Miners in the Cloud: Measuring and Analyzing Cryptocurrency Mining in Public Clouds

Ayodeji Adeniran  
University of Central Florida  
Orlando, FL, USA  
aadeniran@Knights.ucf.edu

David Mohaisen  
University of Central Florida  
Orlando, FL, USA  
mohaisen@ucf.edu

ABSTRACT
Cryptocurrencies, arguably the most prominent application of blockchain technology, have been on the rise with a wide mainstream acceptance. A central concept in cryptocurrencies is “mining pools”, groups of cooperating cryptocurrency miners who agree to share block rewards in proportion to their contributed mining power. Despite many promised benefits of cryptocurrencies, they are equally utilized for malicious activities; e.g., ransomware payments, stealthy command, control, etc. Thus, understanding the interplay between cryptocurrencies, particularly the mining pools, and other essential infrastructure for profiling and modeling is important.

In this paper, we study the interplay between mining pools and public clouds by analyzing their communication association through passive domain name system (pDNS) traces. We observe that 24 cloud providers have some association with mining pools as observed from the pDNS query traces, where popular public cloud providers, namely Amazon and Google, have almost 48% of such an association. Moreover, we found that the cloud provider presence and cloud provider-to-mining pool association both exhibit a heavy-tailed distribution, emphasizing an intrinsic preferential attachment model with both mining pools and cloud providers. We measure the security risk and exposure of the cloud providers, as that might aid in understanding the intent of the mining: among the top two cloud providers, we found about 35% and 30% of their associated endpoints are positively detected to be associated with malicious activities, per the virustotal.com scan. Finally, we found that the mining pools presented in our dataset are predominantly used for mining Metaverse currencies, highlighting a shift in cryptocurrency use, and demonstrating the prevalence of mining using public clouds.

CCS CONCEPTS
• Information systems → World Wide Web; • Security and privacy;

KEYWORDS
Cryptocurrencies, Public Clouds, Abuse, Web Security

1 INTRODUCTION
Cryptocurrencies have recently been on the rise, with the top three cryptocurrencies amounting to over a trillion USD in value [18, 19]. With cryptocurrency gradually gaining acceptance, different cryptocurrencies have emerged and are still emerging [20]. Many cryptocurrencies are a direct application of blockchain technology, a distributed ledger over a distributed network of nodes that record transactions [18]. The blockchain distributed system provides a much safer architecture against failure, and that—along with cryptographic primitives—ensure transactions are safer from being altered [1, 2, 13]. Given the importance and value of those cryptocurrencies, cybercriminals have used them as a way to enable their criminal activities [21].

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 [3, 7, 11, 13–15, 17, 23]. 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 [9]. For instance, with the emergency of blockchain-based technologies, malicious transactions are placed on the blockchain to facilitate malicious activities through the distribution of stealthy command and control channels [6]. Given the significant valuation of cryptocurrencies, cryptojacking, an intentional effort to use others’ machines and resources for mining cryptocurrencies has been on the rise [20]. Particularly, the use of cloud resources has been hypothesized to be the main entry point of mining cryptocurrencies [10], although not systematically analyzed.

The focus of this work is to understand the prevalence of public clouds for mining purposes, possibly mining with malicious intent (e.g., with compromised cloud instance). 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 cyberattacks from the private server(s) that can be traced and shutdown 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 is a number of 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 huge and cheap cloud to benefit from, and a difficult-to-decipher blockchain technology to hide their malicious activities, particularly 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.

In this paper, we study the interplay between mining pools and public clouds by analyzing their communication association through passive Domain Name System (pDNS) traces. We observe that 24 cloud providers have some association with mining pools as observed from the pDNS query traces, where two popular public cloud providers—Amazon and Google—have almost 48% of such an association. We found that the cloud provider presence and cloud
provider-to-mining pool association both exhibit a heavy-tailed distribution, emphasizing an intrinsic preferential attachment model with both mining pools and cloud providers. We measure the security risk and exposure of the cloud providers, as that might aid in understanding the intent of the mining: among the top two cloud providers, we found almost 35% and 30% of their associated endpoints are positively detected to be associated with malicious activities, per the virustotal.com scan. Finally, we found that the mining pools presented in our dataset are predominantly used for mining Metaverse currencies, highlighting a shift in cryptocurrency use, and demonstrating the prevalence of mining using public clouds.

**Organization.** The related work is presented in section 2, followed by our dataset overview in section 3, the main results in section 4, the discussion in section 5, and concluding remarks in section 6.

## 2 RELATED WORK

This work is broadly associated with a body of work on cryptomining (irrespective of the tools used for that mining). Tahir et al. [24] studied the abuse of virtual machines in cloud services for mining digital currencies, which is the most related work to ours. Huang et al. [9] were among the first to notice the illegal use of CPU cycles for malware-induced mining. The initial work on web-based cryptomining was presented by Saad et al. [20] and Ruth et al. [17] who measured the prevalence of cryptojacking among websites (i.e., utilizing mining on visitors’ machines).

Ruth et al. [17] 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. [20] conducted a similar study, but on a larger number of websites; 5703 sites in total. Concurrently, Eskandari et al. [8] 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. [20] goes further by conducting code analysis toward the detection of cryptojacking codes and their economic impact.

Bertino and Nayeem [5] 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 [4]. Krishnan et al. [12] studied a series of computer malware, such as TrojanRansom.Win32.Linkup and HKTL_BITCOINMINER, that turned host machines into mining pools. Sari and Kilik [22], used Open Source Intelligence (OSINT) to study vulnerabilities in mining pools with Mirai botnet as a case study.

## 3 DATASET AND PREPROCESSING

The dataset used in this study combines 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 mining domains from the Stelareum mining pool website. This list contains a set of mining pool addresses that are publicly available.

We examined the mining pools and copied the corresponding URLs for each of them. Subsequently, using the popular Digital Envoy IP allocation dataset, 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 conducted a scan 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 [16]. 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 cloud endpoints to the mining pools, and vice versa, at some point in time in the past. The output of the scan consists of the originating IP address of the mining pool and the corresponding IP subnet of the cloud providers.

The scan result includes 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 lines of response (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 then 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.

## 4 RESULTS

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

### 4.1 Analysis Dimensions

In this study, we are 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 providers-specific distribution, and (potential) illicit activities. We define each of those dimensions as we present the associated results.

### 4.2 Results and Discussion

**Cloud Providers and Country of Origin.** There is a large number of public cloud providers that make up the cloud ecosystem. While the major 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 important 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

---

1. https://www.stelareum.io/en/mining/pool.html
2. https://www.digitalenvoy.com/
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 1 shows the cloud providers mapped to countries of their domain registrations. Interestingly, we find that the distribution of the traffic from the mining pools is vastly distributed, covering a large number of providers and countries, 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) towards a few among them: 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%.

Table 1 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.

**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 the 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 cryptomining 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 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 rate of traffic for the mining pools based in China, while Amazon had higher traffic for pools located in the US and in other countries. The geographical location of the mining pool could be a factor in determining the preferred cloud provider before selecting other available providers.

By the same token, we also found that the top two subdomains (corresponding to the sandpool mining pool) 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.
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.

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 1, 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.

5 DISCUSSION

From our analysis, we notice that more associations are reported on the Google cloud platform than on the Amazon platform. The preference of 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 cryptominig. Both cloud providers have instances with computer power resources to handle the cryptominig 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.
Upon digging into the DNS records of their domains, we found that of those main pools, nor their associated subdomains, are detected in our analysis are quite protective of registration information. Given the lack of pDNS data for those domains, it is not surprising that we could not see them in our analysis. To this end, our analysis comes with a caveat: the estimated association between those cloud providers 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 compute resources required for mining and this comes with a price: using someone else’s 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 cryptocurrency mining [25]. Our results allude to a similar outcome, as many of the cloud addresses shown in our analysis are associated with malicious 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.

Our results allude to a similar outcome, 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 compute resources required for mining and this comes with a price: using someone else’s 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 cryptocurrency mining [25]. 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, are 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 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 monitoring is perceived.

6 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 anecdores through characterization.

Acknowledgement

This work is supported in part by NRF grant NRF-2016K1A1A2912757. We would like to thank Omar Alrawi (Georgia Tech) for providing us with the passive DNS dataset used in this study, and for the various insightful discussions.

REFERENCES

[1] Ashar Ahmad, Muhammad Saad, Mostafa Bassiouni, and Aziz Mohaisen. 2018. Towards blockchain-driven, secure and transparent audit logs. In Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services. 443–448.
[2] Ashar Ahmad, Muhammad Saad, Laurent Njilla, Charles Kamhoua, Mostafa Bassiouni, and Aziz Mohaisen. 2019. Blocktrail: A scalable multichain solution for blockchain-based audit trails. In ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE, 1–6.
[3] SungHa Baek, Youngdon Jung, Aziz Mohaisen, Sungjin Lee, and DaeHun Nyang. 2018. SSD-insider: Internal defense of solid-state drive against ransomware with perfect data recovery. In 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS). IEEE, 875–884.
[4] Sudhir K. Bansal. 2014. Linux Worm targets Internet-enabled Home appliances to Mine Cryptocurrencies. https://thehackernews.com/2014/03/linux-worm-targets-internet-enabled.html
[5] Elias Bertino and Nayeem Islam. 2017. Botnets and internet of things security. Computer 50, 2 (2017), 76–79.
[6] Leon Böck, Nikolaos Alexopoulos, Emine Saracoglu, Max Mühlhäuser, and Emmanuel Vasilomanolakis. 2019. Assessing the threat of blockchain-based botnets. In 2019 APWG Symposium on Electronic Crime Research (eCrime). IEEE, 1–11.
[7] Alesia Chenuforkova, Nicolo Gozzi, Simona Boboila, Priyanka Angadi, John Loughner, Matthew Wilden, Nicola Perra, Tina Eliaissi-Rad, and Alina Oprea. 2022. Cyber Network Resilience Against Self-Propagating Malware Attacks. In European Symposium on Research in Computer Security. Springer, 531–556.
[8] Shayan Eskandari, Andreas Leoutsarakos, Troy Mursch, and Jeremy Clark. Apr 2018. A First Look at Browser-Based Cryptojacking. In IEEE European Symposium on Security and Privacy Workshop, EuroS&P Workshops, London, United Kingdom. 58–66. https://doi.org/10.1109/EuroSP.2018.00014
[9] Danny Yuxing Huang, Hitesh Dharmadasani, Sarah Meiklejohn, Yacine Dache, Chris Grier, Damon McCoy, Stefan Savage, Nicholas Weaver, Alex C. Snoeren, and Kirill Levchenko. 2014. Botcoin: Monetizing Stolen Cycles. In The Network and Distributed System Security Symposium.
[10] Amin Khazraei, Zane Ma, Paul Murley, Charles Lever, Joshua Mason, Andrew Miller, Nikita Borisov, Manos Antonakakis, and Michael Bailey. 2019. Outguard: Detecting In-Browser Covert Cryptocurrency Mining. In The World Wide Web Conference, WWW 2019, San Francisco, CA, USA, May 13–17, 2019, Ling Liu, Ryen W. White, Amin Mantrach, Fabrizio Silvestri, Julian J. McAuley, Ricardo Baeza-Yates, and Lei Zda (Eds.). ACM, 840–852. https://doi.org/10.1145/3308558.3313665
[11] Huyun Kim, Jaeheon Park, Hyoseokg Kwon, Kyounghae Jang, Seung Ju Choi, and Hwajeong Seo. 2020. Detecting Block Cipher Encryption for Defense Against Crypto Ransomware on Low-End Internet of Things. In WISA. Springer, 16–39.
[12] H. Krishnan, S. Saketh, and Venkata Vaibhav. 2015. Cryptocurrency Mining: Transition to Cloud. International Journal of Advanced Computer Science and Applications 6 (2015).
[13] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. 2013. A fistful of bitcoins: characterizing payments among men with no names. In Proceedings of the 2013 conference on Internet measurement conference. 127–140.
[14] Aboeldaziz Mohaisen and Omar Alrawi. 2013. Unveiling zeus: automated classification of Ransomware samples. In Proceedings of the 22nd International Conference on World Wide Web. 829–832.
[15] Sergio Pastrana and Guillermo Suarez-Tangil. 2019. A first look at the cryptocurrency mining ecosystem: A decade of unrestricted wealth. In Proceedings of the Internet Measurement Conference. 73–86.
[16] Roberto Perdisci, Thomas Papastergiou, Omar Alrawi, and Manos Antonakakis. 2020. IoTFinder: Efficient Large-Scale Identification of IoT Devices via Passive DNS Traffic Analysis. In IEEE European Symposium on Security and Privacy, EuroS&P 2020. IEEE, 474–489. https://doi.org/10.1109/EuroS&P5459.2020.00037
[17] Jan Rüth, Torsten Zimmermann, Konrad Wolsing, and Oliver Hohlfield. 2018. Digging into Browser-based Crypto Mining. In Proceedings of the Internet Measurement Conference 2018 (Boston, MA, USA) (DNC '18). ACM, New York, USA, 7 pages. https://doi.org/10.1145/3278532.3278539
[18] Muhammad Saad, Songqing Chen, and David Mohaisen. 2021. SyncAttack: Double-spending in Bitcoin Without Mining Power. In ACM Conference on Computer and Communications Security. ACM, 1668–1685. https://doi.org/10.1145/3460120.3484568
[19] Muhammad Saad, Jinchun Choi, DaeHun Nyang, Joongheon Kim, and Aziz Mohaisen. 2020. Toward Characterizing Blockchain-Based Cryptocurrencies for Highly Accurate Predictions. IEEE Trans. 13, 1 (2020), 321–332. https://doi.org/10.1109/TJSYST.2019.2927707
[20] Muhammad Saad, Aminollah Khormali, and Aziz Mohaisen. 2018. 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. IEEE, 1–12. https://doi.org/10.1109/eCrime47957.2019.9037576
[21] Muhammad Saad, Jeffrey Spaulding, Laurent Njilla, Charles Kamhoua, Sachin Shetty, DaeHun Nyang, and David Mohaisen. 2020. Exploring the attack surface of blockchain: A comprehensive survey. IEEE Communications Surveys Tutorials 22, 3 (2020), 1977–2008.
[22] Arif Sari and Seyfullah Kılıçoğlu. 2017. Exploiting Cryptocurrency Miners with ADBot: Analysis of Adblockers for Defense against Crypto Ransomware on Low-End IoT. In Proceedings of the 2017 International Conference on Internet-of-Things and Smart Spaces. Springer, 838–845. https://doi.org/10.1007/978-3-319-55665-6
[23] Ahmad Selim, Ayodeji Adeniran, and David Mohaisen. 2017. Botnets in the Wild: A New Perspective. In Proceedings of the 13th Conference on Computer and Communications Security. 76–79.
[24] Rashid Tahir, Muhammad Huzaifa, Anupam Das, Mohammad Ahmad, Carl A. Gunter, Faredz Zaffar, Matthew Caesar, and Nikita Borisov. Sept 2017. Mining is Perceived. In 2017 IEEE International Conference on Security and Privacy Workshops, EuroS&P Workshops, London, United Kingdom. 73–75. https://doi.org/10.1109/EuroS&P.2017.8092047
[25] The Guardian. 2021. Cryptocurrency miners using hacked cloud accounts, Google warns. shorturl.at/bgwA9

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      |
| poolbtc.com   | CMC Threat Intelligence  | 1      |