Challenges of Cryptocurrencies Forensics – A Case Study of Investigating, Evidencing and Prosecuting Organised Cybercriminals

S. Naqvi
School of Computing & Digital Technology, Birmingham City University, United Kingdom
Syed.Naqvi@bcu.ac.uk

ABSTRACT

This article presents policing challenges of investigating, evidencing and prosecuting organized cybercriminals for the crimes committed using cryptocurrencies such as Bitcoin. A set of best practices is discussed to tackle these challenges in real world investigations. This work is a result of collaboration with a number of stakeholders the policing and judicial ecosystem with the objective of investigating and prosecuting the new generation of organised cybercriminals. Concrete scenarios of using Bitcoins in a range of cybercrimes were developed as part of this project and the devices were analysed to extract evidence to assist prosecution of organised cybercriminals. We have also presented our return of experience for various stages of digital forensics analysis of devices used in Bitcoin transactions.

KEYWORDS

Cryptocurrencies, cybercriminals, digital forensics, law enforcement, organized crime.

1 INTRODUCTION

Cryptocurrencies [1] such as Bitcoins [2] were designed to facilitate global purchases without any central control nor any need to disclose personal information [3]. Although transactions are recorded in Blockchain [4] and their integrity could also be verified. However, details of sender and receiver could not be extracted if 'private key' is not known to the investigators.

This idea of unregulated universal currency has a number of fiscal challenges notably the volatility of its value [5]. However, from the policing point of view, these currencies have become the premier choice of the cybercriminals who can misuse the anonymity provided by these currencies for the transactions to support their underworld businesses [6]. A number of high-profile Ransomware and Terrorist attacks have found trail of cryptocurrencies [7-8]. These are very sensitive cases where victims are scary of their public image, business interests, etc. [9-10]. This situation is exploited by the criminals and the use of cryptocurrencies provides them ideal shelter behind the intrinsic anonymity of these currencies [11-14].

In the rest of this article, we first present the problem statement of this work in Section 2. In Section 3, we present a range of digital forensic analysis challenges of investigating crimes where Bitcoins are used. This work is a part of collaborative project with the other stakeholders including law enforcement and prosecution service. A number of scenarios are built to reflect real-life situations where organised cybercriminals take advantage of the virtual world to operate without leaving *easy of find* traces. These scenario are part of the case study presented in the Section 4 where we also present our return of experience for conducting digital forensic analysis and best practices to get through its various challenges. A pragmatic discussion is made in the Section 5 on the holistic view of Cyber investigations of Bitcoins in the light of our experience in this project. Finally some conclusions are drawn in the Section 6 together with the perspectives and future directions of this work.

2 PROBLEM STATEMENT

The major problem faced by a number of businesses nowadays is to maintain their image of a 'trustworthy enterprise' that is capable of protecting its assets and can be considered by its partners and customers as reliable entity [15]. Therefore, even if an organization is attacked by Cybercriminals, the first priority of the management is to ensure that the security breach is not made public. In the case of Ransomware, they are even reluctant to inform the law-enforcement and prefer to pay hefty amount to the Cybercriminals to ensure that their public image is not distorted. The same situation happens in other cases such as sextortion [16]. This situation goes in favour of the Cybercriminals as they not only gain illicit money but their trade becomes more and more durable over the time that provide them the opportunity to even expand their activities. This is a very challenging situation for the law enforcement and they are now supporting research in the area of Cryptocurrencies forensics to get operational solutions for the investigations, evidencing and prosecuting organized cybercriminals; and therefore give confidence to the public in general and their victims in particular.

3 CRYPTOCURRENCIES FROM THE POLICING POINT OF VIEW

Cryptography is designed to protect information from the malicious entities. The same technique could be used by the malicious entities to protect their activities from the eyes of law enforcement. Policing of encrypted information and communication is always challenging especially when some robust encryption is used. A robust encryption may not be hard to break but it is time and resource consuming that not only drains considerable amount of the available resources of the law enforcement but also provides criminals sufficient time to escape. This is a major reason for regulating information and communication products that use encryption by a number of countries to ensure their law enforcement agencies have vital access to potential criminal activities. An example is the concern of several governments that encryption technology used by BlackBerry to ensure secure communications with its devices makes it difficult to monitor them. However, this case was comparatively much simpler than cryptocurrencies as governments could negotiate with a tangible entity – BlackBerry Limited (former Research in Motion) to gain access to their encryption keys by offering them the carrot of operating in their countries [17]. There is no similar central figure in the case of cryptocurrencies that could be reached out by the governments with a carrot and stick.

The core design of these currencies such as Bitcoin is to liberate them from the regulatory authorities to ensure speedy and hassle-free transactions in real-time. So there is no controller of these transactions who could be asked to cooperate with the law enforcement agencies to entertain request for access to transactions data. This situation implies that the only viable solution for policing cryptocurrencies is to use technical solutions to monitor their transactions. The challenges include decryption techniques and ultra-high efficiency to match the speed of the peer-to-peer transactions. Moreover, the scale of these transactions due to increasing popularity of these currencies [18] is another challenge for the policing of cryptocurrencies.

On the reactive side of investigations, law enforcement can use the similar technique as Cloud forensics, where it is almost impossible in most of the cases to have access to Cloud resources, the investigators analyse terminal devices to gain access to user data on the Cloud. However, it is not very straight forward comparison as most of the Cloud terminal devices have local folders that synchronise their contents with the Cloud to provide a better user experience independent of any connectivity issue. Device(s) use by Bitcoin user contain Wallet which is in reality a folder and with the user private key, investigators can have access to the transaction details. But unlike Cloud terminal devices could be imaged even if their user are not cooperating; whereas, access to Bitcoin's user private key is essential for decoding the transaction details. Moreover, there are very limited option on the proactive side of investigations, as intelligence may have considerable number of false positives and false negatives that will also put pressure on the law enforcement resources due to higher number of false positives; and there will be the risk of criminals evading scrutiny due to higher number of false negatives.

4 CASE STUDY

We have used a number of real life scenarios to observe the peculiar challenges of investigating, evidencing and prosecuting organised cybercriminals. These scenarios covered a range of cybercrimes such as sextortion and dark web purchases. Research considerations for these scenarios were harmonised to work on the common challenges. These scenarios are executed in the real-life by using Bitcoins. The devices involved in these scenarios are analysed to solve the jigsaw puzzle of investigations.

We have summarised these scenarios in this section and some details of the digital forensic investigations are presented together with the challenges and best practices developed to get through them.

4.1 Sample Scenarios

One of the scenarios for this work is about the use of Bitcoins in a sextortion case. In this scenario, the victim met a member of cybercriminal gangs on a dating website. Their initial exchanges were on the messaging service of that website and after some time they started communicating via Skype. After building-up further confidence, the exploiter managed to get some intimate pictures and videos of his victim. He then asked his victim to give him some money as he is having financial troubles and because his bank account is blocked due to overspending, it should be given to him as Bitcoins. With the passage of time, these requests became blackmailing tool – sextortion. Finally the victim decided to contact the law enforcement to end her ordeal with the obvious risk that her pictures and videos could be published online.

In this scenario, the law enforcement has one cooperating party – the victim, whose electronic devices could be analysed for further details and passwords could be shared with the investigators. The analysts got the name of the dating site and consequently it's hosting information. They also get other information such as Skype id and email address of the cybercriminal. These information could be used to identify the IP address from where the person is usually connected. Moreover, she has provided access to her Bitcoin Wallet and the BTC address of the cybercriminals where the Bitcoins were sent. This helped in resolving the provenance issues of Bitcoin forensics.

In a more complicated scenario, a law enforcement may not have a cooperating party who can provide some key information to lead investigations. We consider a scenario where law enforcement receives intelligence about a person who is allegedly producing counterfeit payment cards. Due to the high credibility of this intelligence report, a warrant is executed at the suspect's home address and a number of devices are seized including an embossing machine, a card reader, and several counterfeit payment cards. From the preliminary inquiry, the investigators discovered that Bitcoins are used in this trade. The criminal gang is using Dark Web to purchase equipment and raw material using Bitcoins. The prices of counterfeit cards are also charged in Bitcoins.

What makes this scenario complicated is that first of all, the detection phase requires rigorous monitoring of the cyberspace which is resource-intensive and time consuming. Moreover, it has considerable ethical issues to be considered. Another possibility is

that law enforcement is alerted when some relevant information is discovered during another investigation of similar or different nature. In these circumstances, the pace of investigations is greatly affected by the level of cooperation from the suspected criminals.

4.2 Digital Forensic Analysis

We have applied industry standard digital forensic methodologies in analysing a range of devices used in these scenarios by using state of the art technologies.

We used more classical investigation approach for the first scenario (sextortion) and obtained the following information from the victim's devices:

1. Details of the **dating website** where the victim met the criminal.
2. **Skype username** and **email address** of the criminal.
3. **Bitcoin Address** of the criminal that he gave his victim for sending him Bitcoins
4. **Bitcoin Wallet** signed up by the victim.

Address of the criminal could be traced through law enforcement's request for data to the service providers. Some of the operational challenges of accessing this data and extracting criminal's address are summarised in the following subsection together with the best practice employed to get through these constraints.

Access to the criminal's Bitcoin address is also possible when he is arrested as this information was obtained during the investigation. This information also provides details of the places where the Bitcoins are used. These could be cascading activities that can lead to further information about the gang's activities.

For the second scenario, the role of the digital forensic analysis is more crucial as almost every information needs to be extracted from the confiscated devices. Evidently, the seizure of embossing machine, blank cards and a card reader provides credible hint. But they don't constitute a smoking gun for prosecuting the arrested person. The first preference of a digital forensic analyst is to find **Bitcoin Wallet** that is used to pay for the dark web shopping. Access to further details of the Bitcoins will depend on the access to this Bitcoin Wallet. If the arrested person is cooperating then a considerable manual work could be avoided otherwise, this is a very hectic investigation.

In this scenario, the criminal used **TOR Proxy Browser** and always used **Public WiFi** in coffee shops for the Internet access. Moreover, the laptop was purchased by cash. He also purchased the Bitcoins in cash at a Bitcoin ATM in the City Centre. This shows the highest level of protective measures these criminals use to cause enormous delays in investigations even if they are flagged by the law enforcement agencies. We describe the operational challenges of recovering this information in the following subsection together with some best practices employed in this investigations.

4.3 Challenges and Best Practices

The very first challenge of digital forensic analysis is to ensure access to the entire dataset including those segments that are stored online. If the service hosting company is not based locally then it is difficult for the law enforcement agencies to get requested access to data even if the company is based in a country signatory of some mutual cooperation agreement for the exchange of criminal data. Moreover, a company may not be based in UK even if it has a website in the .co.uk domain. Its hosting servers could be based in another country and applications (and their data) could be owned by a different company in a different country.

We had to deal with this situation in the first scenario of this project where the dating website was outside UK and would not comply with a request for data by a UK law enforcement agency. Therefore, we had to extract data from other sources notably email and Skype. Criminals are aware that their activities will be investigated one day and therefore they are using more and more sophisticated anti-forensic techniques such as the criminal in this scenario used a VPN (Virtual Private Network) connection so as to hide his location even if his connection IP address is shared by the email service provider with a law enforcement. Moreover, he chose a VPN provider that didn't retain logs.

In this scenario, the goldmine was the IP address from where the Skype account was registered. This real IP address resolved to its account holder whose address was identified to execute a police warrant. This also helped recover access to the criminal's Bitcoin account and provided an insight into how he spent these Bitcoins for further investigations.

The second scenario required more intensive digital forensic analysis to find sound evidence for prosecution. Windows Registry analysis was needed to unveil web search history as well as temporary internet files. However, the starting point was to find Bitcoin wallet folder. A Bitcoin wallet is created with a randomly generated address. This Bitcoin address is encoded by using a specific scheme called Base58Check [19]. This scheme uses numbers and alphabets (both upper and lowercase) except 0 (zero), O (uppercase o), I (uppercase i), and l (lowercase L). So the sum of 26 uppercase letters, 26 lowercase letters, and 10 digits is 62. When these 4 exceptions are deducted, the result is 58. Rosetta code [20] repository provides Bitcoin address validation script in python that implements Base58Check scheme. BTCscan [21] has implemented this code. This Python script requires raw forensic image of a device in .dd format. This has to be considered if instead of drives, only .E01 image files are provided for analysis.

BTCscan is a simple, efficient and very useful tool for analysing Bitcoin activities. It allocates a memory cache for loading the image file. This makes the program execution efficient; however, it can also be a bottleneck if a large hard drive is analysed. It only works on the image file. Therefore, we cannot use it directly on a hard drive connected via write-blocker. There are plenty of possibilities that could be explored to get through these shortcomings of BTCscan to breakup large image's .dd files into smaller sections, but it could be time consuming and tedious. In other words, for smaller drives, BTCscan remain the most powerful tool for the extraction of Bitcoin artefacts.

Bitcoins purchased from ATM machines may also provide considerable information about the buyer if their devices are made available for analysis.

5 DISCUSSIONS

Cryptocurrencies forensics require close cooperation between digital forensic analysts and members of different organizations in the policing and judicial ecosystem to successfully investigate and prosecute organised cybercriminals. Criminals take advantage of the user-friendly nature of cryptocurrencies; whereas, the technical complexity of investigating crimes involving these cryptocurrencies and resulting delays provide enough space to the criminals to change their cyber hideouts. Moreover, these delays threaten the victims with reputation damages that exacerbate the situation to the extent where they may prefer to pay ransom, remain silent, and even withdraw their complains to the law enforcement and refuse to cooperate with the prosecution. All of these eventualities go in the favour of organised cybercriminals and encourage their business model. Sharp rise of cybercrimes such as ransomware shows the advantageous position of cybercriminals [22].

There are some misconceptions about the nature of these attacks and the preliminary steps to be taken when a cybercriminal is asking for ransom in cryptocurrencies. One of such misconception is that cybercriminals create an encrypted container where the files are moved and then the container is locked and files from their original location are deleted. These deleted files should be retrievable by using any of the digital forensic data recovery tool such as EnCase or FTK. This situation delays the investigation cycle as analysts are tasked to create forensic image of the victim's hard drive and use some digital forensic tool to recover the original files. These assumptions could be true in the early days of ransomware with CryptoLocker [23] where even rebooting a Windows PC is safe mode could help recover the files. However, during the last couple of years, attackers have considerably improved their methods. Now they can even exploit security vulnerabilities to take over their victim's computer instead of relying on phishing spams or social engineering techniques to gain admin access to their target computers. Moreover, they no longer delete/move any file. They are simply able to encrypt files thanks to their admin access on their victim's computer.

There are often incidents where victims never get back their files even after paying the ransom [24]. They can provide details of the transaction to the law enforcement for further investigation. However, if they preferred to avoid contacting law enforcement in the first instant, there are the chances that they will remain reluctant even when the attackers don't honour their commitment to provide them access key to their files when ransom is paid.

Quantum computing [25] is emerging as powerful contender to decrypt cryptocurrencies with their ultra-high computing power; however, we need to develop some powerful (and perhaps power hungry) algorithm(s) that can be used by these computers to decrypt these currencies in reasonable time.

6 CONCLUSIONS AND PERSPECTIVES

The use of digital forensics in the lifecycle of organised cybercrimes is very challenging as the investigators have to not only confront with the resourceful gangs of cybercriminals but also to cope with the core technical issues of the cryptocurrencies which at the moment go in the favour of cybercriminals. We have closely worked with the stakeholders of the investigation lifecycle to develop best practices to tackle the challenges of investigating, evidencing and prosecuting organised cybercriminals. We have used both commercial industry standard tools for the acquisition and analysis of hard drives and also open source scripts to address specific issues of investigations. Our work was based on Bitcoins. Our approach may need adaptation if some other cryptocurrency is used by the cybercriminals. We have found that digital forensic analysis of machines infected by ransomware attacks is comparatively easier than digital forensic analysis of Cloud based storage from the point of view of having the opportunity to access resources. However, more powerful decryption algorithms and computing power is needed to execute them.

This is a relatively new area and therefore has a lot of opportunities besides a range of challenges. The ever increasing computing power of the analysis tools is a good news. However, more rigorous research is also needed in the development of new algorithms to decrypt provenance of cryptocurrencies and other parameters. It will be challenging for the governments to bring legislations to regulate the use of cryptocurrencies. However, some global mechanism to monitor the flow of cryptocurrencies, similar to SWIFT [26] in regular banking transactions will not only help monitoring the flow of capital across borders but also provide useful information to the law enforcement for investigations.

ACKNOWLEDGMENTS

This work is partially supported by the Higher Education Funding Council for England (HEFCE) through their Catalyst Grant for N8 Policing Research Partnership Project.

REFERENCES

[1] Wikipedia definition of Cryptocurrencies – https://en.wikipedia.org/wiki/Cryptocurrency

[2] The Bitcoin Project – https://www.bitcoin.com

[3] I. Alqassem, D. Svetinovic, Towards Reference Architecture for Cryptocurrencies: Bitcoin Architectural Analysis, 2014 IEEE International Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom), 2014

[4] F. Dai, Y. Shi, N. Meng, L. Wei, Z. Ye, From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues 2017 4th International Conference on Systems and Informatics (ICSAI), 2017

[5] J. Adkisson, Why Bitcoin Is So Volatile, Forbes Magazine, 9th February 2018 https://www.forbes.com/consent/?toURL=https://www.forbes.com/sites/jayadkisson/2018/02/09/why-bitcoin-is-so-volatile/

[6] C. Janze, Are Cryptocurrencies Criminals Best Friends? Examining the Co-Evolution of Bitcoin and Darknet Markets, Proceedings of the Americas Conference on Information Systems (AMCIS), 2017

[7] Why Cyber-Attackers are Using Bitcoin, RHEA Group Report, 10 July 2017 https://www.rheagroup.com/fr/news/why-cyber-attackers-are-using-bitcoin

[8] S. Gibbs, WannaCry: hackers withdraw £108,000 of bitcoin ransom, The Guardian, 03 August 2017 https://www.theguardian.com/technology/2017/aug/03/wannacry-hackers-withdraw-108000-pounds-bitcoin-ransom

[9] C. Victor, FBI Says Ransomware Victims Don't Report Attacks, Online Security Magazine, 09 October 2017 http://onlinesecurity.trendmicro.com.au/blog/2017/10/09/fbi-says-ransomware-victims-dont-report-attacks/

[10] T. Rowan, Why Are Organizations Failing to Report Cybercrime?, Infosecurity Magazine, 02 February 2017 https://www.infosecurity-magazine.com/opinions/organizations-failing-report/

[11] FBI News: Incidents of Ransomware on the Rise, 29 April 2016 https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise
[12] C. Duckett, Ransomware victims paying up and would do so again: Telstra, Research article by Australian telco Telstra, 10 April 2018 https://www.zdnet.com/article/ransomware-victims-paying-up-and-would-do-so-again-telstra/
[13] M. Viscuso, Why business is looking good for ransomware criminals, CSO Online Magazine, 08 November 2017 https://www.cso.com.au/article/629705/why-business-looking-good-ransomware-criminals/
[14] I. Rijnetu, A Closer Look at Ransomware Attacks: Why They Still Work, Heimdal Security Magazine, 8 August 2017 https://heimdalsecurity.com/blog/why-ransomware-attacks-still-work/
[15] L. Bracey, The Importance of Business Reputation, Business in Focus Magazine, 30 June 2018 https://www.businessinfocusmagazine.com/2012/10/the-importance-of-business-reputation/
[16] Wikipedia definition of Sextortion: https://en.wikipedia.org/wiki/Sextortion
[17] J. T. Philip and K. Parbat, BlackBerry to open code for security check, https://economictimes.indiatimes.com/tech/hardware/blackberry-to-open-code-for-security-check/articleshow/6249666.cms
[18] D. Shane, Bitcoin: What's driving the frenzy?, 08 December 2017 CNN Money Invest Report http://money.cnn.com/2017/12/07/investing/bitcoin-what-is-going-on/index.html
[19] Base58Check encoding – https://en.bitcoin.it/wiki/Base58Check_encoding
[20] Rosetta Code Programming Chrestomathy site – http://www.rosettacode.org/wiki/Rosetta_Code
[21] C. Cohen, Forensics and Bitcoin, Forensic Focus Magazine for Digital Forensics and e-Discovery Professionals, 16 January 2015 https://articles.forensicfocus.com/2015/01/16/forensics-bitcoin/
[22] Overview of fraud and computer misuse statistics for England and Wales, UK Office for National Statistics Report 25 January 2018
[23] K. Liao, Z. Zhao, A. Doupe, G. J. Ahn, Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin APWG Symposium on Electronic Crime Research (eCrime), 2016
[24] M. Passingham, Less than half of ransomware victims get their files back, Which? Online Magazine, 13 March 2018 https://www.which.co.uk/news/2018/03/less-than-half-of-ransomware-victims-get-their-files-back/
[25] M. Steffen, D. P. DiVincenzo, J. M. Chow, T. N. Theis, M. B. Ketchen, Quantum computing: An IBM perspective, IBM Journal of Research and Development, Volume: 55, Issue: 5, 2011
[26] SWIFT (Society for Worldwide Interbank Financial Telecommunication) https://www.swift.com