The State of the Art of Cryptography-Based Cyber-Attacks

Srirath Gohwong
Faculty of Social Sciences, Kasetsart University, Thailand
E-mail: srirathg3@yahoo.com

Article History
Received: 24 June 2019 **Revised:** 1 August 2019 **Published:** 30 September 2019

Abstract
This paper objective was to investigate the state of the art of crypto-based cyber-attacks during 1989-2019. Documentary research was employed for data analysis. The findings found that cryptography-based cyber-attacks during 1989-2019 could be defined as any attacks mainly focus on encryption technology-related crimes, classified into five key groups-ransomware, cryptojacking, coin thief, illegal money transfer, and fake identity. Simultaneously, dirty fiat currency and dirty cryptocurrency were investigated in these categories as mediums of exchange in cybercrimes. In addition, profit and availability were two key incentives for cryptography-based cyber-attackers during 1989-2009. Cybercriminals would change cryptography-based tools and targeted groups or market back and forth due to rise and fall of profit from their attacks. For profit-oriented incentive, cryptojacking, ransomware, coin thief, and illegal money transfer were key cybercrimes. In addition, cybercriminals intentionally lessened availability of their targeted devices of victims with sabotage-oriented disk wipers. Last, all illegal activities-based classification of cryptography-based cyber-attacks could be categorized into eCSIRT's cyber-attacks as follows: Abusive Content, Malicious Code, Intrusion Attempts, Intrusions, Availability, Information Security, and Fraud.
Keywords: State of the Art, Cryptocurrency, Cryptography-Based Cyber-Attacks

Introduction
Cryptography or the art of data protection by encryption from unauthorized persons is one of the oldest human invention at least 1900 B.C. when ancient Egyptian clerks wrote nonstandard hieroglyphs on clay tablets. However, computer-based cryptography started with the development of Lucifer Cipher by Dr. Horst Feistel and his IBM team in 1970. A design on Lucifer became the data encryption standard for US and Worldwide in 1976. After that, the science of encryption like cryptography has been developed by many scholars for increasing easiness and simplicity of crypto-based tools (Whitman and Mattord, 2012; Brooks, Grow, Craig, Short, 2018; Laudon and Laudon, 2019). Unfortunately, many advanced tools have been employed by many cybercriminals at least in 1989 with the appearance of the first known encryption-based malware as data locker ransomware, named the AIDS Trojan. This Trojan horse's real intention was to encrypt sections of the root directory of hard disk in each infected PC (Wilding, 1990; Kaspersky Lab, 2016, 2018). In addition, in 2005, Trojan:W32/Gpcode also emerged as a data locker ransomware (Nazarov and Emelyanova, 2006; Savage, Coogan, Lau, 2015; Symantec, 2015a; Kaspersky Lab, 2016, 2018; F-Secure, 2019). However, these ransomwares were not severe attacks due to their small amount of infected devices. In 2010, the

massive attacks by a computer locker ransomware, another type of ransomware family, locked computers or browsers of thousands of home users' PCs in Russia (Kaspersky Lab, 2016).
Unfortunately, cryptography-based cyber-attacks have become much more complex with the emergence of cryptocurrency in 2009. Cryptocurrency is a very important topic in the cashless society and digital economy era. It directly allows people to do money transfer and business around the globe via blockchain-based technology and advanced technology such as AI and IoT. Data are recorded in blocks which are chained in each specific system. Data consistency are secured by data dissemination and consensus methods such as Proof-of-Work (Pow) and Proof-of-Stack (PoS). Cryptocurrency gets rid of the opportunism problem from middlemen or third party. This is why many people use cryptocurrency like Bitcoin, Ethereum as money, instead of fiat currency. In addition, the appearance of cryptography-based technology in soft digital weapon, malware like ransomware, cryptojacking, and deep webs and dark webs cause a lot of losses for cryptocurrency users since 2011 with the emergence of Trojan.Badminer, a file-based coin miner, that employed Graphics Processing Unit (GPU) for Bitcoin mining (Gohwong, 2015, 2017a, 2017b, 2017c, 2018a, 2018b, 2018c, 2019; Goodman, 2016; Kaspersky Lab, 2016, 2018; Laudon and Laudon, 2019; Symantec, 2010, 2011a, 2012, 2013, 2014, 2015a, 2016a, 2017, 2018a, 2019; Sophos, 2014, 2019). However, there is no systematic study about cryptography-based cyber-attacks. Therefore, this paper objective is to investigate the state of the art of cryptography-based cyber-attacks.

Cyber-attacks

Cyber-attacks are any malicious attempts by cybercriminals, either individual or organization, for getting all sensitive data and/or money from compromised devices and/or systems of victims. (Whitman and Mattord, 2012; Goodman, 2016) In this paper, European Computer Security Incident Response Team Network (eCSIRT)'s taxonomy will be employed for data analysis due to its standardized classifications. The cyber-attacks could be classified into nine groups as follows: Abusive Content (spam, harassment, child/sexual/violence), Malicious Code (virus, worm, trojan, spyware, dialer), Information Gathering (scanning, sniffing, social engineering), Intrusion Attempts (exploiting of known vulnerabilities, login attempts, new attack signature), Intrusions (privileged account compromise, unprivileged account compromise, application compromise), Availability (DoS, DDoS, Sabotage), Information Security (unauthorized access to information, unauthorized modification of information), Fraud (unauthorized use of resources, copyright, masquerade), Other (all attacks beyond the previous groups) (Gohwong, 2016)

Methodology

The duration of the study was during 1989-2019 because the first ransomware appeared in 1989. Documentary research was employed for data analysis in this study. Secondary data from various sources such as Symantec Global Security Threat Reports during 2010-2018 (Symantec, 2010, 2011a, 2012, 2013, 2014, 2015a, 2016a, 2017, 2018a, 2019), KSN Reports during 2014-2018 (Kaspersky Lab, 2016, 2018); SophosLabs Threat Report (Sophos, 2014, 2019) and so on.

Findings

The findings in this paper would be presented into two parts-overall level and categorical level.
First, the overall of findings was that cryptography-based cyber-attacks during 1989-2019 could be defined as any attacks mainly focus on encryption technology-related crimes, classified into four key groups-ransomware, cryptojacking, coin thief, and illegal money transfer. In addition,

dirty fiat currency and dirty cryptocurrency were investigated in these categories as mediums of exchange in cybercrimes. First, ransomware was a profit-driven malware by using cryptography for denying access to the compromised device (such as PC, cell phone) or data in the infected device until the overawed ransom is paid. Next, cryptojacking, by contrast, was another profit-driven malware that designed for stealing its victims' computing resources, or Graphics Processing Unit (GPU) of infected PC or infected computer network, in order to mine cryptocurrency, especially Monero. Then, coin thief was a cybercrime for stealing cryptocurrency, mainly Bitcoin, by using hacking or malware (both as a bit or as a service), Last, illegal money transfer was the service of stolen money transfer with a fee in cryptocurrency (Kaspersky Lab, 2016, 2018; Malanov, 2018; Panda, 2018; Symantec, 2011a, 2011b, 2014, 2016a, 2017, 2018a, 2019; Sophos, 2014, 2019).

In addition, profit and availability were two key incentives for cryptography-based cyber-attackers during 1989-2009 according to Kaspersky and Symantec data. Cybercriminals would change cryptography-based tools and targeted groups or market back and forth due to rise and fall of profit from their attacks. For profit-oriented incentive, cryptojacking, ransomware, coin thief, and illegal money transfer were key cybercrimes. In addition, cybercriminals intentionally lessened availability of their targeted victims' devices with sabotage or vandalism-oriented intentions via malicious tools like Disakil and Petya/NotPetya, two Trojan-oriented disk wipers. (Parkin, 2014; HP, 2018; Kaspersky Lab, 2016, 2018; Panda, 2018; Symantec, 2010, 2011a, 2012, 2013, 2014, 2015a, 2016a, 2017, 2018a, 2019).

Last, the findings in categorical level would be presented into five groups of illegal activities-ransomware, cryptojacking, coin thief, illegal money transfer, and fake identity.

Ransomware

First, ransomware gradually rise year by year since 2013 and reached its peak in 2016 with 1,271 detections per day in 2016 according to Symantec data. Later, in 2017, ransomware was dominated by WannaCry and Petya/NotPetya (which disguised as a ransomware but the real one was a disk-wiper) (Symantec, 2017).

Second, ransomware could be classified in three classifications by three criteria-objective of cyber-attacks, cyber-attacks' techniques, and level of sabotage.

-According to the first classification, ransomware had two main forms as follows: locker ransomware (or windows blocker or computer/mobile Locker or lock screen ransomware) and data locker (or encryption ransomware or file-encrypting ransomware or crypto ransomware). Locker ransomware strictly blocked access to the compromised device (such as PC, cell phone). The examples of locker ransomware were NSA PRISM-Themed Ransomware, FBI-themed ransomware OSX and Android (for locking compromise device), Chinese Ransomlock Malware (that changed Windows Login in Chinese), and Browlock ransomware (a Browser-based locker ransomware that employed JavaScript in order to keep the hijacked browser tab for blocking the victims to access other websites and desktop or use the computer or mobile devices). Data locker, by contrast, strictly blocked access to data or file in the compromised device. Locker ransomware was a profitable source of income for cybercriminals in 2012. However, Data locker replaced locker ransomware in 2015 because the latter one had higher profit and more difficult encryption than the first one. For instance, Trojan.Cryptodefense or Cryptowall as a new crypto-ransonware or data locker ransomware combined cryptocurrency-based-payment ransomware with TOR (when it used its title as Cryptodefense) and I2P (when it employed its title as Cryptowall) for promoting anonymity. Bitcoin and pressure tactics ($500/€500 for normal payment and $1,000/€1,000 for late payment) were used for precipitating payment from victims.

Another instance, CryptoLocker or ransomcrypt is a perfect data locker ransomware due to no solution for it (Barcena, M.B. 2009; Arntz, 2015; European Cybercrime Centre, 2016; Kaspersky, 2009; Kaspersky Lab, 2016, 2018; Liu, 2013; Symantec, 2013, 2014, 2015a, 2015b, 2017; Sophos, 2014, 2019; Mateiu, 2018). In addition, ransomware could elaborate more into five categories as follows: Crypto malware or encryptors, Lockers, Scareware or Fake software, Doxware or Leakware (for threatening the victims by publish their stolen sensitive data online if they did not pay ransom within deadline), Ransomware-as-a-Service (RaaS) (Mateiu, 2018).

-Second classification, ransomware could be classified by cyber-attacks' techniques into three groups as follows: Traditional Ransomware (such as WannaCry or WCry or WanaCryptor), DDoS Ransom Notes, and Data Theft and Extortion via Doxware or extortionware (Tang, C. 2017).

- Last classification, there were three types of ransomware according to level of sabotage-revenue-oriented ransomware, decoy-oriented ransomware, and disruption-oriented ransomware (Symantec, 2017). For example, WannaCry was an example of revenue-oriented ransomware. However, it was just a failure of cyber-attacks in profitability aspect. Its authors did a bad mistake by creating three hardcoded Bitcoin address, instead of one single Bitcoin address. The criminals did not know when and where their victims paid for ransomed files. Therefore, their victims had little motive to pay the ransom. For decoy-oriented ransomware, false appearance as a disk wiper in fake ransomware named Phonywall, a variant of CryptoWall, was a great tricky strategy in order to hide its real intention for data theft with data overwrite, not data encryption as ransomware. It was the same as the employment of DDoS in the past by cyber criminals to hide real intention in intrusion. Another instance of decoy-oriented ransomware, Disakil Trojan (Trojan.Disakil) was false presented as a ransomware by Sandworm, a Russian Sandworm cyber-espionage group which invented a soft digital weapon-BlackEnergy 3. In fact, it was a decoy-oriented ransomware that employed DDoS in order to hide its real illegal activities on the targeted Linux-oriented devices, e.g. disk-wiping. In addition, for disruption-oriented ransomware, Petya/NotPetya was a good example which combined both techniques from revenue-oriented ransomware (here WannaCry) and decoy-oriented ransomware with self-propagation mechanism in order to increase widespread infected devices. In fact, Petya/NotPetya was a disk-wiper because its installation key or private key was generated by cybercriminals before Salsa20 key or public key was made. Therefore, private key did not relate to public key. Badrabbit was a disk-wiper as Petya/NotPetya. However, Petya/NotPetya's target was Ukraine whereas Badrabbit's target was Russia (Malwarebytes Labs, 2017; Symantec, 2017; Șcheau, and Zaharie, 2018).

Third, ransom payment by cryptocurrency was another interesting issue. Payment of ransomware (such as BitPaymer, SamSam, Ryuk, Dharma, GandCrab) was done in Bitcoin via E-mail and/or dark web onion site. However, payment for ransomed files did not assure that the victims would get their decrypted files. According to Symantec's Internet Security Threat Report on April 2017, only 47% of the victims got their files back after payment. An amount of ransomware was mostly paid by Bitcoin. For example, CryptoLocker or ransomcrypt started asking victims to buy its decryption solutions by Bitcoin. According to Symantec analysis, its fee for decryption solution was between 0.5 and 2 Bitcoin (Barcena, M.B. 2009; Symantec, 2013, 2016). Another example, a cybercriminal attacked one Australian E-mail provider by DDoS and asked 20 Bitcoins, or about US$6,600 (Symantec, 2015). Another instance, Payment of ransomware (such as BitPaymer, SamSam, Ryuk, Dharma, GandCrab) was done in Bitcoin via E-mail and/or dark web onion site (Sophos, 2019). Last example, Disakil Trojan, a highly destructive Trojan and

ransomware, encrypted key Linux files, erased discs, and asked a ransom of 222 Bitcoin (approximately US$210,000) in 2016. However, payment was just a trick for keeping its victims from investigating the attacks because the generated encrypted key for encrypted files were not in infected computer and a command and control (C&C) server (Symantec, 2016, 2019; Gohwong 2017; Șcheau and Zaharie, 2018).

Fourth, transmission of ransomware could be infected via many techniques such as fake software (such as fake antivirus, fake Adobe Flash), vulnerability of software (e.g., Trojan.Synolocker or Synolocker, a data locker ransomware, that attacked Synology NAS devices via vulnerability in Synology's DiskStation manager software to access and encrypt all files in any devices), Exploit kits (e.g. Nuclear exploit kit that attacked "Adobe Flash Player Unspecified Remote Code Execution Vulnerability (CVE-2015-7645)" in order to use Trojan.Cryptowall (data locker ransomware) or Trojan.Miuref.B for stealing information), Office documents via Excel and other Office applications with their macros and Common Vulnerabilities and Exposures (CVE), hijacking software update, social media, Skype, Remote Desktop Protocol (RDP), E-mail, and fake warning windows (such as Android.Lockdroid.E with faked FBI warning windows for locking computer) (Symantec, 2012, 2013, 2014, 2015a, 2015b, 2019; mssecurity, 2016).

Fifth, the ransomware business model in 2016 was the combination of strong encryption with hard decryption, Bitcoin payment, and Spam mails. The favorite tactics for fast ransom payment and epidemic of cybercriminals were deadline, user-friendliness with local language, OS-free ransomware. For deadline, some ransomware criminals used deadline as tactics for precipitating payment from victims. For example, the victims who missed the original 72 hour deadline must pay 10 Bitcoin. For local language, languages of Latin America were employed for helping victims in South America to easily understand ransom notes. For OS-free ransomware, ransomware now was free from OS. Before 2014, MS Windows was one and only one target of all ransomware authors. The platform like Windows, Mac, Linux, and Andriod could equally be targets of ransomware. For instance, Android.Lockdroid.G. Internet Explorer (as computer and mobile device locker ransomware) that uses Angler Exploit kit that employed Trojan.Ransomlock.G. and Browlock (for attacking any devices that used MS Windows, Mac, Linux). Another example, Android.Simplocker was the first data locker ransomware for Android in Russia and its latter version was in English (Ladley, and Neville, 2011; Bergen, J. 2013; Symantec, 2013, 2014; Balanza, M.A. 2014; Venkatesan, D. 2015).

Sixth, Internet-based TV and mobile phone were target of ransomware author (Symantec, 2015a).

Seventh, size of organization was the determinants of type of ransomware. For example, BitPaymer, SamSam,and Ryuk were for medium or large organizations whereas Dharma was for small organizations. In addition, GandCrab was for any size (Sophos, 2019).

Cryptojacking

First, cryptojacking had many interchangeable names such as coin mining, coinminer, cryptominer, cryptocurrency mining, and cryptocurrency miner. It employed two techniques-file-based cryptojacking (by downloading and running malicious files on any devices such as computers, servers, and networks) and browser-based cryptojacking or drive-by mining (by embedding malicious code for mining in any compromised Websites) (HP, 2018; Kaspersky lab, 2018; Musch, Wressnegger, Johns, and Rieck, 2018; Panda, 2018; Sophos, 2019; Symantec, 2011a, 2011b, 2014, 2017, 2018a, 2019). For file-based cryptojacking, Trojan.Badminer was found as a file-based coin miner in MS Windows on August 11, 2011 by using GPU of its victims for Bitcoin mining (Jensen, 2011a; Symantec, 2011). In addition, hijacking software

update was another technique of cryptojacking (Symantec, 2017). For browser-based cryptojacking, it was designed for memory-bound cryptocurrencies with CryptoNight algorithm, such as Monero, Bytecoin, and Electroneum. It was created for taking advantage of browser-based JavaScript for running Proof-of-Work (PoW) by reducing total cost of ownership (TCO) of miners on GPU and ASIC mining machine, and pushing high energy consumption of CPU-bound mining of classic cryptocurrencies (e.g. Bitcoin) from miner to website visitors. Mining would be run by JavaScript as long as the visitor still visit the compromised Websites or JavaScript-embedded Websites. CryptoNight was the heart of momory-bound cryptocurrencies by requiring only 2 Megabyte memory region per block/ instance (Saberhagen, 2013; Musch, Wressnegger, Johns, and Rieck, 2018).

Second, browser-based cryptojacking was not new because it had its intellectual root since the emergence of idea about Bitcoin Plus in 2011 for replacing ads by Bitcoin browser miners. After that, there were two unprofitable pioneers of Bitcoin JavaScript miners such as JSMiner in 2011 and MineCrunch in 2014. In 2015, there was Tidbit, a browser-based Bitcoin miner, which was one of the first browser-based cryptominer for legal challenge. The settlement between New Jersey Attorney General's office and Tidbit's developers was that browser-based crypto miners should be done with notification to its user or visitors and rights for doing opt out. In contrast to the first group of cryptojacking, browser-based cryptojacking was much easier than file-based cryptojacking because it did not need high skill in coding for creating an exploit and installing it in the victims' devices. It also made money very well even in full-patched devices (Eskandari, Leoutsarakos, Murschy, and Clark, 2018; Symantec, 2018).

Third, cryptojacking could be discussed in profit-based issues as follows: cryptojacking quickly replaced ransomware in 2017 due to high profit from its easy infection in PCs and/or mobile devices, its stealthiness, increase of cryptocurrency value, low cost of malicious coding for stealing computing processing power and cloud CPU usage of its victims. Cryptojacking was advantageous for sustainable/long-term gain in Bitcoin, Monero, and zcash in contrast to ransomware, which was suitable for making easy money for short-term. In addition, cryptojacking employed Monero (XMR) due to its high value and its stealthiness, instead of Bitcoin (BTC). Furthermore, not only PCs, mobile devices was also infected with cryptocurrency coin-mining malware via an amount of fake apps for mining Monero, not Bitcoin. Tools for Monero-based mining were Desktop Mining Malware (i.e. "Linux.Darlloz", an Internet of Things (IoT) worm, was found on November 26, 2013 for mining cryptocurrencies, especially Mincoins and Dogecoins, "Trojan.Coinliteminer" for mining litecoins, "Trojan.Coinbitminer" for mining Bitcoins, "SONAR.Coinbitminer!g1"-a Trojan for mining Bitcoin, "PUA.WASMcoinminer"-a virus that used JavaScript for mining cryptocurrency, "PUA.Gyplyraminer or Miner.Gyplyra"-a Trojan for mining cryptocurrency, "PUA.Bitcoinminer or Miner.Bitcoinminer"-a Trojan for mining Bitcoin, "OSX.Coinbitminer or OSX/Miner-D or Backdoor:OSX/DevilRobber.A"-a Trojan for mining Bitcoin, "Taskhostw.exe Miner"-a Trojan for mining Monero, and "JS.Webcoinminer or Miner.Jswebcoin or Trojan.JS.Miner.m"-the most frequently detected Trojan that used JavaScript for mining cryptocurrency in 2017 according to Symantec data), Mining Pools (such as WannaMine or BLUWIMPS), Remote Code Execution (RCE) Vulnerabilities /Common Vulnerabilities and Exposures (CVE), Coinhive Websites. After that, cryptojacking growth clearly decreased due to the fall of Monero's value in 2018. However, the fall of cryptojacking and Monero were not in the same rate-cryptojacking with a drop of 52% whereas Monero with a drop of 90%. The consequence of the decline of Monero's value and cryptojacking was that formjacking appeared

as a new cyber-attacks by using malicious JaveScript in Website for stealing credit cards details and other financial information (Jensen, 2011b; Morparia, 2011; Xiao, 2013; Parkin, 2014; James, 2016; Kaspersky lab, 2018; Accenture Security 2018; Balanza, 2018; Gelera, 2018; Gohwong, 2018a; NTTSecurity, 2018; Șcheau, and Zaharie, 2018; Symantec, 2016b, 2017, 2018a, 2018b, 2018c, 2019; Varsanov, 2018; Acronis International GmbH. 2019; Khatri, 2019).
Fourth, cryptojacking-based code, embedded in games, apps, Websites for cell phone in order to continuously employ compromised cell phones' processors for mining, directly caused the shortage of batteries' life of infected cell phones (Symantec, 2019).
Fifth, Beapy was a file-based crypto miner by sending an attached malicious Excel file, which would download DoublePulsar backdoor on its victim's device after the file was opened (Khatri, 2019).

Coin thief

Coin thief was conducted by malware and Crimeware-as-a-Service (CaaS). Two examples of malware for coin thief were OSX.Stealbit.A and OSX.Stealbit.B. They both were two designed Trojan horses for opening backdoors and stealing Bitcoin by getting the victim's login credentials to major Bitcoin websites. For CaaS, comprised Exploits-as-a-Service (EaaS), Denial of Service (DoS) as a Service (DaaS), Ransomware-as-a-Service (RaaS) such as GandCrab, and Cryptojacking-as-a-Service (CaaS). Cybercriminals could buy not only CaaS but also malware, Exploit kits, and vulnerability information in black market. For example, custom malware for payment diversion and Bitcoin Stealing costed between $12 and $3500 in 2014. Next, in 2016, ransomware toolkits was sold between $10 and $1800 in 2016. Another instance, Shadow Brokers claimed that they had NSA's hacking tools and offered for sale about 1 million Bitcoin (Symantec, 2014, 2015a, 2016; Itabashi, 2014; MAYASEVEN Team, 2016; Șcheau, and Zaharie, 2018; Sophos, 2018; Acronis International GmbH, 2019; Avertium. 2019).

Illegal money transfer

Money transfer services for the stolen money in 2018 was priced the same rate as 2016 at 10 percent of total amount of money. For instance, $100 in Bitcoins for cashing out $1,000 (Symantec2017, 2019). In addition, Bytecoin, Verge, Zcash, Zcoin, Monero, MoneroC, Monero Gold, MoneroV, Monero Classic, Monero-Classic, Monero 0, Monero Original were examples of privacy-based cryptocurrency for money laundering (Gohwong, 2018a, 2018b).

Fake identity

Fraudulent certificates for Google, Mozilla add-on, Microsoft Update and others were issued by hacked DigiNotar, a famous SSL provider in Netherland (Symantec, 2012).

Discussion

According to the above findings, all illegal activities-based classification of cryptography-based cyber-attacks could be categorized into eCSIRT's cyber-attacks in order to see a big picture of cryptography in the standardized classification of cyber-attacks as follows: Abusive Content-harassment (e.g. Doxware or Leakware); Malicious Code or Malware-Virus (e.g. PUA.WASMcoinminer), Worm (e.g. WannaCry), Trojan (e.g. Petya/NotPetya); Intrusion Attempts-Exploiting of known Vulnerabilities (e.g. Adobe Flash Player Unspecified Remote Code Execution Vulnerability (CVE-2015-7645), Angler Exploit kit); Intrusions-Privileged Account Compromise and Unprivileged Account Compromise (e.g. Fraudulent certificates for Google, Mozilla add-on, Microsoft Update and others from hacked DigiNotar; A compromised bitcoin exchange service from hacking), Application Compromise (e.g. hijacking software update, Trojan.Synolocker or Synolocker; Chinese Ransomlock Malware); Availability-DDoS

and Sabotage (e.g. Phonywall, Disakil Trojan, Petya/NotPetya, and Badrabbit); Information Security-Unauthorized access to information (e.g. OSX.Stealbit.A and OSX.Stealbit.B that stole Bitcoin by getting the victim's login credentials), Unauthorized modification of information (e.g. CryptoLocker or ransomcrypt); and Fraud-Unauthorized use of resources (e.g. "JS.Webcoinminer", "Trojan.Coinliteminer", "Miner.Gyplyra", "Trojan.Coinbitminer", and "Taskhostw.exe Miner"), Copyright (e.g. selling NSA's hacking tools at 1 million Bitcoin by Shadow Brokers), and Masquerade (e.g. NSA PRISM-Themed Ransomware, FBI-themed ransomware OSX and Android, OSX.Stealbit.A and OSX.Stealbit.B).

Conclusion

This paper objective was to investigate the state of the art of crypto-based cyber-attacks during 1989-2019 by using documentary research for data analysis. The findings found that five key illegal activities of cryptography-based cyber-attacks during 1989-2019 were ransomware, cryptojacking, coin thief, illegal money transfer, and fake identity. In addition, this illegal activities-based classification of cryptography-based cyber-attacks could be classified into eCSIRT's cyber-attacks as follows: Abusive Content, Malicious Code, Intrusion Attempts, Intrusions, Availability, Information Security, and Fraud.

References

Accenture Security. 2018. **MONERO AND WANNAMINE: The cyber-criminal cryptocurrency and miner malware of choice**. Retrieved from www.accenture.com/_acnmedia/PDF-46/Accenture-Threat-Analysis-Monero-Wannamine.pdf**.**

Acronis International GmbH. 2019. **The growing two-headed threat: cryptojackers paired with ransomware**. Retrieved from www.acronis.com/en-us/articles/cryptojacking/.

Arntz, P. 2015. **Regaining Control Over Edge**. Retrieved from blog.malwarebytes.com/cyber crime/2015/09/regaining-control-over-edge/.

Avertium. 2019. **Crimeware-as-a-Service Explained**. Retrieved From www.avertium.com/ crimeware-as-a-service-explained/.

Balanza, M. 2014. **Android.Lockdroid.G.** Retrieved from www.symantec.com/security-center/ writeup/2014-050610-2450-99.

Balanza, M. 2018. **Miner.Jswebcoin**. Retrieved from www.symantec.com/security-center/ writeup/2017-091515-5134-99.

Barcena, M. 2009. **Trojan.Ransomcrypt**. Retrieved from www.symantec.com/security-center/ |writeup/2009-060912-0056-99.

Bergen, J. 2013. **Watch out, Mac OS X users! FBI ransomware is coming for you, too**. Retrieved from www.digitaltrends.com/computing/watch-out-mac- users-ransomwares-coming-for-you-too/.

Brooks, C., Grow, C., Craig, P., & Short, D. 2018. **Cybersecurity Essentials**. New York: John Wiley and Sons.

Eskandari, S., Leoutsarakos, A., Murschy, T., & Clark, J. 2018. **A first look at browser-based cryptojacking**. Retrieved from www.researchgate.net/publication/323654794_A_First_Look_at_Browser-Based_Cryptojacking/download**.**

European Cybercrime Centre. 2016. **Ransomware: What You Need to Know**. Retrieved from www.europol.europa.eu/sites/default/files/documents/ransomware-what_you_need_to_know.pdf.

F-Secure. 2019. **Trojan:W32/Gpcode**. Retrieved from www.f-secure.com/v-descs/gpcode.shtml.

Gelera, B. 2018. **COINMINER_WEBXMR.B-JS**. Retrieved from www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/coinminer_webxmr.b-js.

Gohwong, S. 2016. **The Cyber-attacks and digital economy in Thailand during 2012-2016**. (A paper presented at the 1st International Conference, Hong Kong, 25-27 August 2016).

Gohwong, S. 2017. **Soft Digital Weapons as Predator Insects**. (A paper presented at the 4th International Conference on Security Studies, Bangkok, Thailand, 20 July 2017).

Gohwong, S. 2018a. **The State of the Art of Privacy-oriented Cryptocurrencies**. (A paper presented at the 5th International Social Sciences and Business Research Conference, Lugano, Switzerland, 30 May 2018).

Gohwong, S. 2018b. "The State of the Art of Cryptocurrencies." **Asian Administration and Management Review** 1 (2): 1-16.

Goodman, M. 2016. **Future Crimes: Inside the digital underground and the battle for our connected world**. London: Transworld Publishers.

HP. 2018. **An IT Manager's Guide: Cryptojacking, the Threat to Business and How to Protect the Network**. Retrieved from www8.hp.com/h20195/v2/GetPDF.aspx/4AA7-3873ENW.pdf**.**

Itabashi, K. 2014. **OSX.Stealbit.A**. Retrieved from www.symantec.com/security-center/writeup/2014-022613-0002-99.

James. M. 2016. **Quick Guide to Remove PUA.Gyplyraminer | (Malware Removal Step)**. Retrieved from www.repairtrojans.com/quick-guide-to-remove-pua-gyplyraminer-malware-removal-step/.

Jensen, P. 2011a. **Bitcoin Mining with Trojan.Badminer**. Retrieved from www.symantec.com/connect/blogs/bitcoin-mining-trojanbadminer.

Jensen, P. 2011b. **Trojan.Coinbitminer**. Retrieved from www.symantec.com/security-center/writeup/2011-072002-1302-99.

Kaspersky. 2009. **Cryptolocker Virus Definition**. Retrieved from usa.kaspersky.com/resource-center/definitions/cryptolocker.

Kaspersky lab. 2016. **KSN Report: Ransomware in 2014-2016**. Retrieved from media.kasperskycontenthub.com/wpcontent/uploads/sites/43/2018/03/07190822/KSN_Report_Ransomware_2014-2016_final_ENG.pdf.

Kaspersky lab. 2018. **KSN Report: Ransomware in 2016-2018**. Retrieved from media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/06/27125925/KSN-report_Ransomware-and-malicious-cryptominers_2016-2018_ENG.pdf.

Kevin Savage, K., Coogan, P., & Lau, H. 2015.**The Evolution of Ransomware**. Retrieved from www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf.

Khatri, Y. 2019. **New Crypto-Mining Malware Targeting Asian Firms with NSA Tools**. Retrieved from www.coindesk.com/new-crypto-mining-malware-targeting-asian-firms-with-nsa-tools?fbclid=IwAR2BUxD2oE5qUC4r3TA5WfMz7x7JVOkopdEPdS8a9kcODR8Ja_CG2OQtV3E.

Ladley, F. and Neville, A. 2011. **Trojan.Ransomlock.G**. Retrieved from www.symantec.com/security-center/writeup/2011-051715-1513-99.

Laudon, K. and Laudon, J. 2019. **Essentials of MIS**. Harlow: Pearson Education.

Liu, F. 2013. **Chinese Ransomlock Malware Changes Windows Login Credentials**. Retrieved from www.symantec.com/connect/blogs/chinese-ransomlock-malware-changes-windows-login-credentials.

Malanov, A. 2018. **Cryptocurrency threat predictions for 2019**. Retrieved from securelist.com/ksb-threat-predictions-for-cryptocurrencies-in-2019/88942/.

Malwarebytes Labs. 2017. **EternalPetya and the lost Salsa20 key**. Retrieved from blog.malwarebytes.com/threat-analysis/2017/06/eternalpetya-lost-salsa20-key/.

Mateiu, M. 2018. **The Ultimate Guide to Ransomware**. Retrieved from www.avg.com/en/signal/what-is-ransomware?fbclid=IwAR2BUxD2oE5qUC4r3TA5WfMz7x7JVOkopdEPdS8a9kcODR8Ja_CG2OQtV3E.

MAYASEVEN Team. 2017. **Summary of the vulnerability attack code hacked from NSA and clip about using Fuzzbunch with meterpreter**. Retrieved from mayaseven.com/exploits-nsa-fuzzbunch-meterpreter/.

mssecurity. 2016. **Hacks for sale: Exploit kits provide easy avenue for unskilled attackers**. Retrieved from www.microsoft.com/security/blog/2016/09/19/hacks-for-sale-exploit-kits-provide-easy-avenue-for-unskilled-attackers/**.**

Morparia, J. 2011. **OSX.Coinbitminer**. Retrieved from www.symantec.com/en/uk/security-center/writeup/2011-110201-3434-99.

Musch, M., Wressnegger, C., Johns, M., and Rieck, K. 2018. **Web-based Cryptojacking in the Wild**. Retrieved from www.sec.cs.tu-bs.de/pubs/2018-cryptojacking.pdf.

Nazarov, D. and Emelyanova, D. 2006. **Blackmailer: the story of Gpcode**. Retrieved from securelist.com/blackmailer-the-story-of-gpcode/36089/.

NTTSecurity. 2018. **Monero Mining Malware: Hunting Down the Miners**. Retrieved from www.nttsecurity.com/docs/librariesprovider3/resources/gbl_gtic-monero-mining-malware_uea.pdf?fbclid=IwAR0-WzhkUhlvGy9n9KDrSZq7P2G8MuKcspoE-YOhbSNVePTZHzZOPyIY5yk.

Panda. 2018. **Cryptojacking: A hidden cost**. Retrieved from www.pandasecurity.com/mediacenter/src/uploads/2018/10/Whitepaper-cryptojacking_EN.pdf.

Parkin, M. 2014. **Economics**. Essex: Pearson Education Limited.

Saberhagen, N. 2013. **CryptoNote v 2.0**. Retrieved from cryptonote.org/whitepaper.pdf.

Șcheau, M. and Zaharie, P. 2018. **The Way of Cryptocurrency**. Retrieved from www.economyinformatics.ase.ro/content/EN18/04%20-%20scheau,%20zaharie.pdf.

Sophos. 2014. **Security Threat Report 2014: Smarter, Shadier, Stealthier Malware**. Retrieved from www.sophos.com/en-us/en-%20us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf.

Sophos. 2018. **OSX/StealBit-A**. Retrieved from www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/OSX~StealBit-A/detailed-analysis.aspx.

Sophos. 2019. **SOPHOSLABS 2019 THREAT REPORT**. Retrieved from www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophoslabs-2019-threat-report.pdf.

Symantec. 2010. **Symantec Global Internet Security Threat Report: Trends for 2009**. Retrieved from eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf.

Symantec. 2011a. **Symantec Internet Security Threat Report Trends for 2010**. Retrieved from www.symantec.com/connect/sites/default/files/21182883_GA_REPORT_ISTR_Main-Report_04-11_HI-RES.pdf.

Symantec. 2011b. **Trojan.Badminer**. Retrieved from www.symantec.com/security-center/writeup/2011-081115-5847-99.

Symantec. 2012. **Symantec Internet Security Threat Report: 2011 Trends**. Retrieved from www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf.

Symantec. 2013. **Symantec Internet Security Threat Report: 2012 Trends**. Retrieved from www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf.

Symantec. 2014. **Symantec Internet Security Threat Report: 2013 Trends**. Retrieved from www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

Symantec. 2015a. **Symantec Internet Security Threat Report**. Retrieved from www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf.

Symantec. 2015b. Android.Lockdroid.E. Retrieved from www.symantec.com/security-center/writeup/2014-103005-2209-99.

Symantec. 2016. **Symantec Internet Security Threat Report**. Retrieved from www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

Symantec Security Response. 2016. **Destructive Disakil malware linked to Ukraine power outages also used against media organizations**. Retrieved from www.symantec.com/connect/blogs/destructive-disakil-malware-linked-ukraine-power-outages-also-used-against-media-organizations**.**

Symantec. 2017. **Symantec Internet Security Threat Report**. Retrieved from www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf.

Symantec. 2018a. **Symantec Internet Security Threat Report**. Retrieved from www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf.

Symantec. 2018b. **Miner.Gyplyra**. Retrieved from www.symantec.com/security-center/writeup/2016-062412-0035-99.

Symantec. 2018c. **Miner.Bitcoinminer**. Retrieved from www.symantec.com/security-center/writeup/2011-091213-5424-99.

Symantec. 2019. **Symantec Internet Security Threat Report**. Retrieved from www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf.

Tang, C. 2017. **Are All Ransom Attacks Considered Ransomware?**. Retrieved from www.imperva.com/blog/are-all-ransom-attacks-considered-ransomware/?fbclid=IwAR3siMqlVPdSFmCfp6tHLQghgzT0kQnL_dMaZYcxrAu1A8vyLW_4jptXzys

Varsanov, E. 2018. **PUA.Wasmcoinminer "Virus" Removal**. Retrieved from www.virusresearch.org/pua-wasmcoinminer-virus-removal/.

Venkatesan, D. 2015. **Android ransomware uses Material Design to scare users into paying ransom**. Retrieved from www.symantec.com/connect/blogs/android-ransomware-uses-material-design-scare-users-paying-ransom**.**

Wilding, E. 1990. **Editorial: AIDS Information Version 2.0**. Retrieved from www.virusbulletin.com/uploads/pdf/magazine/1990/199001.pdf.

Whitman, M. and Mattord, H. 2012. **Principles of Information Security**. China: Course Technology.

Xiao, K. 2013. **Trojan.Coinliteminer**. Retrieved from www.symantec.com/security-center/writeup/2013-061003-2414-99.