United States emerges as a prominent host of such websites, exhibiting the highest frequency of occurrences. The analysis of geographical patterns reveals a notable concentration of cryptojacking activities within countries characterized by elevated internet density and extensive website hosting infrastructure. The primary objective of this research is to underscore the prevalence of cryptojacking malware within these geographic regions and advocate for enhancing security protocols to counter this persistent threat effectively.

5.2 Introduction

The cyberattack known as ”cryptojacking” occurs when unauthorized individuals or entities utilize another computer resources for the purpose of mining cryptocurrencies. This type of attack is also referred to as cryptocurrency mining malware or malicious crypto mining. To maintain the security and validity of blockchain transactions, the process of mining cryptocurrencies requires solving intricate mathematical problems, which demands a considerable amount of computational power and energy [30].

A cryptojacking attack is a type of cyberattack in which the perpetrator gains unauthorized access to a computer, server, or network of devices and installs malicious software [28]. The goal of this software is to use the computing resources of the compromised systems for cryptocurrency mining. This activity takes place without the owners' knowledge or permission. The cryptocurrency industry has unfortunately been plagued by malicious activities, and cryptojacking remains a significant threat [27]. Due to the high costs of establishing and maintaining cryptocurrency infrastructures, attackers frequently exploit platforms owned by others to carry out their nefarious activities [11]. By commandeering existing infrastructures, they are able to launch attacks against their desired target without incurring any of the associated expenses.

The process of cryptocurrency mining is both intricate and demanding, calling for substantial investment. Unfortunately, potential profits often tempt attackers who actively search for systems that can generate the greatest returns [19]. In the past, private servers, which consumed vast amounts of energy, were primarily utilized for mining. Nowadays, cloud-based servers offer a more accessible, cost-effective option. However, some miners will resort to hijacking infrastructures owned by others to maximize their profits.

The objective of this paper is to analyze some websites infrastructure that were previously associated with cryptojacking activities, we want to understand the present status of these malicious websites if they are still actively malicious either with cryptojacking malware or with other sort of malware. We also want to understand the geographical distribution of these websites and extract other information to provide insight into these websites. We will discuss the security risks and threats posed by cryptojacking infrastructures and activities.

5.3 Problem Statement and Research Questions

The process of generating a new cryptocurrency involves mining, which produces new units of cryptocurrency and adds transactions to the blockchain [17]. This complex process includes solving intricate mathematical problems that ensure the validation and security of transactions on the blockchain network [4]. The process of mining cryptocurrency differs from one type to another. There are also varying consensus algorithms, such as Proof of Work (PoW) used by Bitcoin, and Proof of Stake (PoS), that determine how new blocks are added to the blockchain [7].

Mining cryptocurrencies demands substantial computational power, particularly in PoW systems. Miners must have access to robust hardware to solve intricate mathematical problems, which has led to the emergence of cryptojacking. We have analyzed the components and properties of cryptojacking infrastructures to gain insight into their operations. Our goal is to address the challenges posed by these infrastructures by answering three crucial research questions.

1. **RQ1: What is the likely transition of a website from being malicious because of cryptojacking to benign?** We conduct an in-depth analysis of malicious websites to determine the level of malicious activity they exhibit over time. This enables us to gain a better understanding of whether malware has been effectively removed in the aftermath of an attack.

2. **RQ2: what are the categories of malicious contents and malware that are common in these cryptojacking infrastructure?** We analyzed various websites and categorized different types of malicious content and malware that are commonly associated with cryptojacking activities. Our findings can provide valuable insights into the different categories of threats.

3. **RQ3: What are the hosting patterns and the geographical distribution of cryptojacking infrastructure?** The websites identified as malicious are hosted in different countries across the world. This analysis will help in understanding the geographical distribution of the websites.

5.4 Technical Approach

This study analyzed websites that use mining scripts for cryptocurrency mining to gain insights into the nature of cryptojacking infrastructures. The study hypothesizes that there may be potential relationships between cryptojacking and other malicious activities like phishing campaigns, malware distribution networks, or botnets. We started by analyzing the websites with the Whois tool to gather information about the domain, IP addresses, name servers, and registrars.

We obtained 887 malicious websites associated with cryptocurrency mining from MANiC dataset and scanned the websites for malicious content with VirusTotal. After scanning around 880 websites, we found that 371 were clean, while the remaining 518 contained malicious content. Our primary goal is to analyze websites that were detected to contain malicious content. Our analysis aimed to extract valuable information on the types of malicious content, the security engines used to detect them, and the categories classified as malicious or suspicious. This information can help us understand the nature and extent of the threats posed by such websites.

A pipeline of our analysis methods is shown in Figure 7.

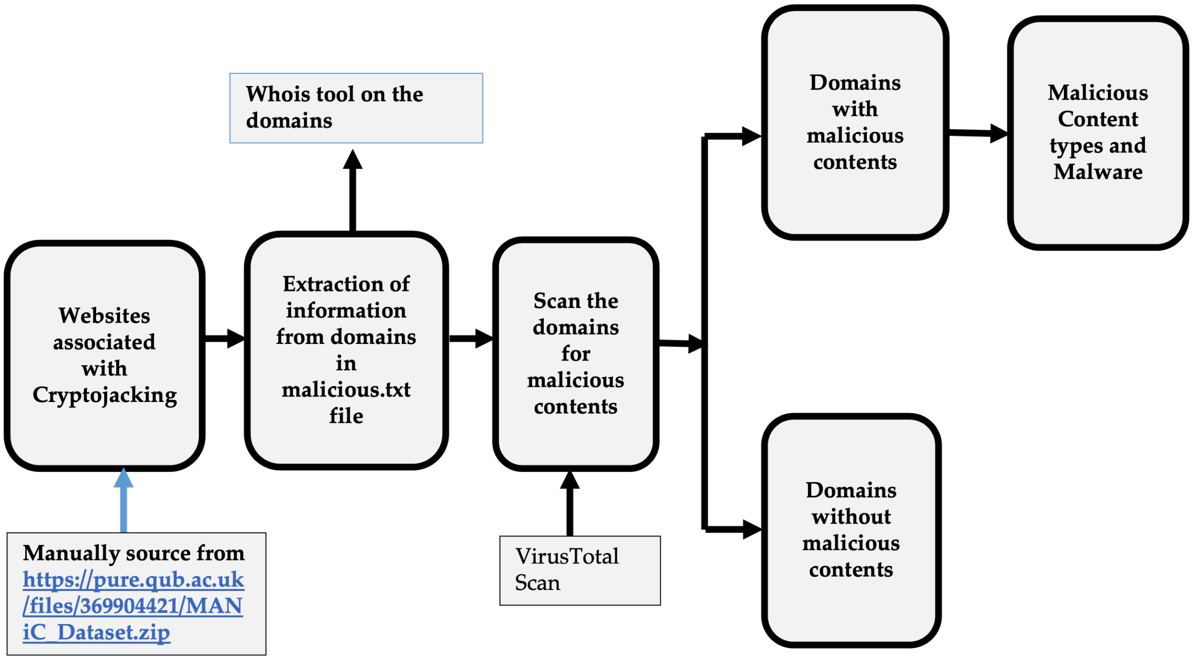
Whois tool on the domains
Websites associated with Cryptojacking
Extraction of information from domains in malicious.txt file
Scan the domains for malicious contents
Domains with malicious contents
Malicious Content types and Malware
Domains without malicious contents
Manually source from https://pure.qub.ac.uk/files/369904421/MANiC_Dataset.zip
VirusTotal Scan

Figure 7: Technical analysis flow

5.4.1 Dataset and Preprocessing

Associated Cryptojacking websites. This paper used the data from the dataset for ”MANiC: Multi-step Assessment for Crypto-miners. The dataset was utilized in the paper titled ”Detecting Cryptomining through Dynamic Analysis.” The data was collected from Alexa’s top 1 million websites (as indexed by Censys) in July 2018. This dataset consists of multiple files. However, we only analyze the malicious file to examine its content. Because the data was collected in 2018, we re-scanned it and discovered the presence of malicious content on 518 websites. We utilized the domain query service to extract information about all the websites in the dataset. We then scanned the dataset to differentiate between infected and clean websites.

Security Data Attributes. Afterward, we conducted a more detailed analysis of the websites in the dataset with malicious infections by scanning them with VirusTotal. We obtained the security engines that performed the scan and categorized the malicious detections into groups. The output of the security engine is classified into method, category, and result. VirusTotal identifies potentially harmful websites with malicious content using the blacklist method. The security engine category may indicate suspicious or malicious activity. Meanwhile, the scan result could be malicious, suspicious, malware, phishing, or spam.

We further analyzed the different types of malware and malicious content associated with each security engine. We have classified various categories of malicious content based on their threat levels and purposes. It is important to note that not all malicious content is related to cryptojacking activity. This classification helps us to identify and concentrate on the malware and other malicious content that may be directly associated with cryptocurrency mining.

5.4.2 Analysis Dimensions

This study aims to examine the infrastructure of cryptojacking by exploring its associated websites. We aim to identify malicious content and the current status of cryptojacking websites. We approach this by examining in different dimensions to provide answers to our research questions. Our discussions is focused on the research questions in section 5.3. The areas covered by our analysis (1) cryptojacking infrastructure websites distribution, (2) threat categories and classifications, (3) Categorize the cryptojacking websites into current status as malicious and benign, and (4) malicious contents in the cryptojacking infrastructures.

5.5 Results and Findings

5.5.1 Cryptojacking malware in the malicious dataset

We have conducted an analysis of the malicious file found in the MANiC dataset. This dataset comprises websites that were found to have related cryptojacking malware. Our analysis revealed the presence of eight (8) different types of cryptojacking malware within the dataset. One of the most significant cryptomining services known as ConHive, which accounted for approximately 74% of the malicious presence in the file, and had ceased its operation in 2019. CoinHive was created for legitimate cryptocurrency mining, but it was hijacked by cybercriminals for cryptojacking. These cryptomining malware were discovered on the websites in the datasets that is analyzed in this study.

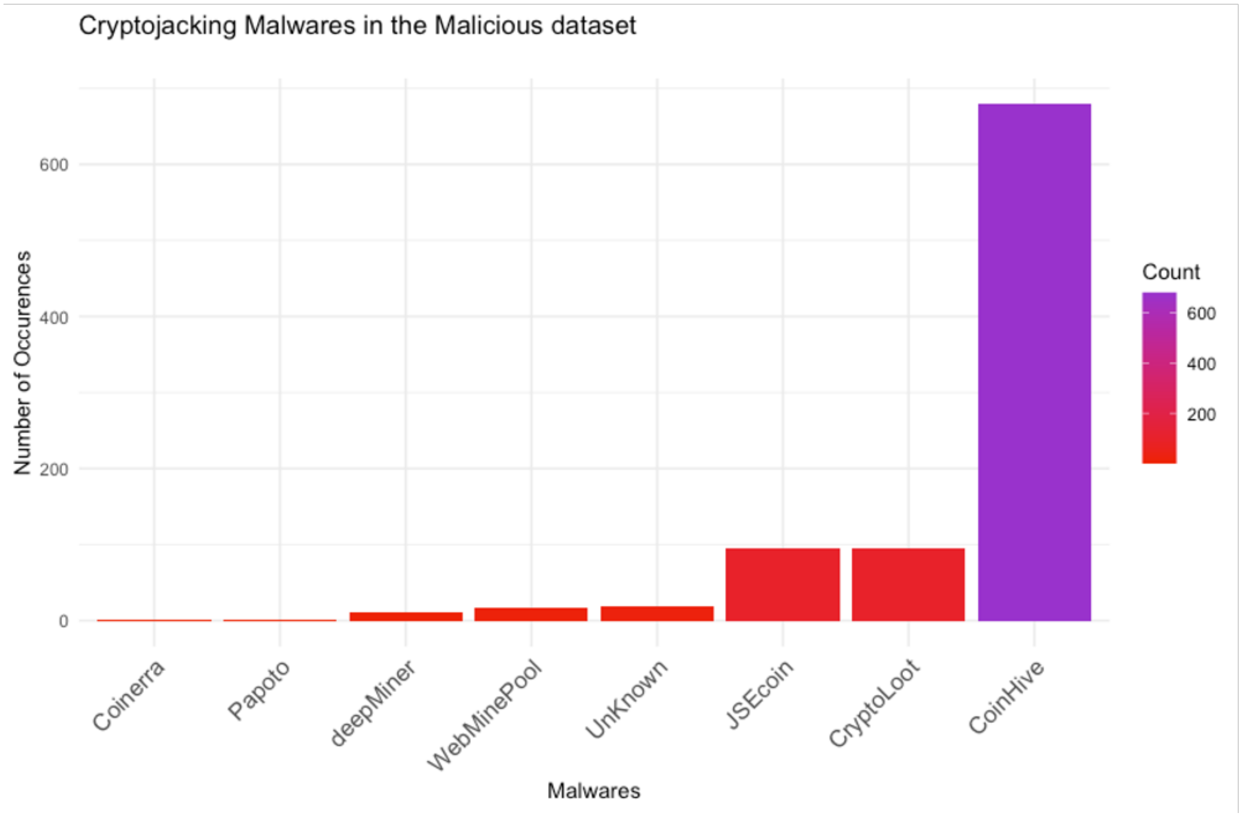

Figure 8: Cryptojacking malware in the malicious dataset

5.5.2 Cryptojacking infrastructure websites distribution

This study undertakes a thorough analysis of a significant number of websites, which are hosted across multiple geographic locations. It is critical to grasp the correlation between the diverse geographical zones where cryptojacking-related websites are situated for two significant reasons. Firstly, it will aid our comprehension of the locations of these websites and their respective hosting countries. Secondly, this examination will offer valuable insights into whether technological advancements and levels of internet penetration are contributing factors. Providing answers to these questions would help us identify the regions that are most affected by cryptojacking activities.

The widespread proliferation of websites worldwide has provided cybercriminals with an opportunity to exploit vulnerable websites for cryptomining, whereby they siphon off the CPU resources. Proper discovery practices will enable vigilance and appropriate measures to safeguard networks against pervasive threats.

Among the 518 websites identified with malicious content, a subset of 116 sites was redacted for undisclosed reasons. As a result, the analysis of country distribution is confined to the unredacted websites. Further examination of these unredacted sites allows for a more focused exploration of geographical trends and patterns associated with malicious online activities.

Country	Count	Percent
USA	188	54.49
Iceland	48	13.91
India	18	5.22
China	13	3.77
Brazil	13	3.77
Great Britain	12	3.48
Canada	7	2.03
Saint Kitts and Nevis	7	2.03
France	7	2.03
Seychelles	6	1.74
Russia	6	1.74
Bahama	6	1.74
Australia	5	1.45
Indonesia	5	1.45
Germany	4	1.16
Total	345	100 %

Table 10: Cryptojacking websites distribution. A heavy-tailed distribution in terms of the number of websites associated with cryptojacking. activities.

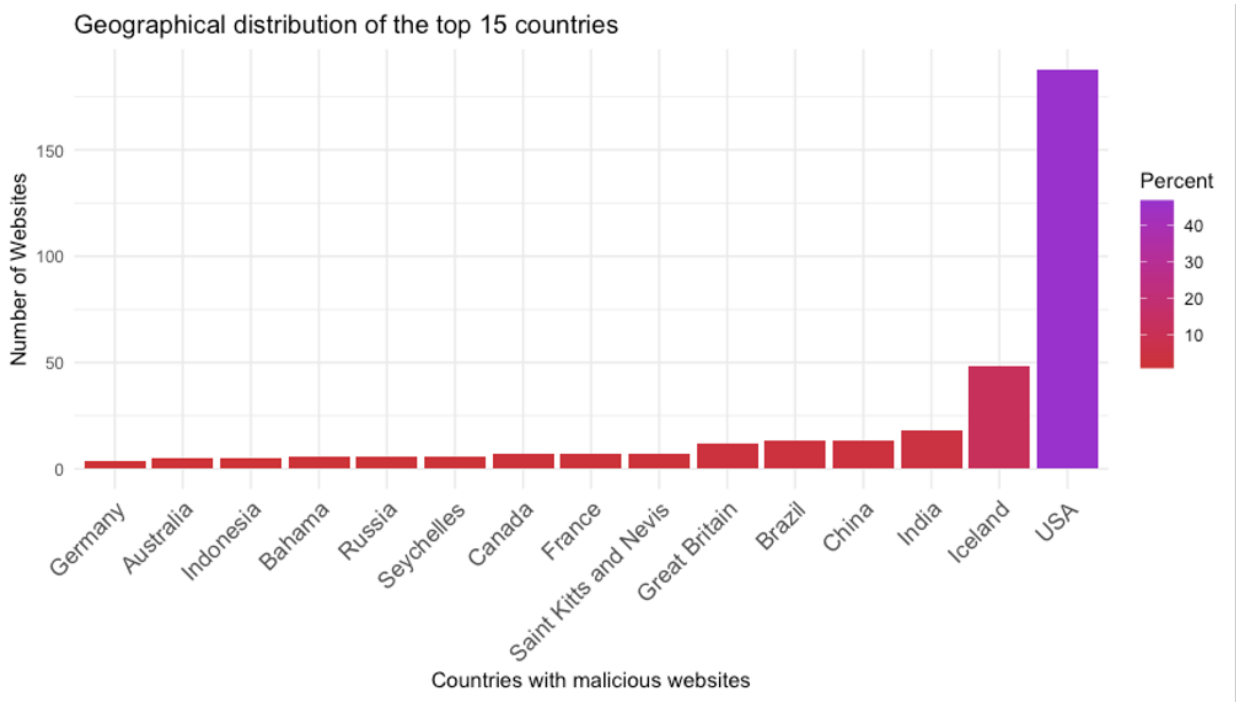

Figure 9: Cryptojacking websites distribution

Observations. Table 10 displays the top 15 countries with the most websites infected with cryptojacking malware, as per our dataset. The websites are spread out in various countries across the Americas, Asia, South America, and Europe. We observed the countries are advanced and have a high internet penetration. The USA has more than 55% of the websites, followed by Iceland, which has about 15%. The USA is known to be well-advanced technologically and hosts most of the domains. The prevalence of cryptojacking websites in the United States may be attributed to the country's significant number of registered websites. Cryptocurrency has gained significant global recognition in recent years. However, it is notable that most cryptocurrency miners reside in regions with high internet penetration and reliable electricity access. Despite the widespread popularity of cryptocurrency investment and trading, the concentration of mining activities in such regions highlights the importance of favorable infrastructure for this practice. This observation suggests a correlation between the two variables and warrants further investigation.

5.5.3 Threat categories and classifications

The virustotal is the primary tool we use in scanning malicious websites. After scanning, we detected various types of malicious activities such as phishing, malware, and spyware from different security engines and we focused on these security engines and the reported malicious contents to gain more insight. While the direct result from the virustotal does not directly indicate cryptomining related scripts but with further analysis of the referrer files, we discovered related cryptomining script. The scan reported a total of 27 security engines with 7 with presence of malicious contents. Table 2 shows the security engines with the summary of the corresponding malicious and suspicious contents.

Forcepoint ThreatSeeker	**Dr. Web**	**Webroot**	**alphaMountain.ia**	**Sophos**	**XcitiumVerdictCloud**	**BitDefender**
media file download	adult content	Malware Sites	Suspicious	spywareandmalware	mediasharing	proxies
compromised websites	known infection source	Peer to Peer	Malicious	puaother	spywareandmalware'	filesharing
proxy avoidance	gambling	BitDefender: porn	Unrated	phishingandfraud		webproxy
application and software download		Proxy Avoidance and Anonymizers	Anonymizers	Suspicious		
hacking		Phishing and Other Frauds	JSEcoin	spamurls		
potentially unwanted software		Spyware and Adware	Scam/Illegal/Unethical	proxies		
coinHives			CoinHives			
suspicious content			Piracy/Plagiarism			
peer-to-peer file sharing						
uncategorized						

Table 5.5.3 contains the list of the top 15 security engines and the number of malicious contents. These contents include malicious, suspicious and undetected contents.

Security Engine	**Count**
alphaMountain.ai	187
Sophos	87
Fortinet	54
Webroot	39
Seclookup	39
Forcepoint ThreatSeeker	35
Scumware.org	14
Bfore.Ai PreCrime	8
CyRadar	7
Xcitium Verdict Cloud	6
Avira	6
CRDF	6
Quttera	5
Heimdal Security	4
Yandex Safebrowsing	3

Table 11: Security Engines Categories

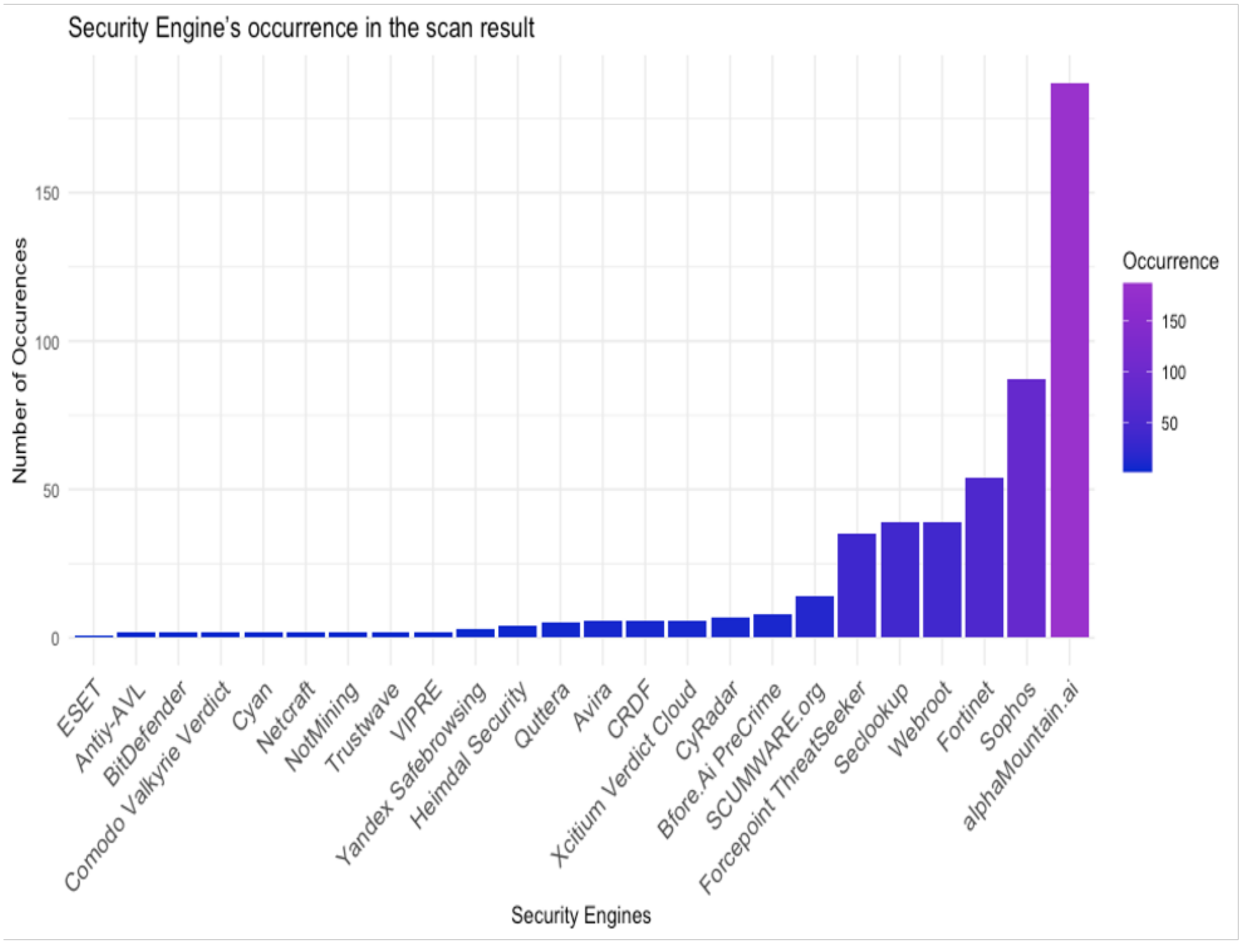

Figure 10: Security Engines Classification

Observations. The outcome of a security scan is determined by the ability of the security engine to accurately identify and classify a malicious item. Sometimes, it may give a positive result for an instance of false positives. It is important to note that the scan results are based on a specific period and could change over time due to modifications in website security or updates to the security engines to correctly identify undetected or misclassified files.

5.5.4 Malicious contents in the cryptojacking infrastructures

The results from the virustotal scan are classified into four categories: harmless, malicious, suspicious, and undetected. Harmless files and contents are considered benign and do not pose a direct or indirect threat. The scan result in the Table 12 shows that the most prominent files detected were harmless contents.The presence of malicious contents in files can be dangerous and can cause harm. These contents can be injected into infrastructure for various reasons, including cryptocurrency mining, which involves using website resources for mining purposes. Malicious files can also be used to bring down websites, make them temporarily unavailable, or even hijack them until a ransom is paid. This is a summary of the malicious files that have been identified, listed in Table 5.5.3. Files that are suspicious but cannot be definitively classified as malicious are also included in this category. If the security engine algorithms are unable to detect or classify a file, it is marked as undetected.

	Harmless	Malicious	Suspicious	Undetected
Count	35370	948	395	8394

Table 12: Security Engine - threat classification

In Table 13, We analyzed 887 websites and found that 58% are malicious and contain either suspicious or malicious files. The remaining 42% are harmless or have undetected files.

Websites	Count	Percent
Malicious	517	58.29
Non-Malicious	370	41.71

Table 13: Websites Categories

For further analysis, Table 14 provides the summary of the malicious websites referenced in Table 13, We categorize the files into three: benign, suspicious, and malicious. These websites contains benign or harmless files but the presence of malicious and suspicious files qualifies them as malicious websites.

Observations. According to the data presented in the table, it can be observed that the number of benign and suspicious files is significantly greater than the number of malicious files. The table provides a visual representation of the file distribution regarding their threat level. Notably, the benign files, which are not considered harmful, constitute the majority of the files analyzed, followed by suspicious files, which require further investigation to determine their threat level. On the other hand, the number of malicious files known to be harmful and pose a risk to the system is comparatively smaller.

Security Engines	Benign	Suspicious	Malicious
Forcepoint ThreatSeeker	21	10	4
Dr. Web	0	2	1
Webroot	0	1	5
alphaMountain.ia	7	4	3
Sophos	7	7	5
XcitiumVerdictCloud	1	0	2
BitDefender	12	5	0

Table 14: Malicious Contents

5.6 Discussion

From our analysis, we discovered that there were several malware and malicious contents present on the websites. These malicious contents were categorized as malicious or suspicious. Although not all of them were related to cryptojacking scripts, some of them were. This indicates that these websites are vulnerable to attacks and are infected with other malicious contents besides the cryptomining scripts.

We have observed that some websites previously labeled as malicious in the MANiC dataset do not contain any malicious content now. The reasons behind this observation could be numerous, such as the dataset being outdated or security improvements like software patching, firewalls, increased security awareness among the workforce, and the use of antivirus may have contributed to the reduction of malicious websites in our study. There are indications suggesting that cryptocurrency mining may no longer be a viable option for websites, owing to several reasons. It appears that the enhanced security measures and awareness have proven effective, as evidenced by the absence of other malicious content on these sites. This could have had a significant impact in curbing further attacks, given that cryptocurrency mining is primarily driven by profit motives. The clean websites could also indicate a temporary hijack of the websites.

We noticed that the distribution of websites is heavily skewed, with most of the websites being concentrated in countries with high internet penetration, primarily the United States. This concentration could be attributed to the fact that most domain registrars are also located in these countries. However, it's important to note that while the websites are registered in these countries, the owners may be from different geographic locations. Additionally, the activities on these websites may take place outside the country in which they are registered. The concentration of websites in certain countries and the prevalence of vulnerabilities being targeted by crypto miners may be contributing factors to the heavy tail distribution of malicious websites. During our investigation, we noticed that certain websites had their Registrar and Name servers masked, which made it difficult to determine their locations. This could be due to the website owners' preference for privacy or security reasons, or it could indicate potential malicious activity.

5.7 Limitations, Conclusion and Future Work

5.7.1 Limitations

In this work, we encountered some limitations in analyzing cryptojacking websites; however, we found that these limitations did not significantly impact our analysis results. The identified limitations are enumerated below.

1. **Limitation with the scanning software.** The virustotal vulnerability scanning software reported a large number of files undetected. This could be because the software is unable to

properly categorized and classify the files as either benign or malicious.

2. **Age of the dataset.** The dataset was collected in 2019, we are able to analyzed the data but having a recent dataset could provided more insight. We have to re-scan the websites and re-calssify them as malicious and benign.

3. **Consider only the malicious file.** We have limited our analysis to only malicious files and have excluded benign and suspicious websites from the MANiC dataset. However, we acknowledge that this approach has limitations. We have found that some of the websites included in the malicious files are now classified as benign, which means that some websites previously categorized as suspicious or benign could now be malicious.

5.7.2 Concluding Remarks

Within this report, we have performed a thorough examination of websites that have been taken over for the purpose of cryptocurrency mining through the use of crypto-mining scripts. By utilizing the whois tool, we have successfully identified the geographical distribution of these websites, which are predominantly situated in areas with significant internet usage. Based on our analysis from the `virustotal.com` scan, it has been found that out of the 887 websites that were previously deemed malicious in our dataset, 370 of them have been cleared of any malicious content or crypto-jacking scripts. This may be attributed to improved security measures implemented on the websites or the fact that they are no longer attractive targets for attackers. Our analysis showed that specific websites had been contaminated with crypto-jacking-related malware. This malicious software operates covertly to exploit a user's computer resources for cryptocurrency mining without their authorization or awareness. Our evaluation suggests that these websites could be vulnerable to re-infection. We identified limitations in our study, therefore improving future studies is necessary to provide more insights into cryptojacking.

5.7.3 Future Work

In our work on analyzing cryptojacking websites, we discovered number of areas that further research could provide more insight into the cryptojacking activities. The possible studies we identify for future work are highlighted below.

1. **Identify what can make a website to become a candidate for cryptojacking.** Based on our analysis, we have discovered that there is a connection between the concentration of websites that engage in crypto-jacking and specific geographic locations. We suggest that this may be due to high internet usage in those areas. Further investigation is needed to fully understand the factors that make certain websites more vulnerable to hijacking for crypto-mining purposes.

2. **The average duration of cryptojacking activities on web-based infrastructures.** Varlioglu *et al*. [48] study the status of cryptojacking after the coinhive is shutdown. The research in this paper shows that certain websites are still infected with cryptojacking malware. By determining the average length of time that these websites are hijacked for cryptomining, we can gain insight into the short and long time impact of the cryptojacking activities that can cause lack of resources and increased financial liability for the website owners.

3. **Study on the frequency of re-hijacking a website for cryptojacking.** We have found evidence of cryptojacking-related malware on certain websites, although the data we collected dates back to 2019. This suggests that these websites may have been re-hijacked for crypto mining purposes. Conducting a study to determine how frequently websites are hijacked over a given period of time would help uncover the frequency of these attacks, and whether websites are used temporarily or repeatedly targeted for a prolonged period.

6 Recommendations

Drawing from the insights gleaned from three distinct studies centered on cryptocurrency vulnerabilities, it becomes evident that cryptocurrency introduces an additional layer of threat to various interfacing systems, including the public cloud, metaverse, and website infrastructure. This research underscores the importance of implementing proactive measures aimed at preventing the infiltration of cryptojacking malware, which poses significant risks to the security and integrity of these interconnected systems.

In order to mitigate the risk of cryptojacking malware infiltration, organizations and individuals must adopt a multi-faceted approach to security. This may entail implementing regular updates of websites to patch known vulnerabilities and address emerging threats. Additionally, deploying multiple layers of security protections, such as firewalls, intrusion detection systems, and endpoint security solutions, can help fortify defenses against cryptojacking attacks. Furthermore, integrating ad blockers within web browsers and disabling JavaScript functionality can serve as effective deterrents against malicious scripts deployed by cryptojacking malware.

By adhering to these proactive security measures, stakeholders can bolster their resilience against cryptojacking threats and safeguard the confidentiality, integrity, and availability of their digital assets and infrastructure.

it was observed that cryptojacking malware tends to be prevalent in countries characterized by high levels of internet density. Implementing proactive measures aimed at prevention is essential to mitigate the risk of cryptojacking malware infiltration. Such measures may include ensuring regular updates of websites, deploying ad blockers within web browsers, and turning off JavaScript functionality in web browsers.

7 Concluding Remarks

Given the substantial market capitalization associated with cryptocurrency, the importance of addressing security and vulnerability concerns cannot be overstated. Malicious activities observed in the cryptocurrency sphere can lead to significant financial losses for stakeholders. In the realm of digital commerce, cryptocurrencies operate within a network of interconnected systems that are predominantly blockchain-based. Because of the decentralized nature of blockchain, the validation of cryptocurrency transactions necessitates a sophisticated algorithm that is executed through an intricate mining process. However, the high cost associated with the required hardware and energy consumption can make mining a costly endeavor. Within this dissertation, our focus is on the exploration of security and vulnerability within the realm of cryptocurrency. Our first area of interest delved into the correlation between cryptocurrency and the public cloud. Through comprehensive analysis, we examined multiple cryptocurrency mining pools and their utilization within the public cloud, evaluating their distribution, frequency, and any potential malicious effects they may have on the cloud infrastructure. Secondly,we evaluated the use of cryptocurrencies within metaverse domains. Our evaluation included analyzing these domains' top metaverse coins and cryptocurrency activities. We analyzed metaverse files to identify any malicious content and established a relationship between domains and malicious activities. We analyzed websites that were previously hijacked for cryptocurrency mining. Our study reveals that many websites still have various types of malicious software. We also determined the geographical distribution of these websites and found that the distribution is skewed, with only a few countries responsible for the majority of crypto-jacking websites. In the future, we recommend further research to determine the frequency of re-hijacking of websites for cryptocurrency mining or to identify the factors that make a website attractive and a candidate for cryptojacking.

References

[1] A. Adeniran and D. Mohaisen. Measuring cryptocurrency mining in public cloud services: A security perspective. In *International Conference on Computational Data and Social Networks, CSoNet*, page 128–140, Berlin, Heidelberg, 2023. Springer-Verlag.

[2] H. T. Akkus, S. Gursoy, M. Dogan, and A. B. Demir. Metaverse and metaverse cryptocurrencies (meta coins): Bubbles or future? *Journal of Economics Finance and Accounting*, 9(1):22–29, 2022.

[3] S. M. Y. Aks, M. Karmila, B. Givan, G. Hendratna, H. S. Setiawan, A. S. Putra, S. H. Winarno, T. A. Kurniawan, Y. N. Simorangkir, R. Taufiq, et al. A review of blockchain for security data privacy with metaverse. In *2022 International Conference on ICT for Smart Society (ICISS)*, pages 1–5. IEEE, 2022.

[4] M. Aloqaily and V. Pandit. Ieee conference on blockchain and cryptocurrency(icbc'23). *IEEE Communications Magazine*, 61(11):6–9, 2023.

[5] S. K. Bansal. Linux worm targets internet-enabled home appliances to mine cryptocurrencies, Mar 2014.

[6] E. Bertino and N. Islam. Botnets and internet of things security. *Computer*, 50(2):76–79, 2017.

[7] N. Bhatia, S. Bansal, and S. Desai. A detailed review of blockchain and cryptocurrency. *CoRR*, abs/2303.06008, 2023.

[8] L. Böck, N. Alexopoulos, E. Saracoglu, M. Mühlhäuser, and E. Vasilomanolakis. Assessing the threat of blockchain-based botnets. In *2019 APWG Symposium on Electronic Crime Research (eCrime)*, pages 1–11. IEEE, 2019.

[9] D. Buhalis, D. Leung, and M. Lin. Metaverse as a disruptive technology revolutionising tourism management and marketing. *Tourism Management*, 97:104724, 2023.

[10] J. Burgess, P. O'Kane, D. Carlin, and S. Sezer. Manic: Multi-step assessment for crypto-miners. In *International Conference on Cyber Security and Protection of Digital Services 03/06/2019 → 04/06/2019 Oxford, United Kingdom*. Institute of Electrical and Electronics Engineers Inc., Oct. 2019. International Conference on Cyber Security and Protection of Digital Services, CyberSecurity2019 ; Conference date: 03-06-2019 Through 04-06-2019.

[11] D. Carlin, J. Burgess, P. O'Kane, and S. Sezer. You could be mine(d): The rise of cryptojacking. *IEEE Secur. Priv.*, 18(2):16–22, 2020.

[12] D. Carlin, P. O'Kane, S. Sezer, and J. Burgess. Detecting cryptomining using dynamic analysis. In *Proceedings of the 2018 International conference on privacy, security, and trust (PST 2018)*, Aug. 2018. Privacy, Security and Trust 2018, PST 2018 ; Conference date: 28-08-2018 Through 30-08-2018.

[13] M. Choi, A. Azzaoui, S. K. Singh, M. M. Salim, S. R. Jeremiah, and J. H. Park. The future of metaverse: Security issues, requirements, and solutions. *Human-Centric Computing and Information Sciences*, 12, 2022.

[14] R. Di Pietro and S. Cresci. Metaverse: Security and privacy issues. In *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, pages 281–288, 2021.

[15] S. Eskandari, A. Leoutsarakos, T. Mursch, and J. Clark. A first look at browser-based cryptojacking. In *IEEE European Symposium on Security and Privacy Workshops, EuroS&P Workshops, London, United Kingdom*, pages 58–66, Apr 2018.

[16] M. S. Farooq, K. Ishaq, M. Shoaib, A. Khelifi, and Z. Atal. The potential of metaverse fundamentals, technologies, and applications: A systematic literature review. *IEEE Access*, 11:138472–138487, 2023.

[17] M. Garriga, M. Arias, and A. D. Renzis. Blockchain and cryptocurrency: A comparative framework of the main architectural drivers. *CoRR*, abs/1812.08806, 2018.

[18] I. Giechaskiel, C. Cremers, and K. B. Rasmussen. When the crypto in cryptocurrencies breaks: Bitcoin security under broken primitives. *IEEE Secur. Priv.*, 16(4):46–56, 2018.

[19] M. Hajiaghapour-Moghimi, E. Hajipour, K. A. Hosseini, M. Tavakkoli, S. Fattaheian-Dehkordi, M. Vakilian, and M. Lehtonen. Hedging investments of grid-connected PV-BESS in buildings using cryptocurrency mining: A case study in finland. *IEEE Access*, 11:66327–66345, 2023.

[20] D. Y. Huang, H. Dharmdasani, S. Meiklejohn, V. Dave, C. Grier, D. McCoy, S. Savage, N. Weaver, A. C. Snoeren, and K. Levchenko. Botcoin: Monetizing stolen cycles. In *The Network and Distributed System Security Symposium*, 2014.

[21] T. A. Jaber. Security risks of the metaverse world. *International Journal of Interactive Mobile Technologies*, 16(13), 2022.

[22] K. Jayasinghe and G. Poravi. A survey of attack instances of cryptojacking targeting cloud infrastructure. In *APIT 2020: 2nd Asia Pacific Information Technology Conference, Bali Island, Indonesia, January, 2020*, pages 100–107. ACM, 2020.

[23] A. Kharraz, Z. Ma, P. Murley, C. Lever, J. Mason, A. Miller, N. Borisov, M. Antonakakis, and M. Bailey. Outguard: Detecting in-browser covert cryptocurrency mining in the wild. In L. Liu, R. W. White, A. Mantrach, F. Silvestri, J. J. McAuley, R. Baeza-Yates, and L. Zia, editors, *The World Wide Web Conference, WWW 2019, San Francisco, CA, USA, May 13-17, 2019*, pages 840–852. ACM, 2019.

[24] H. Kim, J. Park, H. Kwon, K. Jang, S. J. Choi, and H. Seo. Detecting block cipher encryption for defense against crypto ransomware on low-end internet of things. In *WISA*, pages 16–30. Springer, 2020.

[25] H. Krishnan, S. Saketh, and V. Vaibhav. Cryptocurrency mining transition to cloud. *International Journal of Advanced Computer Science and Applications*, 6, 2015.

[26] N. Kshetri. The economics of the industrial metaverse. *IT Prof.*, 25(1):84–88, 2023.

[27] N. Kshetri, M. M. Rahman, S. A. Sayeed, and I. Sultana. cryptoran: A review on cryptojacking and ransomware attacks w.r.t. banking industry - threats, challenges, & problems. *CoRR*, abs/2311.14783, 2023.

[28] N. Kshetri and J. M. Voas. Cryptojacking. *Computer*, 55(1):18–19, 2022.

[29] P. Kürtünlüoğlu, B. Akdik, and E. Karaarslan. Security of virtual reality authentication methods in metaverse: An overview. *arXiv preprint arXiv:2209.06447*, 2022.

[30] A. Menati, Y. Cai, R. E. Helou, C. Tian, and L. Xie. Optimization of cryptocurrency mining demand for ancillary services in electricity markets. In T. X. Bui, editor, *57th Hawaii International Conference on System Sciences, HICSS 2024, Hilton Hawaiian Village Waikiki Beach Resort, Hawaii, USA, January 3-6, 2024*, pages 3052–3061. ScholarSpace, 2024.

[31] P. P. Momtaz. Some very simple economics of web3 and the metaverse. *FinTech*, 1(3):225–234, 2022.

[32] F. N. Naseem, A. Aris, L. Babun, E. Tekiner, and A. S. Uluagac. MINOS: A lightweight real-time cryptojacking detection system. In *28th Annual Network and Distributed System Security Symposium, NDSS 2021, virtually, February 21-25, 2021*. The Internet Society, 2021.

[33] K. Oosthoek and C. Doerr. Cyber security threats to bitcoin exchanges: Adversary exploitation and laundering techniques. *IEEE Trans. Netw. Serv. Manag.*, 18(2):1616–1628, 2021.

[34] R. Perdisci, T. Papastergiou, O. Alrawi, and M. Antonakakis. Iotfinder: Efficient large-scale identification of iot devices via passive DNS traffic analysis. In *IEEE European Symposium on Security and Privacy, EuroS&P 2020*, pages 474–489. IEEE, 2020.

[35] L. Rosenberg. Marketing in the metaverse and the need for consumer protections. In *13th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference, UEMCON*, pages 35–39. IEEE, 2022.

[36] L. Rosenberg. Marketing in the metaverse: Emerging risks. In K. Arai, editor, *Future of Information and Communication Conference (FICC)*, volume 651 of *LNCS*, pages 41–51. Springer, 2023.

[37] J. Rüth, T. Zimmermann, K. Wolsing, and O. Hohlfeld. Digging into browser-based crypto mining. In *Proceedings of the Internet Measurement Conference 2018*, IMC '18, New York, USA, 2018. ACM.

[38] M. Saad, S. Chen, and D. Mohaisen. Syncattack: Double-spending in bitcoin without mining power. In *ACM Conference on Computer and Communications Security*, pages 1668–1685. ACM, 2021.

[39] M. Saad, J. Choi, D. Nyang, J. Kim, and A. Mohaisen. Toward characterizing blockchain-based cryptocurrencies for highly accurate predictions. *IEEE Syst. J.*, 14(1):321–332, 2020.

[40] M. Saad, A. Khormali, and A. Mohaisen. End-to-end analysis of in-browser cryptojacking. *CoRR*, abs/1809.02152, 2018.

[41] M. Saad, A. Khormali, and A. Mohaisen. Dine and dash: Static, dynamic, and economic analysis of in-browser cryptojacking. In *2019 APWG Symposium on Electronic Crime Research, eCrime 2019, Pittsburgh, PA, USA, November 13-15, 2019*, pages 1–12. IEEE, 2019.

[42] M. Saad and D. Mohaisen. Analyzing in-browser cryptojacking. *CoRR*, abs/2304.13253, 2023.

[43] A. Sari and S. Kilic. Exploiting cryptocurrency miners with oisnt techniques. *Transactions on Networks and Communications*, 5(6), 2017.

[44] R. Tahir, M. Huzaifa, A. Das, M. Ahmad, C. A. Gunter, F. Zaffar, M. Caesar, and N. Borisov. Mining on someone else's dime: Mitigating covert mining operations in clouds and enterprises. In *International Symposium on Research in Attacks, Intrusions and Defenses (RAID), Atlanta, GA, USA*, pages 287–310, Sept 2017.

[45] S. Tariq, A. Abuadbba, and K. Moore. Deepfake in the metaverse: Security implications for virtual gaming, meetings, and offices. *CoRR*, abs/2303.14612, 2023.

[46] E. Tekiner, A. Acar, and A. S. Uluagac. A lightweight iot cryptojacking detection mechanism in heterogeneous smart home networks. In *29th Annual Network and Distributed System Security Symposium, NDSS 2022, San Diego, California, USA, April 24-28, 2022*. The Internet Society, 2022.

[47] The Guardian. Cryptocurrency miners using hacked cloud accounts, google warns, September 2021.

[48] S. Varlioglu, B. Gonen, M. Ozer, and M. F. Bastug. Is cryptojacking dead after coinhive shutdown? In *3rd International Conference on Information and Computer Technologies, ICICT 2020, San Jose, CA, USA, March 9-12, 2020*, pages 385–389. IEEE, 2020.

[49] R. Xiao, T. Li, S. Ramesh, J. Han, and J. Han. Magtracer: Detecting GPU cryptojacking attacks via magnetic leakage signals. In X. Costa-Pérez, J. Widmer, D. Perino, D. Giustiniano, H. Al-Hassanieh, A. Asadi, and L. P. Cox, editors, *Proceedings of the 29th Annual International Conference on Mobile Computing and Networking, ACM MobiCom 2023, Madrid, Spain, October 2-6, 2023*, pages 68:1–68:15. ACM, 2023.

[50] H. Xu, Z. Li, Z. Li, X. Zhang, Y. Sun, and L. Zhang. Metaverse native communication: A blockchain and spectrum prospective. In *2022 IEEE International Conference on Communications Workshops, ICC Workshops 2022, Seoul, Korea, May 16-20, 2022*, pages 7–12. IEEE, 2022.

[51] E. Zaghloul, T. Li, M. W. Mutka, and J. Ren. Bitcoin and blockchain: Security and privacy. *IEEE Internet Things J.*, 7(10):10288–10313, 2020.

[52] R. Zhao, Y. Zhang, Y. Zhu, R. Lan, and Z. Hua. Metaverse: Security and privacy concerns. *Journal of Metaverse*, 3(2):93–99, may 2023.

A Appendix

Table 1 shows the list of metaverse tokens in descending order based on market capitalization for the domains with at least 25 million USD capitalization.

Metaverse Token	**Metaverse Domain**	**Metaverse Token**	**Metaverse Domain**
Apecoin	apecoin.com	Phantasma SOUL	phantasma.io
Decentraland MANA	decentraland.org	Metahero	metahero.io
Axie Infinity AXS	axieinfinity.com	DeRace DERC	derace.com
The Sandbox	sandbox.game	Boson Protocol	bosonprotocol.io
Enjin Coin ENJ	enjin.io	Ethernity Chain ERN	ethernity.io
WEMIX	wemixnetwork.com	Step App FITFI	step.app
SushiSwap SUSHI	sushi.com	Wilder World WILD	wilderworld.com
Ontology ONT	ont.io	Star Atlas	play.staratlas.com
Illuvium ILV	illuvium.io	Starlink	starlproject.com
WAXP	wax.io	GameFi GAFI	gamefi.org
LUKSO LYXe	lukso.network	Adshares	adshares.net
PlayDapp PLA	playdapp.io	UFO Gaming	ufogaming.io
Highstreet HIGH	highstreet.market	Aavegotchi GHST	aavegotchi.com
Chromia CHR	chromia.com	Terra Virtua Kolect TVK	virtua.com
Vulcan Forged PYR	vulcanforged.com	Star Atlas DAO POLIS	staratlas.com
Decentral Games DG	decentral.games	Yield Guild Games YGG	yieldguild.io
CEEK VR	ceek.io	Bloktopia BLOK	bloktopia.com
MOBOX MBOX	mobox.io	inSure DeFi SURE	insuretoken.net
Radio Caca RACA	raca3.com	Efinity Token EFI	efinity.io
Ultra UOS	ultra.io	MyNeighborAlice	myneighboralice.com
Verasity VRA	verasity.io	Mines of Dalarnia DAR	minesofdalarnia.com
Alien Worlds TLM	alienworlds.io		

Table 15: Metaverse Tokens