Chapter 7

Use of Botnets for Mining Cryptocurrencies

Renita Murimi
University of Dallas

Contents

7.1 Introduction

Botnets, hackers, and computer malware are some of the symptoms resulting from the vulnerabilities of software, systems, and networks. Together, these and other forms of algorithmic nuisance present challenges concerning the integrity of user data, privacy, and fraud. The devices that we use are becoming increasingly sentient and are finding their way into our lives in smart ways through smart phones, wearables, smart cars, smart home appliances, and smart work environments. Consequently, these Internet of Things (IoT) devices have also been confronted with the challenges posed by malware. It might not be long before robots have their own social media accounts, the smart fridge posts its contents online and a human and a bot meet for coffee and embark on a sightseeing tour of a new town in a self-driving vehicle. Our current networks are rapidly turning into massive online networks inhabited by human users, software, firmware, and software bots. But how well are our existing systems able to scale up to the challenges and opportunities presented by such massive online networks?

While user privacy and data fraud are well-known consequences of malware, the ramifications of malware infections extend widely. This chapter explores the threats that malware, specifically, botnets pose to the mining of cryptocurrencies. The reader will be introduced to the history of botnet-inspired threats, operational mechanisms of botnets, and an in-depth look at significant botnets that have attacked cryptocurrencies. Botnets pose distinct security challenges to cryptocurrencies (such as currency theft and clipboard hijacking), by targeting their command and control (C&C) communications framework, destabilizing their consensus protocols and attempting to sway the decentralized architecture in favor of mining pools that employ higher amounts of processing power, use of forks and attacks on cryptocurrency exchanges [1,2]. This chapter also looks at countermeasures in terms of detection, prevention, and thwarting. Finally, the chapter presents implications for growing cryptocurrency usage and therefore, increasing exposure to various security threats, both organized and unintentional, on botnet black markets, IoT devices and from unsuspecting

users. Cryptocurrencies face significant challenges to widespread adoption. One of these challenges is that the mining for cryptocurrencies is computationally expensive. A comparison of the energy consumption index for Bitcoin and Ethereum presents interesting statistics [3]. The estimated annual global mining costs of Bitcoin are 90% of its global mining revenues, with a single transaction taking up 467 KWh. In contrast, the mining costs equal the mining revenue for Ethereum, where a single transaction consumes 46 KWh. To put this in perspective, 100,000 Visa transactions can be performed in the same amount of power that is used to perform a single Bitcoin transaction. Still, the appeal of cryptocurrencies is rising steadily. This is due to several factors. The distributed nature of currency generation ensures that anyone in possession of a computer with modest processing power is potentially able to mine for coins. The anonymity promised by currencies such as Monero (XMR) is especially valuable to entities operating in the cybercriminal underground, or the dark market. The low barrier to entry is rendered even more appealing by the rise of cryptojacking software, which uses browser-based mining software, some of which is potentially capable of launching malware attacks of greater complexity, such as DDoS attacks and password cracking.

The rest of this chapter is organized as follows. Section 7.2 describes a general overview of the consensus operation in cryptomining and describe how threats to the consensus mechanisms could affect the cryptocurrency mining process. Section 7.3 presents information about prominent cryptomining botnets, and Section 7.4 presents countermeasures. Finally, Section 7.5 provides future directions and concludes the chapter.

7.2 Overview of the Consensus Operation in Cryptomining

This section presents an overview of the consensus mechanism in cryptomining and significant threats posed by botnets to the consensus mechanism. From the initial days of using botnets on Internet Relay Chat (IRC) forum channels to their most popular use for spam distribution, botnets have been used for distributed malware propagation. The distributed nature of botnets has found usage in cryptocurrency mining, since both botnet operation and cryptocurrency mining depend on anonymous, distributed transactions. Anonymity is further emphasized in cryptocurrency frameworks where each node is identifiable only by its IP address. This is in contrast to the framework in fiat currencies, where transactions are required to be account-centric and identifiable for traceability and fraud management.

The initial popular use of botnets for spam production began to wane around the year 2013 due to several factors including better email filters, takedown of spam botnets, and legal and regulatory protections. Around this time, botnets were then predicted to be increasingly used in cryptocurrency mining aided by the anonymity

offered by darknets [4,5]. This prediction has come true, as recent research shows that botnets used in cryptocurrency mining and crypto-based ransomware [6] outrank other botnet-based malware applications. Crypto-based ransomware encrypts a user's files and holds it encrypted until the user pays a ransom. The 2019 Internet Security Threat Report [7] presents, among other malware, statistics on ransomware. This report showed that enterprise ransomware had increased by 12% and mobile ransomware attacks were up by 33%. A notable ransomware attack was the Wannacry ransomware cryptoworm in May 2017 that exploited EternalBlue, an exploit developed by the NSA for older, unpatched Windows systems. The Wannacry ransomware was the most widespread encryptor of 2017, and took on the dubious distinction of the Kaspersky lab's "Story of the Year" [8]. Other notable examples of ransomware are CryptoLocker, SamSam, and Petya, which have targeted web servers [7], operating system kernel files, and enterprise software.

The costs of cryptomining are related to the work done in solving cryptographic puzzles. Cryptocurrencies are validated by the consensus protocol, where other nodes on the network perform the proof-of-work to solve a cryptographic puzzle. Traditionally, the computational power required to mine these cryptocurrencies has been harnessed from mining-specific hardware, such as ASIC or GPU processors. ArtForz [9] first appeared as a pseudonym in Bitcoin mining forums around 2010 where he was among the first few developers to mine Bitcoin with his private code. Using a network of 24 Radeon 5970s, dubbed the farm, ArtForz was purported to control a quarter of the mining power at that time, while having mined approximately 4% of the bitcoins available. He also used FPGAs and ASICs, much before ASICs for dedicated mining operations were commercially available. However, a new breed of computationally less-intensive mining exists, where the mining is performed through in-browser files that execute the mining code. In-browser mining of cryptocurrencies will be explained in detail in Section 7.2.2.

Work on the disruption of the consensus protocol was described in [10]. Such an attack, termed the *Goldfinger attack* was studied, where the disruption of the consensus protocol was motivated not only by the financial utility of the players but also by their desire to introduce a hostile takeover through resource misappropriation such as significant computational power or storage space. Another type of attack, called the "eclipse attack," was studied in [11] on nodes with public IP addresses. A fundamental assumption in blockchain is that of perfect information, where each node can observe the proof-of-work done by peer nodes. An eclipse attack impacts this assumption of perfect information by empowering an attack on all the ingoing and outgoing connections of a node to its peers. Thus, it effectively isolates a node, thereby influencing its view of the proof-of-work done by its peer nodes and subsequently the consensus protocol, which enables transactions to be marked as verified and stored on the blockchain. The study focused on attacks originating from infrastructure (ISP, enterprise, and similar domains with contiguous IP address blocks), as well as attacks from

botnets that contain IP addresses from diverse blocks. They showed that their experimental botnet eclipse attacks were more efficient than infrastructure-based attacks, since an attacker needed far fewer nodes in botnets (approximately a tenth of the number of infrastructure-based attacks) to eclipse a target victim.

7.2.1 Browser Evolution and Adaptability for Cryptomining

Since cryptomining code runs in the browser, a brief step back into browser evolution and its current capabilities is in order. This section presents an overview of browser capabilities that can be harnessed for botnet-based attacks, ranging from the more popular attacks such as cryptojacking to others such as clipboard hijacking.

7.2.1.1 HTML, CSS, JavaScript, HTML5

The first version of HTML was developed by Tim Berners-Lee in 1993. Since then, HTML has evolved from being a simple mark-up language containing only 18 elements in its first version to becoming the foundation on which cores, apps, scripts, and frameworks are built. The introduction of JavaScript, a scripting language for application programming on the Web developed by Brendan Eich in the mid-1990s, created an avenue for developing interactive web pages. Together with HTML and CSS, JavaScript has emerged as a core technology for web development that could be used on server and client machines. HTML has since undergone substantial revisions. Aided by the Internet Engineering Task Force (IETF) and World Wide Web Consortium (W3C) standards, HTML is currently in its 5th version. HTML5, released in 2014, allows for application programming interface (API) support and allows for cross-platform mobile applications. JavaScript also provides support for web workers that allows scripts to run in threads in the background without affecting webpage performance.

7.2.1.2 Cross Origin Resource Sharing (CORS)

One of the tools in HTML5 and JavaScript that supports interoperability between domains and enables API support is the Cross-Origin Resource Sharing (CORS) feature. CORS allows websites on different domains to share data and enables communication between servers and client browsers for data requests. CORS allows for mechanisms to override the same-origin policy, thus enabling web browser scripts from one page to offer access to data from another page even if they do not have the same origin. (Origin is defined as a combination of URI scheme, port number, and host name.) Same origin policy was also one of the limitations of JavaScript Web workers, however, CORS has offered an ingenious work-around to the problem of same-origin policy. CORS and Web Workers

together allow for cross-domain workers through the creation of intermediate pseudo-JavaScript formats called blobs. A detailed description of web worker operation is found on the Mozilla Developers Network (MDN) documentation website. The capabilities of background operation without interrupting website performance offered by web workers, cross-domain data sharing, and the ability to work with APIs have provided a fertile landscape for distributed cryptomining operations. Users who visit a site, knowingly or unknowingly, perform the proof-of-work operations required for mining cryptocurrencies over the duration that the page is loaded in the browser. Stealthy tactics, such as pop-unders, which open additional browser windows that hide under the Windows taskbar behind the clock are not easily detected. These pop-under windows have the potential to stay open indefinitely, while also using up CPU cycles for mining cryptocurrencies. Some of the pop-under windows persist beyond clicks on the X icon to exit the browser, leaving the only recourse for exit to the Task Manager. More evasive cryptomining botnet code has been developed with advanced anti-detection techniques, where the mining operations are file-less (running as native applications, not injected code), and are able to kill other cryptomining processes found on the system [12].

Other features of modern web technology have aided the rapid spread of cryptomining capabilities. WebAssembly, abbreviated as WASM, is one such standard developed by the W3C group. The modern web platform can be thought of as having two parts: the virtual machine (VM) and the API collection. The VM runs the code of the web application and the API collection offers tools to control webpage functionality. Traditionally, the VM has only been able to load JavaScript code, however, WebAssembly offers a way to run application code from any language on the web browser through a compact binary format. The advantages it offers are numerous: speed of running native apps, improved performance, portability, and interoperability. Although WebAssembly enforces same-origin policies, CORS and web workers in conjunction with WebAssembly have created a versatile platform for cryptomining operations. This platform leverages the power of distributed computing using the browser. A detailed analysis of web workers is provided in [13], where the authors develop cost models for various kinds of web worker attacks, including cloud-based attacks and botnet-attacks. The applications of web workers studied in [13] include browser-based password cracking, and cryptocurrency mining, and DDoS attacks. Web sockets, another feature of modern browser technology, offer full duplex communication between the browser and server on TCP. Web sockets also allow browsers to facilitate secure data exchange without having to poll the servers for responses. Figure 7.1 depicts the significant aspects of contemporary web development frameworks that support cryptomining, and are being utilized for botnet-enabled threats to cryptocurrency mining.

The concurrency afforded by web workers, and the convenience of browser plugins like TamperMonkey install scripts that allow web content to be modified on the fly have created an environment that is conducive to browser-based

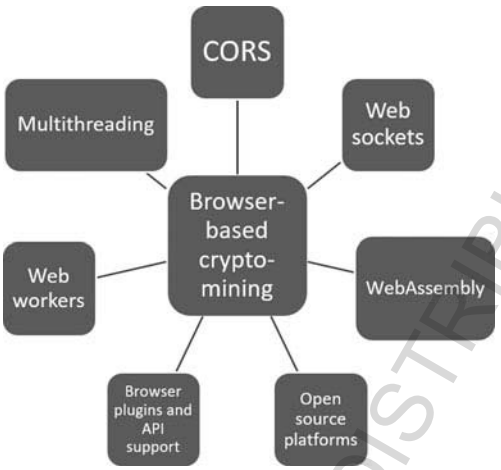

Figure 7.1 Affordances of contemporary web development frameworks that support cryptomining.

distributed mining of the likes of Monero. Created in 2014, Monero is an open-source cryptocurrency that uses an obfuscated public ledger that blocks the source, destination, and amount of the transactions. This untraceability afforded by Monero, as opposed to the transparency offered by Bitcoin, has been one of the key factors in its popularity. As of early 2019, Monero is the ninth largest cryptocurrency based on market capitalization.

7.2.2 Cryptojacking

In cryptojacking, also referred to as drive-by mining, in-browser mining executable files run, usually without the consent of the client machine and the corresponding payoff is delivered to the website. These executables are generally JavaScript files or WebAssembly modules that infect web servers and are enabled by third-party libraries, browser misconfigurations, or advertisements [14]. In doing so, the computational resources of the user machine running the browser are leveraged when the user visits the website, and has the ability to render such client machines into bots for a botnet.

C&C architectures are the backbone of these botnet operations. Aided by the IRC protocol, a C&C server sends commands to malware-infected machines, which are then capable of launching DDoS attacks, data manipulation, and malware propagation. The IRC protocol is a text-based protocol that allows clients in various topology configurations to connect to a server over communication

channels. Botnets can also use the HTTP protocol [15] as a means for C&C communication. In [16], the authors describe two frameworks of C&C communications. The push framework contains bots that wait for commands from the C&C server, i.e., the server pushes the commands to bots in real time. IRC-based bots fall into the push category. The pull framework consists of servers that store commands in a file, and bots check back at later times to retrieve and execute the commands, i.e., the bots pull the commands from a file stored in the C&C server. Most HTTP-based bots fall into this category of botnets that do not adhere to real-time botmaster control.

Coinhive was one of the first platforms to offer browser-based cryptomining. The work in [17] details the cryptojacking activities powered by Coinhive [18], a legitimate framework for browser-based mining that provides developers with APIs and is geared toward optimized performance by browser-based mining. Browser-based cryptomining is in contrast to GPU or ASIC-based mining, which are able to use more computationally intensive resources for completing the proof-of-work component of mining cryptocurrencies. The cryptomining operation in Coinhive enables the creation of unique IDs called "site keys" in Coinhive. These site keys map to miners and are therefore used to link rewards for the mining operation. Multiple site keys can map to the same wallet [19]; thus botmasters are able to leverage the computational power of multiple browser sessions across distributed IP addresses to mine for rewards.

Cryptojacking raises several issues related to the abuse of user consent, compromise of user machines by transforming them into bots, and profit models of complicit websites hosting the JavaScript executables that run mining scripts. Additional issues include breach of the existing browser, network, and cloud configurations, as well as the ubiquitous problem of botnet-powered payload and loot. To mitigate the problem of user consent for in-browser mining, Coinhive launched AuthedMine, which asks for user consent prior to using the computational hashing power of the user's machine. Coinhive receives 30% of all Monero currency that is mined, with the other 70% sent to the cryptocurrency wallet that is associated with the mining account. These payments are made even if the mining is carried out without the user's consent. Thus, even though Coinhive is a legitimate distributed mining utility providing a valid source of revenue in lieu of ads on webpages, it often surfaces on hacked websites. A do-not-mind HTTP header has also been proposed but has not been widely adopted due to lack of mandatory rules on enforcement.

Coinhive targeted Monero, a cryptocurrency that enjoys popularity on dark-web markets and is typically used to trade with alternative cryptocurrencies (e.g., exchanging Monero with Bitcoin). The payoff of cryptojacking with Coinhive is divided between the developer and the website. Monero uses the CryptoNight and the CryptoNote algorithms [20]. CryptoNight was developed to be compatible with the computational resources of CPUs, as opposed to the computationally

intensive, mining-friendly ASICs. CryptoNote, used in Monero and ByteCoin, offers the added advantage of anonymity due to ring signatures, an algorithm that prevents accurate pinpointing of the details of a transaction, while only allowing transactions to be traced to a group.

Although browser-based cryptomining is less computationally intensive than GPU or ASIC-based mining, it still has the potential to consume higher than usual amount of resources. This tendency to use more resources also lends itself to detection of cryptomining activity. Due to the increased usage of computational resources by drive-by mining software, it is possible to build a profile of resource consumption that can lend itself to predictive modeling for future attacks. However, Coinhive and similar other miners have now evolved to a point where they are able to restrict CPU usage, so as to avoid triggering alarms about possible mining activities based solely on pattern matching algorithms.

A summary of the operational details of bitcoin-mining bots is presented in [21]. Three categories of mining activity are summarized: direct mining, proxied mining, and dark-pool mining. In direct mining, a botmaster distributes the mining executable inside a wrapper script that contains the specified parameters to be mined. This executable is made available as trojans inside external applications, which are deployed with the botmasters credentials. Thus, a large number of bots in the botnet are mining and delivering the cryptocurrencies directly to the botmasters account. Proxied mining, on the other hand, uses a proxy server deployed by the botmaster. The proxy serves to hide the addresses of all the bots and appears as a single powerful miner. It also requires the additional costs of installing and maintaining the proxy server. In dark pool mining, the botmaster maintains a mining pool that participates in the mining of bitcoins on the Bitcoin peer-peer network.

Further analysis of the operational costs and revenues of botnet-powered mining activities is presented in [21]. The life cycle of a botnet, with an emphasis on the economic impact of botnets, is presented in [22]. Profit analysis of cryptomining is also presented in [14]. Cryptomining by IoT devices has been studied in [23] and [24]. In [23], the authors posit that botnets of thousands of smaller IoT processors could be instrumental in mining altcoins, where the hashing power required to mine a block is not computationally expensive. Thus, IoT devices could be used not just to mine alternative cryptocurrencies, but also for creating platforms for launching DDoS attacks, distributing spam, and stealing credentials. The work in [25] details the use of IoT devices in enabling and propagating a DDoS attack using the Mirai malware. Studies on the profitability of cryptojacking versus ad impressions from a publisher's perspective have been performed in [26], where the authors determined statistics on the criteria for profitable cryptojacking, the impact of in-browser mining on the energy consumption and computational resource consumption, as well as revenue generation for the publisher.

A recent study has shown how remote frameworks with C&C architectures can be used in cryptomining. In [27], the authors present MarioNet, a framework with a remote C&C environment for browsers and using them to engage in activities such as cryptomining, DDoS, and password mining. MarioNet is configured to withstand tab crashes and browser shutdowns, while being robust across different browser platforms. The authors present three properties for robust operation: isolation (independent from the browsing session thread for optimal performance), persistence (ability to control browser for longer than a short browser session), and evasiveness (ability to execute cryptomining in stealth).

In addition to cryptomining using browsers and IoT devices, cryptomining software has been found in the form of apps distributed through the Google Play store for mining litecoin, dogecoin, and casino coin. Work in [28] presents a detailed analysis of building botnets using free cloud-based services by abusing the development-environment-as-a-service paradigm. A first step toward using these services to create bots is by generating scripts to enable automatic registration. The resulting botnet can be shown to enable DDoS attacks, distributed password attacks, and network scans, as well as cryptocurrency mining. Referring fake friends lets the botnet amass unlimited storage space. The next section presents specific attacks posed by cryptocurrency-mining botnets.

7.2.3 Cryptocurrency Theft, Clipboard Hijacking, and Other Attacks

In addition to cryptojacking, other botnet-based cryptocurrency attacks have been noticed. In 2014, the Pony botnet software [29] was linked to the theft of more than $200,000 in cryptocurrency wallets of about 30 different currencies such as bitcoin, dogecoin, and litecoin. The Pony software was activated by clicks on suspicious links or spam software that was hidden inside executable files. Once activated, it avoided detection by antivirus software and was able to access the wallet.dat files on users' computers. Another attack related to cryptocurrency theft is clipboard hijacking [30]. Clipboard hijacking exploits the fact the long cryptocurrency wallet addresses made up of alphanumeric characters are difficult to remember. Users copy and paste this information on a clipboard. The ComboJack malware [31], which gets installed by clicking on an infected attachment, scans the clipboard every half second and scans it for wallet addresses. Once a wallet address is detected, ComboJack replaces it with a hard-coded wallet address belonging to the attacker. The unsuspecting user, in the meanwhile, returns to the clipboard and pastes the address inserted in the clipboard by ComboJack. A Kaspersky Lab report showed that attackers stole roughly $10M worth of Ethereum using social engineering tricks such as fake websites and phishing emails.

Attacks on cryptocurrencies have also exploited vulnerabilities in the underlying structure of the Internet. An analysis of bitcoin attacks using the routing architecture of the Internet was presented in [32]. These routing attacks involved the BGP routing protocol, which is used to store and broadcast route information between neighbor networks. Since BGP does not check for the validity of broadcasted route announcements, it was exploited to inject fraudulent route information from an autonomous system (AS) to intercept and send traffic to the wrong destination. This kind of attack is called "BGP hijacking," and was shown to enable node and network-wide attacks by isolating portions of the network (partitioning attack). BGP hijacking was also able to slow traffic and thereby propagation of blocks in the bitcoin protocol toward other nodes (delay attack). BGP hijacks are prevalent in network traffic resulting in thousands of attacks every month, and specifically causing up to hundreds of events every month. However, since cryptocurrencies use a consensus mechanism to approve transactions and encode blocks, attacks such as the BGP attack have a particularly strong impact on cryptocurrency mining.

7.3 Prominent Cryptomining Botnets

This section presents a list of several botnets that were chosen for their technical complexity, diversity, and impact. Additionally, botnets targeting websites, mobile devices, and IoTs are also profiled.

7.3.1 ZeroAccess Botnet

The ZeroAccess botnet that first appeared in 2011 is the largest known botnet that uses P2P mechanisms for communication. Although initially used to download a payload for bitcoin mining, the newer version uses ZeroAccess for click fraud. The distributed P2P C&C architecture creates redundancy; however, it also ensures that there is no central C&C mechanism that can be taken down to shut down botnet operations. Although many variants of ZeroAccess exist, the most prevalent version is the Type II version that uses UDP to load malware payload modules on the user's computer. The malware is able to distinguish between 32-bit and 64-bit computers, and earlier versions were able to download both the bitcoin mining module and the click fraud module. The bitcoin mining module has been phased out in favor of the greater revenue generated by the click fraud module that generates artificial clicks for advertisements and makes these clicks appear as if they are legitimate clicks. The bitcoin mining module of ZeroAccess, titled Network #1, has a file that links to a Upfinex (UPX) decentralized exchange and wallet platform, while also generating signatures for authenticity. In test computers, it was observed that the

profitability increased exponentially when the bitcoin mining operation was conducted on a network of infected computers instead of on a single computer. The test operation revealed that, at the Bitcoin USD rate of 131, the potential benefits of bitcoin mining using ZeroAccess were less than 50 cents a day for one computer, versus thousands of dollars a day for a botnet. In contrast, the click fraud operation of ZeroAccess was more profitable, resulting in potentially tens of millions of dollars a year.

7.3.2 Smominru Botnet

In early 2017, a group of hackers called the "Shadow Brokers" released a gigabyte worth of software exploits developed by the NSA. One of those exploits was Eternal Blue, which targeted vulnerabilities in the Windows servers, specifically the Server Message Block (SMB) protocol, a network file sharing protocol. With a worm-like ability, infected machines were capable of exploiting the vulnerabilities in other connected Windows machines, leading to rapid infection. The Smominru botnet, powered by the Eternal Blue exploit, turned infected machines mostly Windows servers into cryptominers [33]. At its peak, the Smominru botnet had infected 526,000 machines and had generated roughly $2.3 million in cryptomining revenue. The Eternal-Blue exploit was also leveraged in WannaMine, launched by clicking on a fraudulent link [34]. WannaMine used a credential harvester called "Mimikatz," which if unsuccessful resulted in the use of EternalBlue. Although it uses EternalBlue, WannaMine connects to a different mining pool with different servers and is file-less, making detection by antivirus harder. Similar rapidly spreading botnets include Dofoil [35], a cryptomining application for mining Electroneum, where the botnet spread to half a million computers in less than 24 hours. Dofoil used a combination of spawned processes, thereby tricking the process manager into believing that the original process was running (process hollowing). This resulted in modification of the Windows registry and connection to a remote C&C architecture. Dofoil was then able to infect a large number of computers while being able to resist detection.

7.3.3 Adylkuzz

Another widely spread malware using Eternal Blue is the DoublePulsar malware that provides a covert channel through which kernel code can be executed for a variety of applications. The Adylkuzz mining botnet uses both EternalBlue and DoublePulsar by determining the public IP address, cryptomining instructions for Monero, and clean up tools. Infection by Adylkuzz had an interesting side effect: Adylkuzz worked as a backdoor and closed the doors behind it to prevent further

exploitation of the SMB vulnerability. Thus, machines infected with Adylkuzz were protected from Wannacry, a bitcoin ransomware cryptoworm that also leveraged the Eternal Blue vulnerability. Unlike Wannacry that was linked to three hardcoded bitcoin wallets, Adylkuzz created numerous wallets over time that resulted in small amounts of revenue [36].

7.3.4 Botnets Targeting Mobile Apps

Although mobile devices do not traditionally possess the computational resources required for cryptomining and thereby result in insignificant revenues, cryptomining software has made its way to mobile apps [37]. Examples include Google Play apps such as Recitiamo Santo Rosario Free (designed to help users pray the rosary), SafetyNet Wireless App (designed to produce discounts) and in repackaged versions of popular apps such as Football Manager Handheld (an app for European soccer club player management) and TuneIn Radio (an app for free Internet radio), Songs and Prized. The mode of operation is to use software such as Androidos CPU Miner (Songs, Prized, Football Manger Handheld, Tune In Radio) and Androidos JS Miner (Recitiamo Santo Rosario Free, SafetyNet Wireless). In the JS Miner software, the apps load the JavaScript library from Coinhive, whereas with the CPU Miner software, the apps are repackaged versions of legitimate apps that are infected with CPU mining code. Another significant cryptomining operation that had not been distributed via Google Play but discovered by Kaspersky Labs researchers is Loapi [38], which downloads a Monero cryptocurrency miner that overheats the phone components and destroys the phone. Dubbed as a jack-of-all-trades for its ability to perform cryptomining, launching DDoS attacks, inject ads, and ability to hide under the logos of antivirus solutions and porn sites, Loapi is capable of boosting ratings for ads, directing SMS messages, and subscribing users to paid services. Other seemingly innocuous apps discovered on Google Play include wallpaper apps that contained BadLepricon, a bitcoin mining malware, which was used to mine dogecoin and litecoin, with careful consideration on throttling resource usage [39]. These apps used a Stratum proxy to control which nodes were used for mining, where the coins were delivered, and was designed to run when the display was turned off and the battery level was above 50%.

7.3.5 Botnets Targeting Websites

Cryptomining software has been found on a variety of sites including WordPress [40], CBSs Showtime [41], live chat and help widget [42], government websites [43], and BitTorrent distribution sites [44]. Mining software was discovered in the public WiFi offered by Starbucks at a Buenos Aires location, where users were

given a ten-second delay on connection, during which time the computers were mining Monero [45]. Monero mining software has also been found on the desktop version of Facebook Messenger [46]. Potential mining activity has been found in gaming software distributed through Steam, an online gaming distribution portal [47], and in gaming software updates [48]. Vulnerabilities in the Drupal Content Management System (CMS) that powers millions of websites were exploited for mining Monero in what came to be known as Drupalgeddon 2, where public servers were forced to download and mine cryptocurrencies [49]. Botnets have also been found disguised behind reverse proxy networks, where users were able to connect to servers behind firewalls, or those without public IP addresses [50]. However, not all mining software is distributed through covert channels. XMRig, a high-performance miner advertised with official Windows support is freely available for both the ASIC and GPU operations. XMRig is designed to mine Monero and avoids detection by shutting down as soon as Task Manager is opened. Modified versions of XMRig are available, including WaterMiner, which was discovered in a repackaged version of Grand Theft Auto mods, a popular video game utility. WaterMiner was designed to cease mining during computer scans and debug operations, resulting in high usage of gamers processing powers for cryptomining activities [51].

7.3.6 Botnets Targeting IoTs

Botnets have also made their way to IoT devices. The Mirai botnet [52] targeted insecure IoT devices, while avoiding device addresses linking to GE, HP, or the US DoD. It scanned the Internet for big blocks of open Telnet ports and used default user ID/password combinations to gain control of closed-circuit TVs, DVRs, and routers in one of the biggest IoT-powered attacks. Although initially Mirai was used to launch DDoS attacks, recent variants of Mirai include bitcoin mining modules [53]. A range of solutions for botnets targeting IoTs has been studied. In [54], the authors present strategies focused on intrusion detection systems (IDSs). Given the geographically distributed natures of IoT devices, the authors study placement of IDSs in three architectures: distributed, centralized or hybrid. In the distributed architecture, IDSs are placed in every physical object, compared to the centralized architecture, where an IDS is placed in a centralized location such as the border router or a dedicated host. Several hybrid approaches have been surveyed, such as the use of clusters and building a backbone of monitor nodes. The IDS operation for detecting botnets has been surveyed in four categories: signature-based detection, anomaly-based, specification-based, and hybrid. The authors also study the security threats faced by IoTs, in particular, routing attacks, Dos attacks, and man-in-the-middle attacks. Anomaly-based botnet detection techniques have also been studied in [55]. Here, the

authors proposed unsupervised learning models with reduced feature-set sizes with the aim of decreasing computational resources. Neural-network-based approaches have also been studied in [56], where the authors propose a dense random neural network architecture for detection of DoS attacks as well as denial-of-sleep attacks. Empirical results from packet-capture software have shown that the proposed neural network architecture is effective in detecting ongoing attacks against IoT gateways. Work in [57] describes the use of autoencoders as fully automated standalone encoders in detecting botnet malware. The authors propose the use of an autoencoder for each IoT device, where the autoencoder is trained on the benign traffic data at the device. An autoencoder is a neural network that can reconstruct its input after compression. Failure to reconstruct the input is considered a failure, and therefore, is an anomaly in this model. Anomaly models are built for each device separately. Empirical data evaluated from using autoencoders against the Mirai and Bashlite botnet malware in this work has shown promising experimental results, including high probability of attack detection, lower false alarm rate, and low detection time.

Although the bulk of this chapter focuses on botnets targeting cryptocurrencies, these attacks may be carried over into other domains, such as health and medicine, finance, and education. A recent study offers a look at two crucial sectors in infrastructure that might be easily targeted through open-source intelligence: water and the energy sectors [58]. In this detailed report, the authors name several attacks aimed at modifying the amount of chemicals added to water treatment plants, dam control, power grids, and other water and energy industries, which were carried out by cybercriminals.

7.4 Countermeasures for Cryptomining Botnets

This section will focus on countermeasures for cryptocurrency mining botnets. Proactive and reactive countermeasures for botnet operation will be examined. These countermeasures will be examined categorically along the lines of proof-of-concept approaches, experimental approaches, and viable protocols that have already been deployed as countermeasures. The countermeasures described in these sections fall into four categories: profiling, secure web development frameworks, software engineering, and social frameworks, as shown in Figure 7.2.

7.4.1 Profiling

This category of countermeasures falls along the lines of signature-based detection. Cryptomining software exhibits certain characteristics that impact the client machine's hardware. Together, the software and hardware impacts are used to develop software profiling and hardware profiling countermeasures.

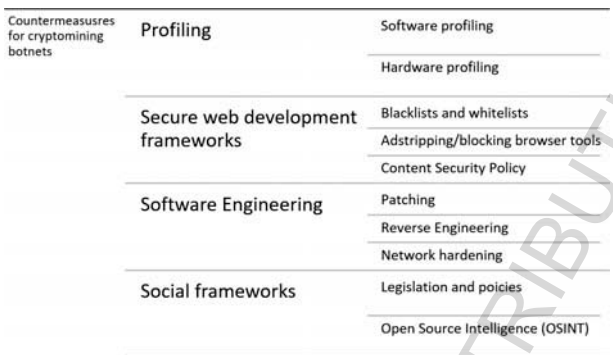

Figure 7.2 Categories of countermeasures for botnet-enabled cryptomining.

7.4.1.1 Software Profiling

Unusually high CPU usage and the presence of traditional mining software (WebAssembly, WebWorkers) have been shown to be effective in the detection of cryptomining software on websites. In [59], the authors propose a semantic inline script monitor called "SEISMIC (SEcure In-lined Script Monitors for Interrupting Cryptojacks)" that detects incoming WASM binary programs, changes their profile during execution and warns the user about cryptomining software in the website. The user is then given the option to opt out (halt the script) or opt in (continue mining). The use of free cloud services to create botnets can be mitigated by enabling multiple authentication mechanisms such as the use of an email address, CAPTCHAs including puzzles, phone/SMS, and credit card details. Other proposed countermeasures include analyzing Sybil accounts, creation rate of new accounts, and flagging of accounts with new domain names.

Software profiling by analyzing code is another countermeasure for detecting botnet activity intended for targeting cryptocurrencies. In [14], the authors propose MineSweeper, a range of techniques that target cryptomining activity that has been obfuscated in varying levels of severity. MineSweeper employs algorithms that look for core cryptographic operations (shift, XOR, rotate), bytecode of specific hashing algorithm primitives, and CPU cache usage.

7.4.1.2 Hardware Profiling

Hardware profiling, by evaluating microarchitectural execution patterns, has been proposed in [60] as a countermeasure for detecting cryptomining. Based on the premise that mining and non-mining application produce differing CPU/GPU signatures, the authors propose MineGuard for detecting mining activity on cloud/

enterprise platforms. In [61], the authors use a network theory approach for bot detection on the Ethereum network. Based on the premise that the duration between transactions on a network follows the power law distribution (as observed in networks with human agents), any nonhuman activity, for example, bot activity should be detectable based on the deviation from the power law distribution.

7.4.2 Secure Web Development Frameworks

Existing flaws and loopholes in web development frameworks have led to exploitation by malware. This category of countermeasures proposes the use of whitelists/blacklists, adstripping and blocking in existing browsers, and development of new browsers and profitability models. The use of headers such as the Content Security Policy (CSP) header is another proposed mechanism that blocks cross-site scripting attacks.

7.4.2.1 Blacklists and Whitelists

In March 2018, the US Department of Treasury's Office of Foreign Asset Control (OFAC) published new guidelines about virtual currency compliance obligations. The OFAC has maintained a list of Specially Designated Nationals and Blocked Persons List (SDN). This list contains a list of individuals and organizations that participate in illegal activities, and with whom US persons are prohibited from conducting transactions. The OFAC announcement from March 2018 now allows the addition of individuals and entities associated with digital currency identifiers to the SDN list. Individual users can use browser extensions such as No Coin, which works with Chrome, Firefox, and Opera browsers to block Coinhive and similar cyrptojacking software in websites. It also gives users options to whitelist a particular miner and allow it to run.

MinerBlock is another Chrome extension that uses a two-pronged approach to blocking mining scripts. It works by using the traditional approach of blocking mining software associated with blacklists and is also capable of detecting potential mining behavior inside loaded scripts and killing them immediately. CoinBlockerLists maintains a frequently updated list of websites associated with cryptomining, and offers this list in various formats for integration with existing website anti-mining solutions.

7.4.2.2 Adstripping Browsers and Blocking Mechanisms

Ads have emerged as a popular way to distribute cryptomining software and have been found in Googles DoubleClick ads and YouTube ads. The introduction of cryptojacking software, first popularized by Coinhive has made it possible for

publishers and advertisers to make for the shortfall in advertising revenue by using ads for cryptomining. Some websites (Salon, Pirate Bay) are taking a different approach to the ads versus cryptomining debate by presenting users with an option: Would you like to watch our ads or would you rather spare CPU cycles for cryptomining? Different solutions have been proposed for this challenge. Adstripping extensions on browsers such as Silent Site Sound Blocker and uBlock Origin are two of the many freely available tools that target different aspects of the web browsing experience in addition to blocking ads. For example, Silent Site Sound Blocker for the Chrome browser blocks ads that run in webpage corners when the site is loaded. Magic Actions is another ad stripping extension that works on Chrome, Firefox, and Opera browsers that suppresses ads on YouTube, disables the comments, and presents clear selections for controlling the volume and resolution.

A novel approach to the challenge of advertising revenue, user preferences, and privacy has been offered in the form of a Basic Attention Token (BAT). Developed by the team that developed JavaScript and Firefox, the BAT is an Ethereum-based digital token that eliminates the middlemen in the digital advertising spaces. Users are rewarded for their attention in the form of BAT and publishers receive a majority of the ad revenue that was previously lost to bots and middlemen, and advertisers are able to obtain superior data analytics. The BAT currently works with the Brave browser, and open-source web browser that blocks ads and trackers, while also enforcing the HTTPS protocol. The Brave browser monitors user's activities, and the data is stored on a distributed ledger. Advertisers send ads in the form of smart contracts to the browser, which are unlocked when a user views the ads who then gets rewarded in BATs. BAT can be spent in the browser for premium articles, donations, and other in-browser transactions.

7.4.2.3 Content Security Policy

CSP, first proposed in [62], was developed as a solution to mitigate the impact of attacks against Web Application Vulnerabilities using Cross Site Scripting (XSS) and Cross Site Request Forgery attacks (CSRF). XSS and CSRF attacks work in bidirectional modes of trust exploitation—CSRF attack is a confused deputy attack that exploits the trust that a site has in a user's browser, while XSS attacks exploit the trust that a user has for a site. XSS attacks typically involve the injection of malicious code into web applications. Examples of CSRF attacks including changing user information, adding items to the cart, unauthorized money transfers, and other such user activities that could be performed on reproducible links [63]. The use of CSP headers allows website owners to declare approved origins of files using specific directives to block content, and with verification that the content delivered has not been manipulated (request-sri-for). Using a whitelist approach, the sri and other similar

directives in CSP (default-src, connect-src, etc.) can be used to detect and block cryptojacking operations.

7.4.3 Software Engineering

This category of countermeasures presents a holistic view of threat modeling and management. Tools such as patching, reverse engineering of attacks, and network hardening are described in this section to offer proactive mechanisms to assess existing vulnerabilities, model threats, and mitigate their impact.

7.4.3.1 Patching

Security patching has been an integral part of the software lifecycle management and computer security protocols to protect systems and users from system vulnerabilities and exploits. The EternalBlue exploit, developed at the NSA and leaked by the Shadow Brokers, was patched by Microsoft in the MS17-010 patch. This patch resolves the vulnerability in the SMB protocol that allowed remote code execution. As hackers divert more of their resources toward cryptomining and DDoS attacks, it has been shown that patching still remains an effective tool to counter cryptomining attacks [64].

7.4.3.2 Reverse Engineering

Studies have been conducted in the creation of botnet-like networks that could attack cryptocurrencies. In [65], the authors provide a framework for ZombieCoin, which uses the distributed, verifiable, cryptographic transformations offered by Bitcoin to create a mechanism that enables the C&C architectures instrumental to botnets. The botmaster generates a public–private key pair and an instruction set that can be decoded by individual bots. The infection mechanism may be trivial (such as advertisements containing links), which can be activated by clicks and then can be used to infect the machines of unsuspecting users. These machines are then transformed into bots, which can be used to deliver information (such as financial data, passwords) or propagate spam, phishing, and DoS attacks.

A range of possible solutions for ZombieCoin has been proposed. These include rapid response from ISPs to block sites that host rendezvous points for botmasters and collaboration with law enforcement to detect and mitigate the impact of such blockchain polluters [66]. Other approaches described include the employment of honeypots deployed by whitehat hackers. These honeypots function as Sybils and disrupt the economic relationship between bots and the botmaster. For example, these machines may join the botnet and create multiple clicks for ad impressions without generating revenue for the botmaster.

7.4.3.3 Network Hardening

The eclipse attacks presented in [11] described a method to isolate victim nodes, wherein attackers monopolize all the incoming and outgoing connections of a node, thereby disrupting the assumption of perfect information. Several countermeasures were proposed to harden the network against such attacks propagated by botnets, with an emphasis on limiting and testing new incoming connections, tracking of known and new connections, random eviction of connections from the tables that store known and new connections, banning unsolicited addresses, and increasing the size of the tried and new tables. Some of these countermeasures have now been incorporated into the Bitcoin infrastructure through a software upgrade.

Counterattacks to the BGP attacks described in [32] are based on increasing the diversity of connections. Since mining pools use multiple gateways hosted (homed) by different ISPs, the degree of multihoming provides a measure of additional security against BGP attacks. The authors show that using encrypted traffic, incorporating the use of VPNs, and deliberate refresh of network connections (network churn) are some of the countermeasures to BGP hijacks. Additionally, network monitoring statistics such as the round-trip time, sudden changes in node connections, and the use of distinct channels for control and data have been suggested as effective tactics for countering BGP hijacks to the bitcoin network.

While most of the attacks against the Bitcoin ecosystem focuses on external threat actors such as botmasters launching cryptomining [67], studies attacks on the Bitcoin ecosystem by framing it as a problem of one or more mining pools that are set to achieve maximum utility by potentially undermining the utilities of other mining pools. The authors in [67] used a game-theoretic approach to study the strategic choices of mining pools in launching attacks against other pools. In the case of MarioNet [27], several strategies have been proposed for countermeasures, including the use of blacklists and whitelists, user permission criteria, and restrictions on WebWorkers by disabling their services and limiting their active time in proportion to browser session duration.

7.4.4 Social Frameworks

The countermeasures described thus far fall along the spectrum of technical measures for proactive and reactive botnet-based threats. Recent studies have shown that social frameworks are valuable sources of information about threat sources. This kind of information, called "open source intelligence (OSINT)" is found on popular websites, message boards, forums, and social media. OSINT can be mined for a trove of information about cryptocurrency activity and threats. Additionally, the role of policies and legislation is crucial in determining the scope of legal activities concerning cryptocurrencies.

7.4.4.1 Open Source Intelligence

In addition to the technical countermeasures to cryptocurrency mining discussed in this section, a computational social scientific approach for coin success presented in [68] could be used for attack prediction. Here, the authors analyzed discussions in online forums to infer the role of discussion and the resulting hype around certain kinds of cryptocurrencies as a viable predictor of the potential success of certain kinds of coins. Similar tactics combining social network data, discussion forum conversations, and other network science approaches to infer attack modes and operational mechanisms of botnets employed in cryptomining. An analysis of the frequency of mentions of cryptocurrencies and its correlation with the price of bitcoin was performed in [69]. Other similar detection tools based on bot activity on the C&C channels were used to build tools such as BotSniffer [16], where the authors studied the crowd-like behaviors of bots in a botnet responding to commands or generating messages for botnet detection. Another such bot detection tool was developed in [70], where they develop BotDet that detects bot activity based on malicious IP addresses, SSL connections, domain detections, and Tor connections. A summary of current bot detection software is also presented in [70].

A similar detection technique was used in [19], where the authors conducted additional statistical analysis on the characteristics of websites that employ cryptomining. The authors studied popularity of the website, location of the websites host, and website content as indicators of the probability that the website was containing cryptomining software. They found that there was no strong correlation between popularity (as measured by the websites rank on Alexa), location, or content.

7.4.4.2 Legislation and Policies

In 2016, the European Union (EU) Parliament announced a new legislative framework for protection of user data called "GDPR (General Data Protection Regulation)." It provided a two-year transition period for websites to adapt to the GDPR regulation and officially came into force in March 2018. The EU GDPR affects not just organizations within the EU, but all organizations that offer goods and services, or monitor the activity of EU citizens. Under the terms of the EU GDPR, the emphasis has been placed on receiving user consent for collecting and processing data in clear terms, and user rights have been expanded to include, among others, notification of breaches, access to data, privacy, and the right to be forgotten. Violators of the GDPR terms are penalized according to a tiered framework, where the maximum penalties imposed are 4% of annual turnover or 20 million euros.

Varying opinions about the impact of GDPR on blockchain have arisen. In a recent whitepaper [71], IBM highlighted how blockchain can be utilized to

assist in the five major GDPR areas: Rights of EU Data Subjects, Security of Processing, Lawfulness and Consent, Accountability of Compliance, and Data Protection by Design and by Default. However, others point to the potential for GDPR to disrupt the fundamental tenets of blockchain. Blockchain, and by association, cryptocurrency mining, in general, is based on the general concepts of transparency and immutability. Researchers have pointed out several arguments that threaten the operational mechanisms of blockchain: are encryption keys considered as personal data? [72]. Also, resolving questions about accountability in the event of breaches is a complex process [73]. GDPR might thus serve to mitigate the impact of cryptojacking operations by limiting the stealthy modes in which the computational resources of unsuspecting users of websites, apps, and IoT devices are leveraged for cryptojacking.

In [74], the authors present a detailed treatment of cryptocurrency legislation in various countries around the world. The work in [75] presents ideas for creating regulatory instruments that do not stifle the potential for innovation achievable with cryptocurrencies and are able to prevent the use of cryptocurrencies as vehicles for criminal activities. The financial technology sector is uniquely positioned to offer solutions and platforms for cryptocurrency. Initial coin offerings (ICOs) for various kinds of cryptocurrencies have surpassed the $20 billion mark and have emerged as a significant source of fundraising in cryptocurrencies. An interesting primer concerning the role of ICOs in fintech, IT, and enterprises and domestic and foreign regulations for ICOs is presented in [76].

7.5 Future Directions

As we ponder the road ahead for cryptocurrencies, we will see that cryptocurrencies are beginning to gain wider acceptance across various domains in government, banking, electronic commerce, and other sectors. It remains to see how the increased exposure will attract diverse challenges. This chapter explored threats to cryptocurrency mining offered by botnets, the challenge of in-browser mining as both utility and nuisance and countermeasures to these challenges. Other such challenges lie along the spectrum of user expertise in cryptocurrency trade. At one end of this spectrum lies the botnet black market that has created avenues for unpoliced creation, usage, and evolution of botnets. At the other end of the spectrum lies the lay user who is using cryptocurrency for trading but is unaware of the numerous ways that his or her devices are being used to aid in the operation of botnets.

The distributed nature of cryptomining raises several questions that are intertwined in the legal, fintech, and social spheres. While many countries around the world have warmed up to the idea of cryptocurrencies, some countries deem

cryptocurrencies illegal. These countries include China, Bolivia, Columbia, Ecuador, Russia, Vietnam, and Russia, among others. In the countries where cryptocurrencies are legal, differing laws exist on the mining and use of cryptocurrencies for trading of goods and services. The need for more energy-efficient mining operations will also be a significant factor in the development of mining regulations and the development of newer protocols such as proof-of-stake (PoS), as opposed to the PoW algorithms that are energy-intensive. Regulations surrounding cryptocurrencies will have to account for the diversity of coins, an issue that does not affect fiat currencies since, for the most part, currencies in countries are homogeneous. Regulations will also have to consider the anonymity championed by cryptocurrencies, which serve to empower mining and trading entities yet create massive incentives for engaging in criminal activities such as those found on the dark web.

Finally, the perception of cryptocurrencies plays a role in its adoption. The bitcoin PoW requires user buy-in, and while recent literature has studied challenges to adoption and growth of cryptocurrencies, scant research exists on the public perception of its viability as an alternative to cryptocurrencies. The initial findings of the Cryptoasset Sentiment Survey [77] show that the public is aware of cryptocurrencies, but the operational details are elusive. Other research on perceptions of cryptocurrency have been documented in [78] and [79]. The threats posed by malware such as botnets only serves to fuel the confusion surrounding cryptocurrencies and could turn into a major impediment to widespread adoption.

References

[1] S. Silva, R. Silva, R. Pinto, and R. M. Salles. Botnets: A survey. *Computer Networks*, 2:378–403, 2013.

[2] M. Anagnostopoulos, G. Kambourakis, and S. Gritzalis. New facets of mobile botnet: Architecture and evaluation. *International Journal of Information Security*, 15 (5):455–473, 2016.

[3] Bitcoin Energy Consumption Index. Available at https://digiconomist.net/bitcoin-energy-consumption.

[4] L. Ablon, M. C. Libicki, and A. A. Golay. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*. Rand Corporation, 2014.

[5] A. Minnaar. 'Crackers', cyberattacks and cybersecurity vulnerabilities: The difficulties in combatting the 'new' cybercriminals. *Acta Criminologica: Southern African Journal of Criminology*, 2014(Special Edition 2):127–144, 2014.

[6] R. Richardson, and N.M. North. Ransomware: Evolution, mitigation and prevention. *International Management Review*, 13(1), 10–21, 2017.

[7] Symantec. Internet Security Threat Report. Vol. 24 Retrieved from www.symantec.com/security–center/threat-report, 2019

[8] F. Sinitsyn. Kaspersky security bulletin– Story of the year 2017. Ransomwares new menace. Retrieved from https://securelist.com/ksb–story–of–the–year–2017/83290/.

[9] J. Redman. Bitcoin Personalities: Artforz and the GPU Arms Race. Retrieved from https://news.bitcoin.com/bitcoin-personalities-artforz-gpu-arms-race/.

[10] J. Bonneau. Hostile blockchain takeovers (short paper). In *Proceedings of the International Conference on Financial Cryptography and Data Security*, pages 92–100, 2018.

[11] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg. Eclipse attacks on bitcoin's peer-to-peer network. In *Proceedings of the USENIX Security Symposium*, pages 129–144, 2015.

[12] R. Vigliarolo. GhostMiner fileless cryptomining malware has code that kills itself and other strains. Retrieved from www.techrepublic.com/article/ghostminer-fileless-cryptomining-malware-has-code-that-kills-itself-and-other-strains/

[13] Y. Pan, J. White, and Y. Sun. Assessing the threat of web worker distributed attacks. In *Proceedings of the IEEE Conference on Communications and Network Security (CNS)*, pages 306–314, 2016.

[14] R. K. Konoth, E. Vineti, V. Moonsamy, M. Lindorfer, C. Kruegel, H. Bos, and G. Vigna. Minesweeper: An in-depth look into drive-by cryptocurrency mining and its defense. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 1714–1730. ACM, 2018.

[15] R. Perdisci, W. Lee, and N. Feamster. Behavioral clustering of http-based malware and signature generation using malicious network traces. In *Proceedings of the USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 10:14, 2010.

[16] G. Gu, J. Zhang, and W. Lee. Botsniffer: Detecting botnet command and control channels in network traffic. In *Proceedings of the 16th Annual Network & Distributed System Security Symposium Proceedings*, 2008.

[17] S. Eskandari, A. Leoutsarakos, T. Mursch, and J. Clark. A first look at browser-based cryptojacking. *arXiv preprint arXiv:1803.02887*, 2018.

[18] Coinhive. A cryptominer for your website. https://coinhive.com/

[19] M. Musch, C. Wressnegger, M. Johns, and K. Rieck. Web-based cryptojacking in the wild. *arXiv preprint arXiv:1808.09474*, 2018.

[20] Z. Yu, M.H. Au, J. Yu, R. Yang, Q. Xu, and W.F. Lau. New empirical traceability analysis of CryptoNote–Style blockchains. In *Financial Cryptography and Data Security (FC)*, 2019.

[21] 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 *Proceedings of the Network & Distributed System Security Symposium Proceedings*, 2014.

[22] C.G.J. Putman, Abhishta, and L. Nieuwenhuis. Business model of a botnet. In *Proceedings of the 26th IEEE Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP), 2018*, pages 441–445, 2018.

[23] J.-W. Nijhuis. Effect of IoT botnets on cryptocurrency, 27th University of Twente Student Conference on IT July, pages 1–6, 2017.

[24] J. M. Pedersen and E. Kidmose. Security in internet of things: Trends and challenges. In *Bir Proceedings of the 2018 Short Papers, workshops and Doctoral Consortium Co-located With 17th International Conference on Perspectives in Business Informatics* Research *(bir 2018)*, 2018.

[25] K. Fong, K. Hepler, R. Raghavan, and P. Rowland. Riot: Quantifying consumer costs of insecure internet of things devices University of California Berkeley White Paper. Retrieved from www.ischool.berkeley.edu/projects/2018/riot-quantifying-consumer-harms 2018.

[26] P. Papadopoulos, P. Ilia, and E. P. Markatos. Truth in web mining: Measuring the profitability and cost of cryptominers as a web monetization model. *arXiv preprint arXiv:1806.01994*, 2018.

[27] P. Papadopoulos, P. Ilia, M. Polychronakis, E. P. Markatos, S. Ioannidis, and G. Vasiliadis. Master of web puppets: Abusing web browsers for persistent and stealthy computation. *arXiv preprint arXiv:1810.00464*, 2018.

[28] R. Ragan and O. Salazar. Cloudbots: Harvesting crypto coins like a botnet farmer. *BlackHat USA*, 2014.

[29] Pony. Retrieved from www.cyber.nj.gov/threat-profiles/trojan-variants/pony.

[30] J. Biggs. New malware highjacks your Windows clipboard to change crypto addresses. Retrieved from https://techcrunch.com/2018/07/03/new-malware-highjacks-your-windows-clipboard-to-change-crypto-addresses/

[31] B. Levene, and J. Grunzweig. Sure, Ill take that! New ComboJack Malware Alters Clipboards to Steal Cryptocurrency. Retrieved from https://unit42.paloaltonetworks.com/unit42-sure-ill-take-new-combojack-malware-alters-clipboards-steal-cryptocurrency/, 2018.

[32] M. Apostolaki, A. Zohar, and L. Vanbever. Hijacking bitcoin: Routing attacks on cryptocurrencies. In *Proceedings of the IEEE Symposium on Security and Privacy (SP)*, pages 375–392, 2017.

[33] D. Palmer. A giant botnet is forcing Windows servers to mine cryptocurrency. Retrieved from www.zdnet.com/article/a-giant-botnet-is-forcing-windows-servers-to-mine-cryptocurrency/.

[34] E. Tannam. WannaMine and Smominru: The cryptocurrency botnets causing havoc. Retrieved from www.siliconrepublic.com/enterprise/wannamine-smominru-botnets-cryptocurrency/.

[35] M. Kumar. New cryptocurrency mining malware infected over 500,000 PCs in just few hours. Retrieved from https://thehackernews.com/2018/03/cryptocurrency-mining-malware.html.

[36] H. Washburn. How Adylkuzz uses the EternalBlue Exploit. Retrieved from www.datto.com/au/blog/how-adylkuzz-uses-the-eternalblue-exploit.

[37] J. Gu. Coin miner mobile malware returns, hits Google play. Retrieved from http://blog.trendmicro.com/trendlabs-security-intelligence/coin-miner-mobile-malware-returns-hits-google-play/.

[38] C. Cimpanu. Android malware will destroy your phone. No ifs and buts about it. Retrieved from www.bleepingcomputer.com/news/security/android-malware-will-destroy-your-phone-no-ifs-and-buts-about-it/.

[39] S. Higgins. Google pulls five mobile wallpaper apps due to bitcoin mining malware. Retrieved from www.coindesk.com/google-pulls-six-mobile-wallpaper-apps-bitcoin-mining-malware.
[40] B. Haas and M. Veenstra. Botnet of infected Word-Press sites attacking WordPress sites. Retrieved from www.wordfence.com/blog/2018/12/wordpress-botnet-attacking-wordpress/
[41] K. McCarthy. CBS's Showtime caught mining crypto-coins in viewers' web browsers. Retrieved from https://bit.ly/2gjzQas.
[42] C. Cimpanu. Cryptojacking script found in live Help widget, impacts around 1,500 sites. Retrieved from www.bleepingcomputer.com/news/security/cryptojacking-script-found-in-live-help-widget-impacts-around-1-500-sites/.
[43] P. Greenfield. Government websites hit by cryptocurrency mining malware. Retrieved from www.theguardian.com/technology/2018/feb/11/government-websites-hit-by-cryptocurrency-mining-malware.
[44] J. Grunzweig. Monero miners continue to plague users via Russian BitTorrent site. Retrieved from https://researchcenter.paloaltonetworks.com/2018/03/unit42-monero-miners-continue-plague-users-via-russian-bittorrent-site/.
[45] L. Kelion. Starbucks cafe's wi-fi made computers mine crypto-currency. Retrieved from www.bbc.co.uk/news/technology-42338754.
[46] A. Sulleyman. Hackers infect Facebook Messenger users with malware that secretly mines bitcoin. Retrieved from www.independent.co.uk/life-style/gadgets-and-tech/news/digmine-facebook-messenger-cryptocurrency-mining-malware-monero-bitcoin-a8125021.html.
[47] E. Kent. Steam game accused of turning PCs into cryptocurrency miners. Retrieved from www.eurogamer.net/articles/2018-07-30-steam-game-abstractism-turns-pcs-into-cryptocurrency-miners.
[48] R. McMillan. Gaming company fined 1M dollars for turning customers into secret Bitcoin army. Retrieved from www.wired.com/2013/11/e-sports/.
[49] D. Maciejak. Yet another crypto mining botnet? Retrieved from www.fortinet.com/blog/threat-research/yet-another-crypto-mining-botnet.html.
[50] C. Cimpanu. Sly malware author hides cryptomining botnet behind ever-shifting proxy service. Retrieved from https://dollardestruction.com/15396/.
[51] J. Grunzweig. Large scale Monero cryptocurrency mining operation using XMRig. Retrieved from https://researchcenter.paloaltonetworks.com/2018/01/unit42-large-scale-monero-cryptocurrency-mining-operation-using-xmrig/.
[52] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas. DDoS in the IoT: Mirai and other botnets. *IEEE Computer*, 50:7, 80–84, 2017.
[53] D. McMillen. Mirai IoT Botnet: Mining for Bitcoins? Retrieved from https://securityintelligence.com/mirai-iot-botnet-mining-for-bitcoins/.
[54] B. B. Zarpelao, R.S., Miani, C.T. Kawakani, and S.C.de Alvarenga A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, 84:25–37, 2017.
[55] S. Nomm, and M. Bahsi. Unsupervised anomaly based botnet detection in IoT networks. In *Proceedings of the 17th IEEE International Conference on Machine Learning and Applications*, pages 1048–1053, 2018.

[56] O. Brun, Y. Yin, and E. Gelenbe. Deep learning with dense random neural network for detecting attacks against IoT-Connected home environments. *Procedia Computer Science*, 84:458–463, 2018.

[57] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, Y. A. Shabtai, D. Breiten-Bacher, and Y. Elovici. N-BaIoTNetwork-Based detection of IoT botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, 17 (3):12–22, 2018.

[58] S. Hilt, N. Huq, V. Kropotov, R. McArdle, C. Pernet, and R. Reyes. Exposed and vulnerable critical infrastructure: Water and Energy Industries. In *Trend Micro*, Trend Labs Research Paper, pages 1–70, 2018.

[59] W. Wang, B. Ferrell, X. Xu, K. W. Hamlen, and S. Hao. Seismic: Secure inlined script monitors for interrupting cryptojacks. In *Proceedings of the European Symposium on Research in Computer Security*, pages 122–142. Springer, 2018.

[60] R. Tahir, M. Huzaifa, A. Das, M. Ahmad, C. Gunter, F. Zaffar, M. Caesar, and N. Borisov. Mining on someone elses dime: Mitigating covert mining operations in clouds and enterprises. In *Proceedings of the International Symposium on Research in Attacks*, Intrusions, *and Defenses*, pages 287–310. Springer, 2017.

[61] M. Zwang, S. Somin, A. Pentland, and Y. Altshuler. Detecting bot activity in the Ethereum blockchain network. *arXiv preprint arXiv:1810.01591*, 2018.

[62] S. Stamm, B. Sterne, and G. Markham. Reining in the web with content security policy. In *Proceedings of the 19th International Conference on World Wide Web*, pages 921–930. ACM, 2010.

[63] W. Zeller and E. W. Felten. *Cross-site Request Forgeries: Exploitation and Prevention*. Bericht, Princeton University, 2008.

[64] J. Perez. Cryptomining is all the rage among hackers, as DDoS amplification attacks continue. Retrieved from https://blog.qualys.com/news/2018/03/09/cryptomining-is-all-the-rage-among-hackers-as-ddos-amplification-attacks-grow.

[65] S. T. Ali, P. McCorry, P. H.-J. Lee, and F. Hao. Zombiecoin: Powering next-generation botnets with bitcoin. In *Proceedings of the International Conference on Financial Cryptography and Data Security*, pages 34–48. Springer, 2015.

[66] G. Hurlburt. Shining light on the dark web. *IEEE Computer*, 50:4, 2017.

[67] A. Laszka, B. Johnson, and J. Grossklags. When bitcoin mining pools run dry. In *Proceedings of the International Conference on Financial Cryptography and Data Security*, pages 63–77. Springer, 2015.

[68] E. Jahani, P. M. Krafft, Y. Suhara, E. Moro, and A. Pentland. Scamcoins, s*** posters, and the search for the next bitcoin tm: Collective sensemaking in cryptocurrency discussions. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW):79, 2018.

[69] A. Barysevich, P. Moriuchi, and D. Hatheway. Proliferation of mining malware signals a shift in cybercriminal operations. *In Recorded Future Insikt Group Research Report*, pages 1–17, 2017.

[70] I. Ghafir, V. Prenosil, M. Hammoudeh, T. Baker, S. Jabbar, S. Khalid, S. Jaf. Botdet: A system for real time botnet command and control traffic detection. In *IEEE Access, 6*, pages 38947–38958, 2017.

[71] IBM Whitepaper. Blockchain and GDPR: How blockchain could address five areas associated with GDPR compliance, 2017.

[72] F. Coelho. The GDPR-blockchain paradox: A work around. In Proceedings of the 1st workshop on GDPR compliant systems, co-located with 19th ACM International Middleware Conference, 2018.
[73] O. Jackson. Is it possible to comply with GDPR using blockchain? *International Financial Law Review*, May 2018.
[74] R. Broadhurst, D. Lord, D. Maxim, H. Woodford-Smith, C. Johnston, H. W. Chung, S. Carroll, H. Trivedi, and B. Sabol. Malware trends on darknetcrypto-markets: Research review. *Available at SSRN 3226758*, 2018.
[75] O. Marian. A conceptual framework for the regulation of cryptocurrencies. *University of Chicago Law Review Dialogue*, 82:53, 2015.
[76] J. D. Moran. The impact of regulatory measures imposed on initial coin offerings in the United States market economy. *Catholic University Journal of Law and Technology*, 26(2):7, 2018.
[77] A. J. Watson. The Inaugural Cryptoasset Sentiment Survey. Retrieved from https://medium.com/@ajwatson/the-inaugural-cryptoasset-sentiment-survey-ade3a92ca4d0.
[78] R. Farrell. An analysis of the cryptocurrency industry, Wharton Dissertation, University of Pennsylvania, 2015.
[79] L.-C. Chen and D. Farkas. Individual attitude, trust and risk perception towards blockchain technology, virtual currency exchanges, cryptocurrency transactions and smart contracts. In *AIS Technology Research, Education and Opinion*, 2018.