An Investigation of Cryptojacking: Malware Analysis and Defense Strategies

Victor Marchetto
Marymount University

Xiang (Michelle) Liu
Marymount University

Cybercriminals are capitalizing on the global interest in speculative cryptocurrencies for their own gain. By exploiting vulnerabilities in web browsers and client systems on a large scale, such new operating model named as cryptojacking allows cybercriminals to siphon computational resources from their victims to illicitly generate cryptocurrency. The authors analyze cryptojacking malware samples using both static and dynamic methods and discuss their potential impacts on services running on enterprise servers and operating systems including critical infrastructure industries. The paper further provides strategies for how to detect and defend against these threats.

INTRODUCTION

According to the 2018 Symantec Internet Security Threat Report (ISTR), cryptocurrency mining applications on endpoints was spiking in 2017 by 8500% (Symantec, 2018). Accordingly, a new act of cybercrime scheme centered on cryptocurrency has emerged. During the late 2017 and early 2018, those who have visited MSN.com or Politifact.com, clicked on a YouTube Ad or downloaded a popular app to their Android smartphones may have inadvertently financed cyber criminals involuntarily. Due to its high lucrative nature and low barrier of entry, cyber criminals have swarmed into this emergent attack surface of using coinminers to steal computer processing power and cloud CPU usage from consumers and enterprises to mine cryptocurrency (Symantec, 2018).

From 2016 to 2017 companies such as Coinhive and its contemporaries including CoinImp and deepMiner have created software to embed within webpages that monetizes the compute power from visitors (Krebs, 2018). This is offered as a way to support a website in lieu of traditional advertisements. However, many cyber criminals have seized on the opportunity to forcibly embed this JavaScript within vulnerable websites and ads. For example, a search on https://publicwww.com/, a search index engine for website source code, currently shows upwards of 43,000 websites running a potentially malicious coin mining script. This script requests additional resources from the visitor's browsers for the duration of time staying on the website in order to mine a cryptocurrency called Monero. It has been noted that this script was installed onto websites of high-profile companies such as The Los Angeles Times, Politifact, and Showtime as well as the mobile device maker Blackberry (Krebs, 2018). Another attack attempting to mine the Monero cryptocurrency using the open-source XMRig utility may have affected more than 30 million systems worldwide (Budd, 2018). It was uncovered that attackers utilized a URL link shortening service Bit.ly to hide a drive-by download of malware that installs and runs the Monero mining client.

Cyber criminals are exploring a new operating model called cryptojacking which exploits resources from their victims to illicitly generate cryptocurrency. This new model, if widely adopted, will change the landscape of cybercrime. This paper aims to explore the factors that influenced this development as well as the function and commonalities in current malware campaigns that utilize these techniques. The top 132 malware samples associated with a crypto-mining tag were gathered and analyzed by running static and dynamic malware analysis methods. The authors seek to investigate the risks and potential impacts on individual users as well as larger enterprises. Further, practical guidance on how to mitigate these risks and detect the presence of active malware is put forward and discussed in detail. The last section of this paper concludes with a brief summary of this study and our reflection on the future of these tactics given their current trajectory.

BACKGROUND

The theft of assets and currency are almost as old as civilization itself. The recent introduction of vast interconnected computer systems has not changed the risk versus reward equation that individuals face. The Internet introduced the capacity for goods and services to be bought and sold instantaneously and at great distances. E-commerce, online banking, and the ability to consult a doctor on call via a smartphone are just some of the many modern conveniences available today**.** This technology on one hand provides the basis for these modern conveniences, but also enables old habits to take new forms. Bruce Schneier succinctly sums these parallels in his book, *Secrets and Lies: Digital Security in a Networked World*,

"*The Threats in the digital world mirror the threats in the physical world. If embezzlement is a threat, then digital embezzlement is also a threat. If physical banks are robbed, then digital banks will be robbed…the attacks will look different-the burglar will manipulate digital connections and database entries instead of lock picks and crowbars… But the motivation and psychology will be the same." (Schneier, 2015,* page 25*)*

There are numerous analogies to cryptojacking in the physical world such as siphoning gas or electricity. However, its counterpart in the physical world is rare because it is difficult to access enough cars to supply gas needed for a weeks' worth of driving. Not to mention the high likelihood of discovery and incarceration over a sustained period of time. Cyber criminals, however, are shielded from these dangers by the technical nature of their craft. They can remain anonymous and operate safely behind international borders while carrying out the theft of minimal resources from many devices. With this computational "gasoline" they can refine a profit through the legitimate support of the burgeoning cryptocurrency industry by mining.

SUPPORTING CONDITIONS AND TECHNOLOGY

No one trend or event occurs in a vacuum. Cryptojacking attacks have developed in a supportive cradle of new technology and global trends. Cryptojacking would not be occurring without blockchain technology, the digital currencies based on blockchain technology, the significant global investment in these currencies, and a vast ecosystem of vulnerable devices and services. A brief overview of the concepts of these elements is provided as the foundation for better understanding of such evolving phenomenon and malware analysis.

Blockchain

In 2008, an individual or group named Satoshi Nakamoto published a whitepaper titled *Bitcoin: A Peer-to-Peer Electronic Cash System*. In this document, Nakamoto established the foundation for bitcoin, a digital currency still in use today. Satoshi Nakamoto's identity remains unknown. Nakamoto's goal with bitcoin was to create "a version of electronic cash (that) would allow online payments to be sent directly from one party to another without going through a financial institution" (Nakamoto, 2008, p.1). To do this, Nakamoto created a model of distributed trust. Transactions are made by requesting verification by nodes on the bitcoin network. Once enough of these nodes have come to a consensus about the transaction (i.e., the sender possesses the required funds), the transaction joins other valid and verified transactions and is added to the public ledger. Groups of transactions are known as blocks and the blockchain is a ledger of all previously verified transactions. The blockchain is a public record held by participants in the bitcoin network and is not beholden to any traditional financial institution.

Blockchain and its subsequent developments are heralded as the next great catalyst to modern financial systems. A study published in the Harvard Business Review disclosed that the majority of financial institution in the world have been drawn to blockchain research and 15% of banks were expected to be using blockchain in 2017 (Gupta, 2017). An incentive structure was introduced to reward individuals to support the bitcoin network. This is where bitcoin mining and miners come into play.

Mining Cryptocurrencies

Through the act of mining, individuals or "miners" support cryptocurrencies by validating transactions. The founders of cryptocurrency incentivize this by compensating miners with new coinage. In doing so, new coins can be introduced at a regulated rate. Mining cryptocurrencies is based on a so-called Proof of Work (PoW) consensus mechanism, which accounts for more than 90% of the total market capitalization of existing digital cryptocurrencies (Gervais et al., 2016). The mining process takes the following structure:

1. An unvalidated transaction is added to others adding up to specific size or block by specialized nodes on the network;
2. A miner solves a computationally intensive puzzle, known as the Proof of Work (PoW);
3. This solution (PoW) is then communicated to other miners on the network;
4. Other miners validate this solution;
5. Enough miners come to a consensus on the validity of this solution;
6. The block of transactions is added to the Blockchain;
7. The miner receives the predetermined reward along with additional transaction fees.

For instance, the bitcoin PoW utilizes the SHA256 hashing algorithm. To solve a PoW the miner must guess a nonce (i.e., arbitrary single use number) that produces a value that meets the difficulty criteria when combined with the following data and hashed twice with the SHA256 algorithm:

- Timestamp;
- Bitcoin version;
- Previous Blockhash; and
- Merkle root of unvalidated transactions.

This difficulty rate is provided by the network and is a number starting with 0s. For example, a successful answer to the PoW challenge for a difficulty requiring 15 zeros could look like this.

00000000000000029870946B63E11EE744355454F78181FE19D76CB63C9F4054

The current SHA256 digest value of this paper computes to the following:

585CE87F4AE51ED29870946B63E11EE744355454F78181FE19D76CB63C9F4054

Even adding a single character will change the algorithm's output to the following:

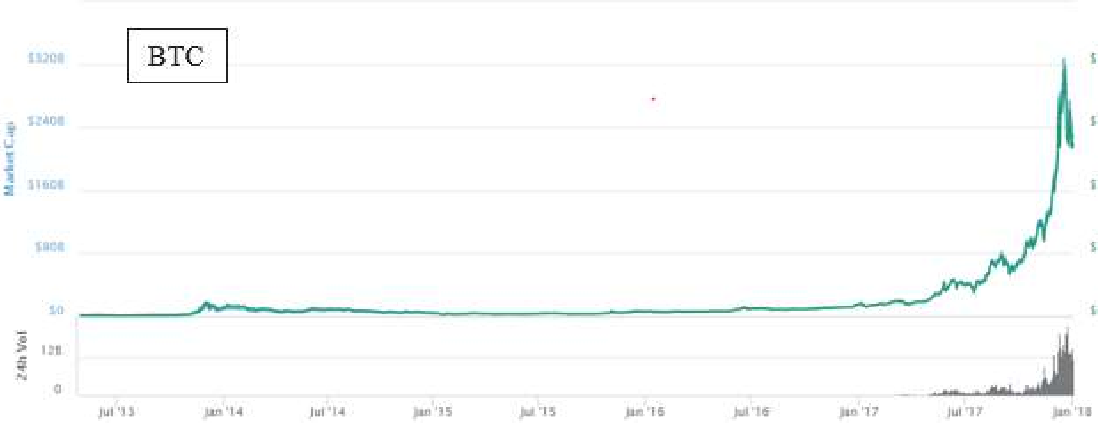
17B7A8B13F0B725FA180A637C299532B0BDF35907B46CB94F7EEAAC3F9EB0C70

This digest is currently not reversible, which is known as a one-way function. The more computational power a miner or mining pool possesses, the faster and the greater chances it has of discovering the correct nonce. There are a fixed number of acceptable outputs per difficulty which gives bitcoin and other cryptocurrencies their fixed total supply.

Speculative Cryptocurrency and Its Unintended Consequences

There has been a meteoric rise in the price of many cryptocurrencies during the year of 2017. This can be seen in Figure 1 which charts the price of a single unit (teal) as well as the market capitalization (black). Bitcoin, for example, hit an all-time high of $19,530 in December 2017. Cryptocurrencies generally function outside and apart from the traditional institutions of wealth, i.e. states and precious resources. This increase was the result of a rising mania surrounding cryptocurrencies as it became easier to convert fiat currencies (like the dollar) into various cryptocurrencies.

FIGURE 1
CYPTOCURRENCY MARKET CAPITALIZATION PROVIDED BY COINMARKETCAP.COM



What is possible association between this rise and the cybercriminal market? Some cybersecurity professionals speculated an interesting correlation between cryptocurrencies and instances of ransomware styled malware. (Kshetri and Voas, 2017). Ransomware is a type of cyber attack where the threat actor is able to deny the user access to their device or data, usually achieved through unsanctioned encryption. A ransom note is left on the device demanding payment in exchange for the encryption key. Ransomware as a business model is more of a gamble than cryptojacking because not every ransomware victim elects to pay the ransom, but every cryptojacking victim helps generate digital revenue for the attacker.

There has been interplay between the rise in cryptocurrency market value and the increase in browser-based cryptojacking attacks (Marshall, 2018). The researcher further revealed that approximately 1 in 1,000 of the top websites is running Coinhive scripts intentionally or unintentionally. Cryptojacking and ransomware both "succeed" by generating a sum of cryptocurrency for the attacker so they share an affinity for a strong cryptocurrency industry. A growing cryptocurrency market supports a malware ecosystem by providing a safe means of stealing money. For instance, cryptocurrencies such as Monero, Dash, and Z-Cash can reduce the probability of detection due to their built-in anonymity features (Kshetri and Voas, 2017).

Monero (XMR): Cryptojacker's Choice

Monero was minted in April 2014 as an offshoot of CryptoNote v 2.0, designed in 2013 by Nicolas van Saberhagen. Its goals were to provide the following attributes missing in Bitcoin and other cryptocurrencies:

- **Untraceability**: Each transaction has an equal probability to be sent by all possible senders.

- **Unlinkability**: It is impossible to prove that any two transactions were sent to the same address.

Unlike Bitcoin, Monero is focused on privacy. It is not currently possible to ascertain who sent a payment, who has received it, and how much XMR was sent without the disclosure of either the sender or receiver. This is due to a complex implementation of cryptography. XMR's have no maximum supply and the difficulty can be adjusted over time to control inflation. With these features it is no wonder that criminals are interested in incorporating Monero into their business models. For example, Alphabay, a dark market site, offered its vendors the option to accept Monero as an alternative to Bitcoin (Greenberg, 2017).

MALWARE ANALYSIS

To analyze and better understand the techniques used by native attacks for this research, the authors first gathered malware samples using VirusTotal. VirusTotal is a service offered to the public where one can submit files or URLs which are then scanned by over 70 different antivirus and URL filtering products. The scan results include the number of antivirus engines that convicted the scanned file as malicious. This gives a crowd-based verdict of what has been classified as malicious as well as the unique name for a given antivirus engine. The top 132 malware samples associated with a crypto-mining tag were acquired and a safe testing environment was set up where we could analyze the samples.

To test the samples gathered from VirusTotal, it is important to take the proper precautions. Both the testing environment and malware analysis methods were carefully configured and conducted based on the widely adopted malware analysis guidelines (Sikorski and Honig, 2012). The authors utilized a type 2 hypervisor, Oracle's VirtualBox, to simulate a separate operating system or Virtual Machine (VM). One of the benefits of having multiple VMs is that we can limit its connection to the outside network and also save uninfected configurations. This allows us to run suspected malicious files and observe as well as record their behavior without the risk of infecting other devices on our network or compromising the VM. After a specific observation is complete, we can roll back the state to a known good, uninfected state and attempt another observation.

Static Method and Dynamic Method

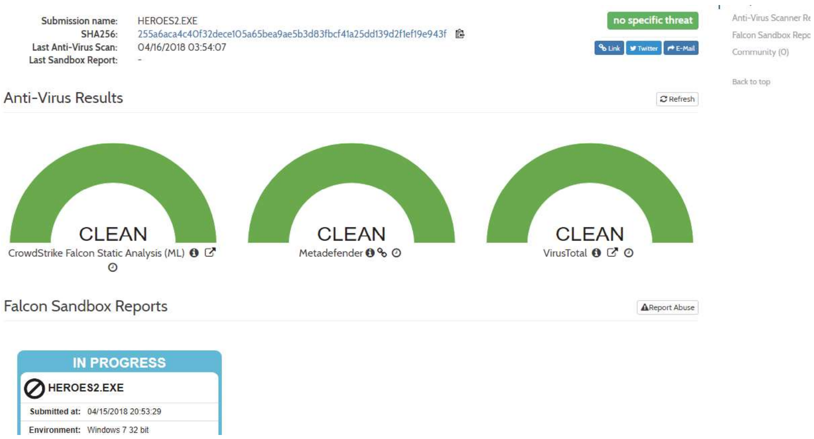
Static analysis focuses on observing what the characteristics of a malware file can show about its nature. We utilized a program called PEStudio which can at a glance provide information including the original filename, the architecture it was written for, imported libraries, and possible relevant strings.

Dynamic methods attempt to elicit malicious behavior by running and observing the behavior of a portable executable (PE). This was completed by running two separate programs: RegShot and Process Monitor. RegShot allows for the comparison of the windows registry hive before and after running a program or set of programs. Process Monitor captures process level events and threads as they occur in real time. This filters for a specific program and records its activity to see the libraries it may call, or files it may create.

A sandbox is a purpose-built environment used to test and simulate a victim in order to catalogue its behavior. This detection approach takes more time than the signature based matching that traditional antivirus software employees. A sandbox can take a pre-programmed approach and attempt a number of different techniques. Malware sandboxes are deployed as an alternate form of detection and as a means of automating a malware analyst's first look at a particular sample. We used the Hybrid-Analysis web service which provides some flexibility in the vulnerable operating system and individual parameters of the vulnerable machines within the sandbox. Hybrid-Analysis will submit the PE file against a number of specific engines as well as generating a report, as depicted in Figure 2.

We used this malware sandbox to validate and provide additional context for the findings produced by the static and dynamic analysis.

FIGURE 2
CLEAN REPORT SAMPLE FROM HYBRID-ANALYSIS.COM



Submission name: HEROES2.EXE
SHA256: 255a6aca4c40f32dece105a65bea9ae5b3d83fbcf41a25dd139d2f1ef19e943f
Last Anti-Virus Scan: 04/16/2018 03:54:07
Last Sandbox Report: -

Anti-Virus Results

CLEAN — CrowdStrike Falcon Static Analysis (ML)
CLEAN — Metadefender
CLEAN — VirusTotal

Falcon Sandbox Reports

IN PROGRESS
HEROES2.EXE
Submitted at: 04/15/2018 20:53:29
Environment: Windows 7 32 bit

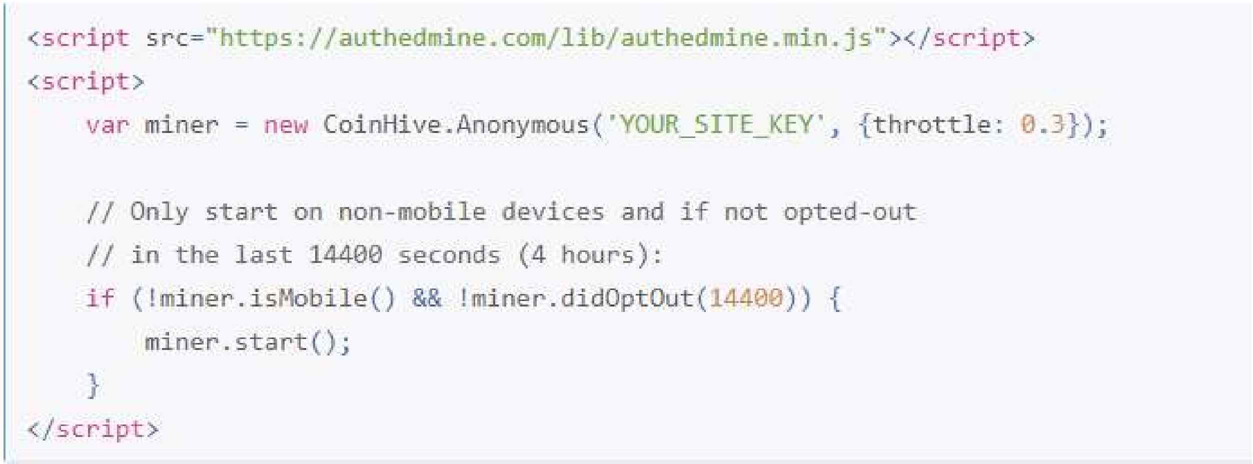
CRYPTOJACKING ATTACK VECTORS

We examined multiple attack vectors of cryptojacking in this section. Detailed analyses and discussions are provided also.

Hijacking the Browser

Browser based attacks have the benefit of potentially affecting a large population of victims without having the difficulty of persisting on as many systems. By injecting a mining script into an ad or webpage, the cryptojacker is able to profit off of its popularity. There are different javascript miners as discussed in this section; the most utilized being the Coinhive service. Figure 3 is a depiction of the Coinhive service.

FIGURE 3
COINHIVE SERVICE



```
<script src="https://authedmine.com/lib/authedmine.min.js"></script>
<script>
    var miner = new CoinHive.Anonymous('YOUR_SITE_KEY', {throttle: 0.3});

    // Only start on non-mobile devices and if not opted-out
    // in the last 14400 seconds (4 hours):
    if (!miner.isMobile() && !miner.didOptOut(14400)) {
        miner.start();
    }
</script>
```

ADOPTED FROM COINHIVE DOCUMENTATION

This service requires a site key that is provided by creating an account with Coinhive. There is also a throttle to attempt to limit the user's CPU usage. According to Coinhive, the site administrator or cryptojacker can expect to turn a monthly profit (not accounting for fees) of approximately .3 XMR or $76.08 USD from a single site sustaining 10-20 miners. It is in the cryptojacker's best interest to install the Coinhive or similar browser mining script in as many sites as possible and to keep a close watch on the XMR payouts to avoid being locked out by potential abuse claims from their victims. In such a case, the cryptojacker will need to update the installed script to match a newly generated sitekey.

Native Code Attacks

This type of attack vector refers to malware designed to run on vulnerable endpoint devices such as personal PCs or servers. They are installed through different processes but run natively on the device. We drew from a pool of 132 malware samples. These samples with a few exceptions were targeting the Windows OS. 96 of which appear to be masquerading as a free Chinese antivirus application, 360 Security by Qihoo 360 Technology Co. Ltd. This product is free to the public. 23 others appeared to be a masquerading as a nondescript folder and later identified as a worm-type. 5 others appear to mining clients outright.

The workflow starts with fingerprinting the sample. Three samples are shown as in Figure A1 that share the 360 Security file name mark and their respective hash digest values. Each has the same company information of 360.cn as well as the same original file name. It was noticed when looking at the section headers that one was packed or compressed with the UPX packer, as shown in Figure A2. By packing or compressing the PE file, the attacker can sometimes evade detection by antivirus software. Programs are rarely created with all the resources and functions they require. It is more efficient for them to import these libraries so they can be referenced within the program. At this stage you can glean clues to behavior from the functions and libraries a PE imports.

Strings are important clues to a malware's capabilities and behavior. A string is a sequence of characters such as "the." A program contains strings if it prints a message, connects to a URL, or copies a file to a specific location. There were a number of suspicious strings which will shed light during dynamic analysis. In these three samples we found the strings containing the Coinhive mining script. Each of these samples is configured to mine for the following site key:

yuNWeGn9GWL72dONBX8WNEj1aVHxg49

This would indicate that these samples are the work of the same threat actor. All three samples of the Zhudongfangyu.exe type show these elements suggesting they are variants of the same original malware (Figure A4). It also appears that the virus is looking for .com, .scr, .pif, .html., .gho, and .iso files. We verified this by creating an .html file to see what the malware would do with it. Test.html was infected as it spawned the zhudongfangyu.exe process (Figure A5). Icon changes throughout the test environment also corroborate this behavior (Figure A6). This malware disables registry tools (Figure A7).

There is also an interesting grouping of IP addresses. Some of these addresses are associated with antivirus products. (Qihoo.com, Kaspersky.com, Nod32club, Virustoal.com, Eset.com) It appears that the loop back address 127.0.0.1 is used to disable access to updates as well as these websites (Figure A8). After running the program, many of these addresses are also captured in the program's memory (Figure A9). Some of these IP addresses, namely 58.17.236.92 may be associated with the virus's command and control server. This allows the malware author to issue new commands and updates to their successfully installed malware. In the strings there was also a file location on a user's(jim) computer in the metro research folder. It is interesting to find personal artifacts in these samples (Figure A10). The malware is also targeting the safe boot settings and the autorun/autoplay feature in some fashion. This is a persistence mechanism which makes it harder for the user to remove the virus through a safeboot that disables networking on the device (Figure A11). This malware creates a value in the registry to run itself (Figure A12). It also disables the security settings on internet explorer (Figure A13). The malware alters the registry to not show hidden files or folders in an attempt to hide the Zhudonfangyu.exe PE file (Figure A14). When running the file the browser CPU usage can be seen to spike (Figure A15). Hybrid-Analysis.com reports that these PE files exhibit the following behavior (Figure A16).

This virus functions by injecting itself and the Coinhive javascript into many files and programs on the device. In this way, the user will run this script and begin mining for the malware's authors as he or she attempts to continue using their device. This virus also takes efforts to persist on the device and resist removal by disabling security features possibly present on the device. This prolongs the time that the malware can coopt the device's CPU to mine Monero.

We also conducted malware analysis on cryptomining worm (Night Miner). This worm disguises itself by appearing as an images folder which prompts the user to click it and thus start its attack routine. This malware is particularly dangerous as it can spread itself to connected media as well as networkshares, broadening the scope of the initial infection. Once running it spawns a CPU miner with preset instructions to join with existing pools to mine Monero.

Both sampled malware types had different methods and used different techniques but both had the same visible goal. Their aim once landing on the device was to force the device to launch a cryptocurrency miner to mine Monero. Zhudongfangyu.exe did this through injecting the Coinhive javascript into various file types on victim computer and the Night Miner worm launched a local CPU miner and attempted to spread to other network locations as well as attached media. The native code attacks differ from the browser based attacks in that they are working towards bringing the devices under control instead of harvesting a captive browsing audience.

IMPACTS

According to the Cisco 2018 Security Capabilities Benchmark Study, 53% of cyber attacks costed organizations upwards of $500K in 2017 (Cisco, 2018). However, measuring impact is largely about context. A denial of service attack on a server providing an underutilized nonessential service is not often a top priority. The impact for different cyber-attacks will vary from industry to industry as well as between individual companies. Cryptojacking attacks appear to be more benign when compared with ransomware or sensitive information theft, but they can still present unplanned costs that individuals and organizations must deal with.

First, the impact for critical services such as access to water and electricity is possibly severe and might endanger lives and economies. SCADA systems and their Operational Technology (OT) networks are attractive targets for cryptojacking attacks because often legacy software must run unpatched to interface with industrial control software. These systems are also designed to be well over scoped for the average workload due to the critical nature of the service they provide. In February of 2018, the security firm Radiflow had encountered a cryptojacking attack on the Operational Technology network of a Water Utility company. According to the Radiflow's CTO Yehonatan Kfir (Miller, 2018), *"Cryptocurrency (cryptojacking) malware attacks involve extremely high CPU processing and network bandwixdth consumption, which can threaten the stability and availability of the physical processes of a critical infrastructure operator. This new case of a cryptocurrency malware attack on an OT network poses new threats as it runs in stealth mode and can remain undetected over time."* Time will tell what cost society will pay if this attack is repeated.

Second, the IT industry continues to go through a revolution in the freedom to consume IT resources and software via cloud offerings. Amazon Web Services (AWS) and Microsoft Azure are two of the largest platforms that provide companies and agencies with servers, storage, or software like the MS Office Suite on demand. This provides many benefits, one being the ability to pay for what you use. However, if these Windows or Linux servers were infected with a cryptojacking virus, an organization could find themselves with a large, unplanned bill from AWS or Microsoft. While Amazon and Microsoft offer security features and oversite to products they operate on a shared responsibility model, the tenant, or customer, must also provide their own security controls and oversight in addition to what is offered. Just as the customer is expected to secure the networks and assets on premise, so to must they be expected to play a part in the security of these workloads in Amazon or Microsoft datacenters.

Third, networks on premise are not safe from the impact of a cryptojacking attack. As demonstrated in the Night Miner worm sample gathered during our research, one infection can be spread through

Windows network shares to other vulnerable nodes on the network. Left unchecked, this can significantly slow down services and responsiveness. This may generate costs for the organization by accelerating the wear of IT equipment. There is also the productivity cost to consider. If end users are constantly waiting for services, they may become frustrated as well as require more time to complete tasks. Beyond the effect to networked services, cryptojacking malware often introduces backdoors so the threat actors can modify and tweak the settings. There is also an underground market for access to organizations. It may become more lucrative for a cyberjacker to provide access at some point.

Lastly, according the Cisco study, 55% of companies had to manage their public image after a cybersecurity breach (Cisco, 2018). It is hard to measure the cost of brand damage, but hiring independent Incident Response professionals in order to timely disclose relevant information about a breach to affected parties can cost organizations hundreds of thousands of dollars respective to the size of the breach.

DEFENSE STRATEGIES

There are system and network monitoring tools ranging from open source to proprietary. Monitoring network traffic with deep packet inspection at the firewall can offer administrators the opportunity to write broad reaching policies to prevent mining traffic from within the network. Endpoint detection software companies are including a suite of functions known as endpoint detection and response (EDR). This feature set monitors the system and the applications running on it at any given time. Who runs what process, what child processes did it spawn, what external IP has it attempted to contact, and what share of the system's resources has it requested. These are all examples of the informational time EDR can supply to system administrators.

As many cryptojacking attacks target the browser, this would seem an ideal place to thwart the cryptojacker. There are browser plugins which can assist the user in this task. Some specifically target mining sites like NoCoin. NoCoin and its ilk function like anad blocker, but targeted to URLs associated with the javascript mining operation such as "*://coinhive.com/lib*" or "*://cryptoloot.pro/lib/*". This application's author regularly updates a list of 158 libraries and scripts. It also provides the user the ability to temporarily whitelist a site if the user wishes to cooperate with a legitimate use of cryptomining. Extensions like ScriptSafe accomplish the same task by blocking all JavaScript by default. This implicit deny trades convenience for security and requires the user to allow or trust sites to enable features that require JavaScript.

Traditional antivirus is a legacy application. As the endpoint is most often the intended target for malware, it is prudent to continue to improve the efficacy of the detection and prevention of malicious activity at the intended target. Many commercially available endpoint security products provide a spectrum of detection and protection methods including machine learning algorithms, pre-exploit protection, sandbox analysis, and application vulnerability scans. It is imperative that more than one malware detection methods to be employed to protect the endpoint. The days of relying on an antivirus scanner to accurately convict files based on static signatures have passed. Conveniently, many products can offer multiple layers of insight in a single software platform.

As the proverbial yellow pages to the internet, the Domain Name System (DNS) is integral to the internet. Solutions like Cisco's Umbrella, WebTitan, and StrongArm.IO provide the ability to use a custom DNS server which omits known malicious IP addresses. In this way if the end user contacts malware from another source, the command and control communications cannot proceed as those addresses do not resolve in the custom DNS database. These network security appliances provide the ability for organizations to filter traffic as it passes the device. They are particularly useful as if properly configured can go undetected by the intruder. The intrusion prevention service and intrusion detection service function differently as one can take action while the other informs only. These network security solutions can sometimes detect cryptojacking network activity. This was how Radiflow being able to discover the cryptojacking malware on their customer's OT network.

Finally, policy is important to an organization because it functions as reference for acceptable and prudent process. Most organizations have a fair use policy where the organization outlines its expectations regarding electronic equipment such as personal computers and wireless infrastructure. The goal of such a policy is to protect employees and the organization from risk incurred by inappropriate use.

CONCLUSIONS

Cryptojacking is still evolving. It has shown to be a product of its environment. Namely, it is the culmination of a technology that provides untraceability, unlinkability, and the ability to trade computational resources, electricity and time for a digital currency. Monero helps to lower risks for cybercriminals as it provides anonymity in a revenue stream. Illicit goods and services can be purchased with Monero or it can be exchanged for another cryptocurrency and eventually fiat currency like the U.S. Dollar or Russian Ruble. This incentivizes cybercriminals to lower the cost of mining Monero by stealing the resources from their victims any way they can.

As cryptojacking continues to be adopted we can be certain to see its effects on organizations and their services. These attacks can cost organizations by slowing down or denying networked services, causing brand damage, or causing advanced wear and unbudgeted expenses. Much of the malware resident on the endpoint targets the Windows operating system which will remain a global constant for the foreseeable future.

There are defense strategies and technologies organizations can deploy to combat this growing criminal practice. An important step in meeting this threat is to understand the objective, behavior, and indicators of cryptojacking attacks. As the cyber threat landscape evolves, responses must adapt to understand, overcome, and ultimately defeat it.

REFERENCES

Budd, C. (2018, January 4). Threat Brief Malware Authors Mine Monero Across Globe Big Way. Retrieved from https://researchcenter.paloaltonetworks.com/2018/01/threat-brief-malware-authors-mine-monero-across-globe-big-way/

Cisco (2018, February). Cisco Annual Cybersecurity Report 2018. Retrieved from https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fa27ff73da9690a5b&elqaid=9452&elqat=2

Gervais, A., Karame, G., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the security and performance of proof of work blockchains. *Paper presented at the 2016 ACM SIGSAC Conference,* 3-16. doi:10.1145/2976749.2978341

Greenberg, A. (2017, January 25). Monero, The Drug Dealer's Cryptocurrency of Choice, is on Fire. *Wired.* Retrieved from https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/

Gupta, V. (2017, February 28). A Brief History of Blockchain. *Harvard Business Review*. Retrieved from https://hbr.org/2017/02/a-brief-history-of-blockchain

Krebs, B. (2018, March 18). Who and What Is Coinhive? Retrieved from https://krebsonsecurity.com/?s=coinhive&x=0&y=0

Kshetri, N., & Voas, J. (2017). Do crypto-currencies fuel ransomware? *IT Professional,* 19(5), 11-15. doi:10.1109/MITP.2017.3680961

Marshall, S. (2018). *Cryptomining: Paying the price for cryptocurrency.* Retrieved from https://www.lookingglasscyber.com/news/cryptomining-paying-the-price-for-cryptocurrency/.

Miller, T. (2018, February 08). Radiflow Reveals First Documented Cryptocurrency Malware Attack on a SCADA Network. Retrieved from https://www.prnewswire.com/news-releases/radiflow-reveals-first-documented-cryptocurrency-malware-attack-on-a-scada-network-300595714.html

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

Schneier, B. (2015). *Secrets and lies* (15th anniversary ed.). Indianapolis, In: Wiley.

Sikorski, M., & Honig, A. (2012). *Practical malware analysis* (9th ed.). San Francisco: No Starch Press.

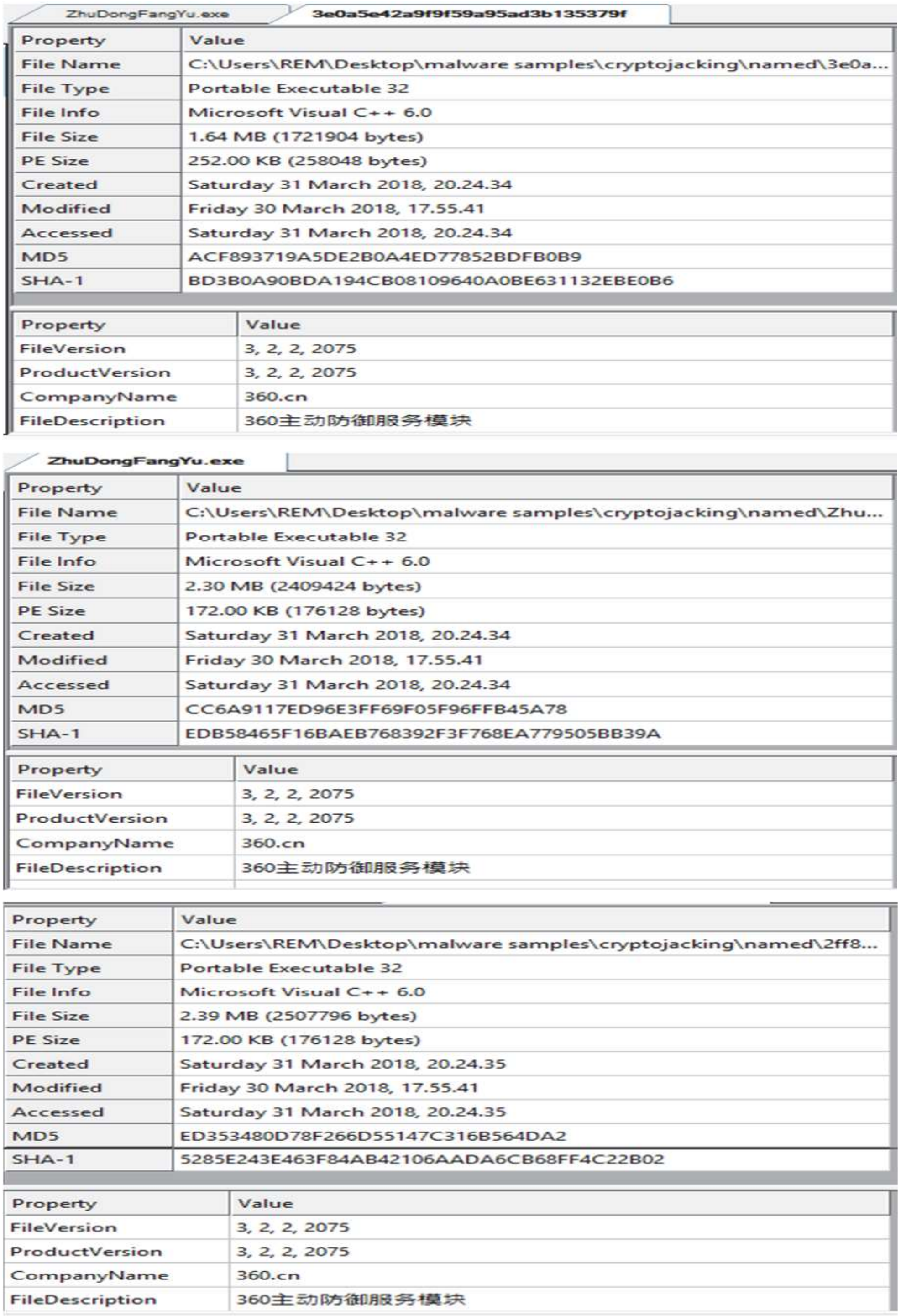
Symantec. (2018). 2018 Internet Security Threat Report (ISTR). Retrieved from https://www.symantec.com/security-center/threat-report

APPENDIX A

Malware Analysis Figures

***Note:** Due to the space limitation, only sample figures are included in this version of the paper.

FIGURE A1
THREE MALWARE SAMPLE FINGERPRINTING



Property	Value
File Name	C:\Users\REM\Desktop\malware samples\cryptojacking\named\3e0a...
File Type	Portable Executable 32
File Info	Microsoft Visual C++ 6.0
File Size	1.64 MB (1721904 bytes)
PE Size	252.00 KB (258048 bytes)
Created	Saturday 31 March 2018, 20.24.34
Modified	Friday 30 March 2018, 17.55.41
Accessed	Saturday 31 March 2018, 20.24.34
MD5	ACF893719A5DE2B0A4ED77852BDFB0B9
SHA-1	BD3B0A90BDA194CB08109640A0BE631132EBE0B6

Property	Value
FileVersion	3, 2, 2, 2075
ProductVersion	3, 2, 2, 2075
CompanyName	360.cn
FileDescription	360主动防御服务模块

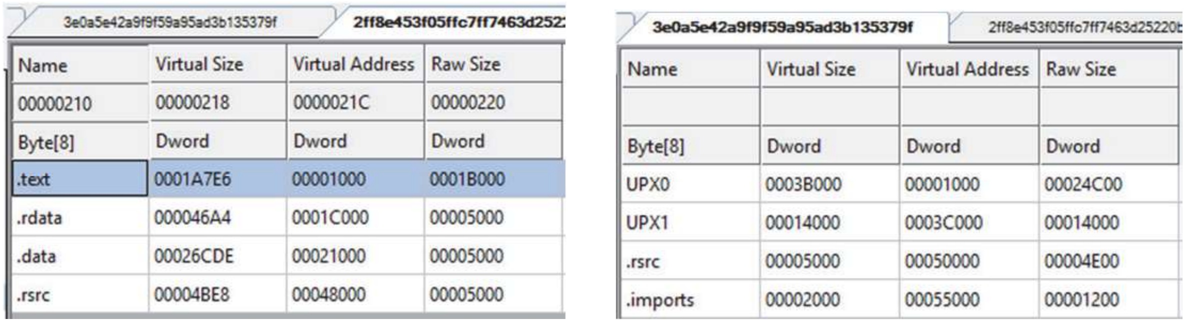
Property	Value
File Name	C:\Users\REM\Desktop\malware samples\cryptojacking\named\Zhu...
File Type	Portable Executable 32
File Info	Microsoft Visual C++ 6.0
File Size	2.30 MB (2409424 bytes)
PE Size	172.00 KB (176128 bytes)
Created	Saturday 31 March 2018, 20.24.34
Modified	Friday 30 March 2018, 17.55.41
Accessed	Saturday 31 March 2018, 20.24.34
MD5	CC6A9117ED96E3FF69F05F96FFB45A78
SHA-1	EDB58465F16BAEB768392F3F768EA779505BB39A

Property	Value
FileVersion	3, 2, 2, 2075
ProductVersion	3, 2, 2, 2075
CompanyName	360.cn
FileDescription	360主动防御服务模块

Property	Value
File Name	C:\Users\REM\Desktop\malware samples\cryptojacking\named\2ff8...
File Type	Portable Executable 32
File Info	Microsoft Visual C++ 6.0
File Size	2.39 MB (2507796 bytes)
PE Size	172.00 KB (176128 bytes)
Created	Saturday 31 March 2018, 20.24.35
Modified	Friday 30 March 2018, 17.55.41
Accessed	Saturday 31 March 2018, 20.24.35
MD5	ED353480D78F266D55147C316B564DA2
SHA-1	5285E243E463F84AB42106AADA6CB68FF4C22B02

Property	Value
FileVersion	3, 2, 2, 2075
ProductVersion	3, 2, 2, 2075
CompanyName	360.cn
FileDescription	360主动防御服务模块

FIGURE A2
HEADER ANALYSIS



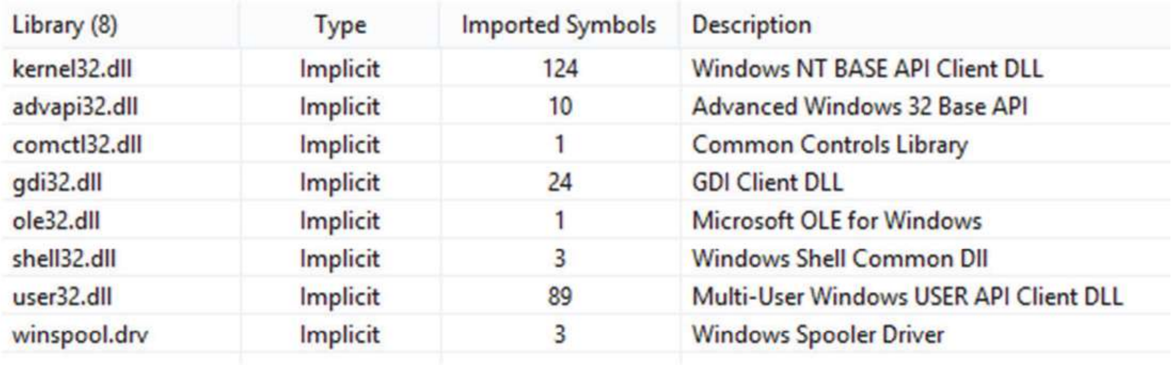
3e0a5e42a9f9f59a95ad3b135379f | 2ff8e453f05ffc7ff7463d2522

Name	Virtual Size	Virtual Address	Raw Size
00000210	00000218	0000021C	00000220
Byte[8]	Dword	Dword	Dword
.text	0001A7E6	00001000	0001B000
.rdata	000046A4	0001C000	00005000
.data	00026CDE	00021000	00005000
.rsrc	00004BE8	00048000	00005000

3e0a5e42a9f9f59a95ad3b135379f | 2ff8e453f05ffc7ff7463d25220b

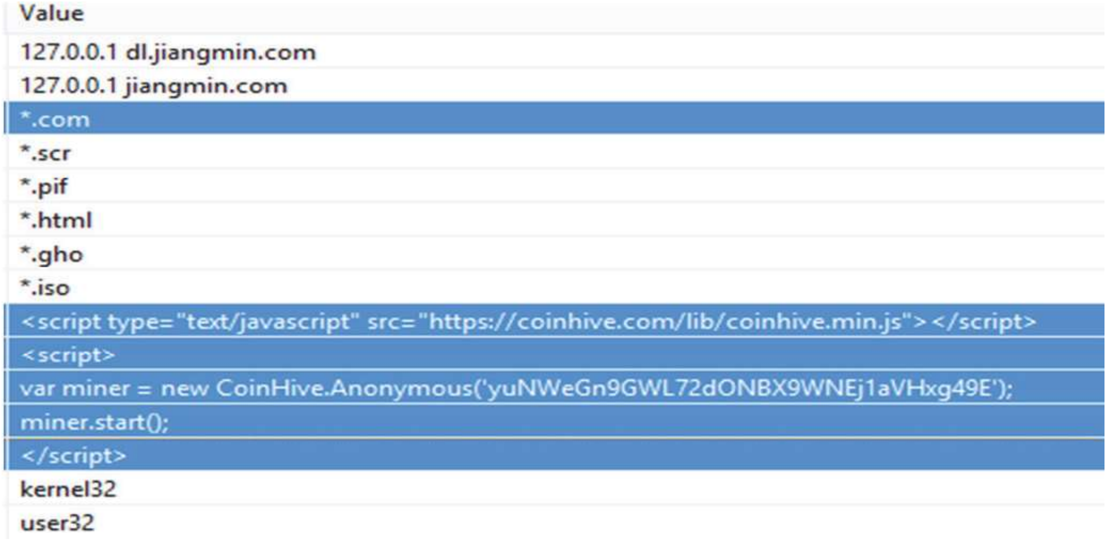
Name	Virtual Size	Virtual Address	Raw Size
Byte[8]	Dword	Dword	Dword
UPX0	0003B000	00001000	00024C00
UPX1	00014000	0003C000	00014000
.rsrc	00005000	00050000	00004E00
.imports	00002000	00055000	00001200

FIGURE A3
MALWARE FILE INFORMATION



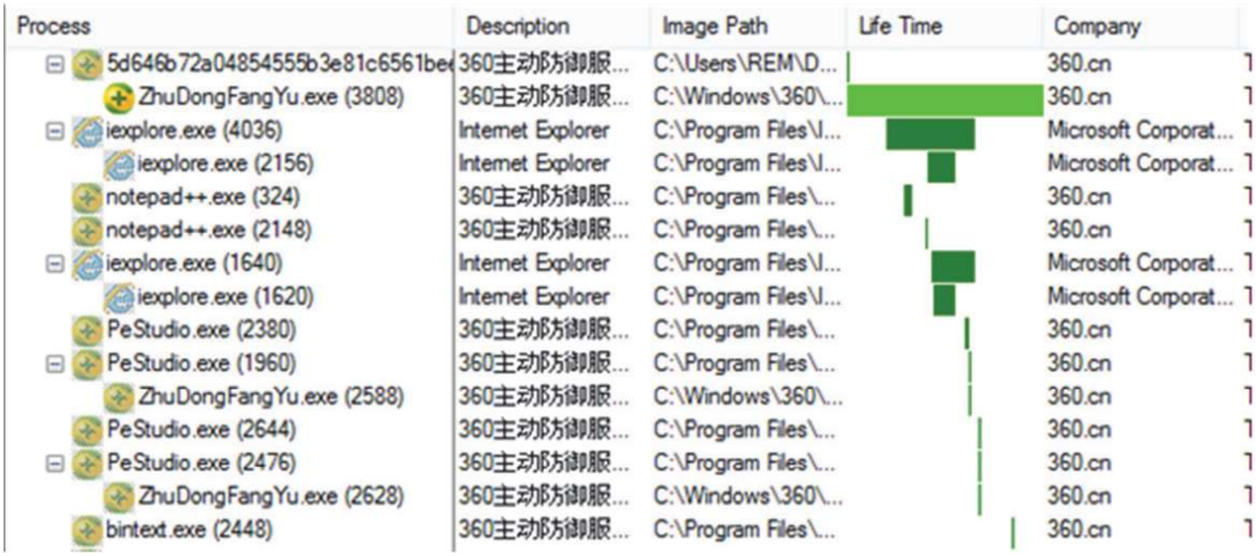
Library (8)	Type	Imported Symbols	Description
kernel32.dll	Implicit	124	Windows NT BASE API Client DLL
advapi32.dll	Implicit	10	Advanced Windows 32 Base API
comctl32.dll	Implicit	1	Common Controls Library
gdi32.dll	Implicit	24	GDI Client DLL
ole32.dll	Implicit	1	Microsoft OLE for Windows
shell32.dll	Implicit	3	Windows Shell Common Dll
user32.dll	Implicit	89	Multi-User Windows USER API Client DLL
winspool.drv	Implicit	3	Windows Spooler Driver

FIGURE A4
Zhudongfangyu.exe MALWARE SAMPLE



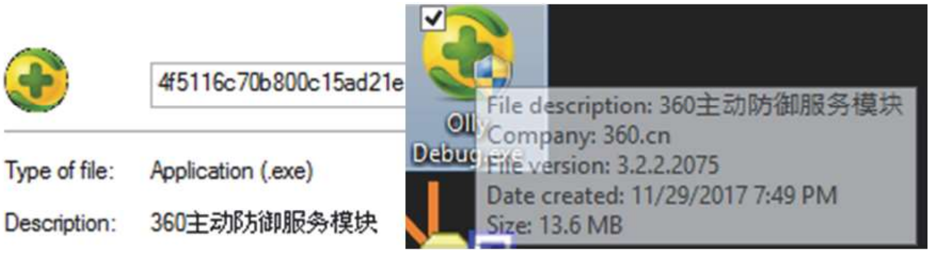
Value
127.0.0.1 dl.jiangmin.com
127.0.0.1 jiangmin.com
*.com
*.scr
*.pif
*.html
*.gho
*.iso
<script type="text/javascript" src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
var miner = new CoinHive.Anonymous('yuNWeGn9GWL72dONBX9WNEj1aVHxg49E');
miner.start();
</script>
kernel32
user32

FIGURE A5
Zhudongfangyu.exe SPAWNING PATH



Process	Description	Image Path	Life Time	Company
5d646b72a04854555b3e81c6561be	360主动防御服...	C:\Users\REM\D...		360.cn
ZhuDongFangYu.exe (3808)	360主动防御服...	C:\Windows\360\...		360.cn
iexplore.exe (4036)	Internet Explorer	C:\Program Files\I...		Microsoft Corporat...
iexplore.exe (2156)	Internet Explorer	C:\Program Files\I...		Microsoft Corporat...
notepad++.exe (324)	360主动防御服...	C:\Program Files\...		360.cn
notepad++.exe (2148)	360主动防御服...	C:\Program Files\...		360.cn
iexplore.exe (1640)	Internet Explorer	C:\Program Files\I...		Microsoft Corporat...
iexplore.exe (1620)	Internet Explorer	C:\Program Files\I...		Microsoft Corporat...
PeStudio.exe (2380)	360主动防御服...	C:\Program Files\...		360.cn
PeStudio.exe (1960)	360主动防御服...	C:\Program Files\...		360.cn
ZhuDongFangYu.exe (2588)	360主动防御服...	C:\Windows\360\...		360.cn
PeStudio.exe (2644)	360主动防御服...	C:\Program Files\...		360.cn
PeStudio.exe (2476)	360主动防御服...	C:\Program Files\...		360.cn
ZhuDongFangYu.exe (2628)	360主动防御服...	C:\Windows\360\...		360.cn
bintext.exe (2448)	360主动防御服...	C:\Program Files\...		360.cn

FIGURE A6
ICON CHANGE



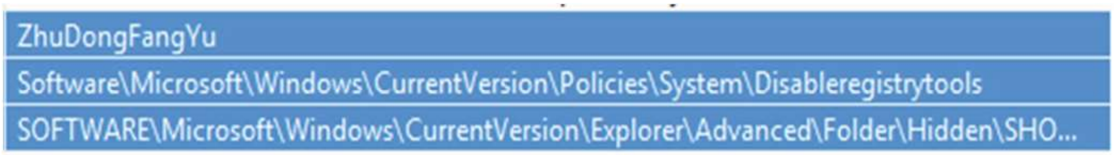
4f5116c70b800c15ad21e

Type of file: Application (.exe)

Description: 360主动防御服务模块

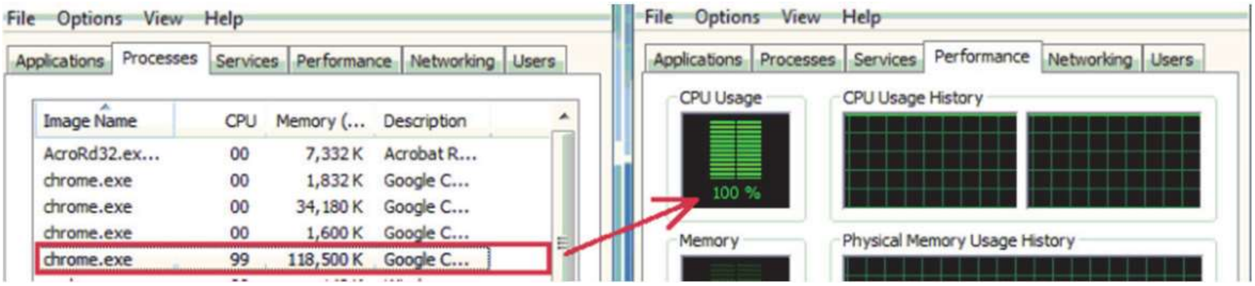
File description: 360主动防御服务模块
Company: 360.cn
File version: 3.2.2.2075
Date created: 11/29/2017 7:49 PM
Size: 13.6 MB

FIGURE A7
REGISTRY TOOL



ZhuDongFangYu
Software\Microsoft\Windows\CurrentVersion\Policies\System\Disableregistrytools
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHO...

FIGURE A15
CPU USAGE SPIKING



File Options View Help
Applications Processes Services Performance Networking Users
File Options View Help
Applications Processes Services Performance Networking Users
CPU Usage
CPU Usage History
Memory
Physical Memory Usage History

Image Name	CPU	Memory (...	Description
AcroRd32.ex...	00	7,332 K	Acrobat R...
chrome.exe	00	1,832 K	Google C...
chrome.exe	00	34,180 K	Google C...
chrome.exe	00	1,600 K	Google C...
chrome.exe	99	118,500 K	Google C...

100 %