Crytocurrency challenges to cybercrime prosecution

Abduqodirov Shohruxbek Oybek o'g'li

Tashkent State University of Law

Abduqodirovshokhrukh@gmail.com

Abstract

The aim of the article is to show cryptocurrencies role increasing of crime, especially cybercrime. This article presents policing challenges of investigating, evidencing and prosecuting organized cybercriminals for the crimes committed using cryptocurrencies especially Bitcoins. A set of best practices is discussed to tackle these challenges in real world investigations. 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.

KEYWORDS

Cryptocurrencies, Bitcoin cybercriminals, law enforcement, organized crime.

Introduction

The concept of cryptocurrencies was first introduced in an original publication by Satoshi Nakamoto in 2008(Reddy and Minnaar, 2018; Nakamoto, 2008). Defined simply as currencies in a digital format, cryptocurrencies were intended to be operationalized as a means of electronic payment. But unlike the equally revolutionary movement of funds electronically, between traditional financial institutions or for payment purposes, this form of electronic transfer would be more secure and fraud-proof, and would not need the role of trusted intermediaries like banks Nakamoto, 2008. In fact, most of these currencies would be free from deflationary forces and from the control of a central institution—such as a central bank or national government This unregulated universal currency has a number of fiscal challenges notably the volatility of its value . 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. A number of Terrorist attacks have found trail of cryptocurrencies. These are very sensitive cases where victims are scary of their public image, business interests, etc. This situation is exploited by the criminals and the use of cryptocurrencies provides them ideal shelter behind the intrinsic anonymity of these currencies.

CYBERCRIME

Simply defined as criminal activity involving computers, networks and networked devices as

accessories, weapons or targets, cybercrime comes in many forms today (Scheau and Pop, 2018) some similar

to traditional crime types and others entirely novel by virtue of a complete reliance on computer technologies.

Generally speaking, the number and sophistication of the forms of cybercrime obtainable today are the result of

the steady evolution of these technologies.

Problem and Discussion

Cryptocurrency assets don't just impact people who mine or trade crypto. It turns out that anonymous platforms that run crypto are also increasingly associated with cybercrime. A recent study from Interisle Consulting Group revealed that phishing attempts related to cryptocurrencies grew 257 percent compared to last year especially for attacks on wallets and exchanges. Cyber criminals use the same techniques they use in other online financial crimes on virtual currencies, and they have great success in their efforts.The international community has also taken a serious look at cybercrime. Cybercrime using crypto (cryptocurrency)reached US $ 8.6 billion last year. These digital assets are obtained from hacking or other criminal acts. Overall, money laundering using crypto has exceeded $33 billion since 2017. According to Chain analysis, the perpetrators targeted centralized exchanges. Chain analysis said money laundering using crypto is a process of disguising the origin of money obtained illegally. Then, the perpetrator transfers it to a legitimate business. These funds come from the sale of data stolen by the dark ransomware attacks. Various forms of cybercrime that are often used by perpetrators include email spoofing is forgery of email headers. The received email message appears to have been sent by a genuine, actual and trusted source. This mode is usually used in spam or phishing campaigns. The target may open the email thinking that the email has been sent by a legitimate source. Hacking is a secret breach of a computer system and stealing valuable data from the system without permission. The spread of a virus or malware is a set of cyber instructions capable of performing some malicious operation. Viruses and malware stop the normal functioning of system programs and insert some abnormalities from the performance of the affected system. Viruses and malware can spread through email, chat messages, data storage, multimedia, the internet and other electronic media. Phishing is the act of stealing personal

information such as passwords, credit card details, victim user data targeted over the internet. This form of cybercrime is carried out by spoofing emails and instant messages to victims.

The money laundering crime utilizes technological sophistication ranging from manual to complicated or super sophisticated by utilizing cyberspace and money laundering crime known as cyber loundering is a cybercrimesupported by knowledge of banks, business, and electronic bankingEstablished and with technological advances already exist, this is done easily, where actors can store or send money through banks using electronics and can be done anywhere and anytime. Money launderers can also deposit the money in a bank without having to include their identity.

Here are some of the most common cybersecurity risks related to cryptocurrency:

1. Cryptojacking– Cryptojacking is the unauthorized use of someone else's computer to mine cryptocurrency.Hackers do this by making victims click on malicious links in emails that load crypto mining code on computers or by infecting websites or online ads with JavaScript code that executes automatically after loading in the victim's browser.

2. Phishing –Phishing campaigns target trading platforms with the primary purpose of stealing user credentials which fraudsters can then use to demand profits or ransom

3. Hacked trading platforms–Cybercriminals compromise trading platforms by stealing fundsfrom users.

4. Compromised registration forms–Cybercriminals steal user information and then sell it on the black market for profit.

5. Third-party apps–Cybercriminals hack other apps to then steal user data and use it to target further attacks.

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.

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.

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. 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 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. 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 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.

Conclusion

Cryptocurrencies are attractive to both risk-averse investors and the criminal underworld. They are interesting to criminals as a target of attack, as a means of payment, and as a way of laundering money. The use of digital forensics in the lifecycle of organized 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. 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 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.

References

1. Wikipedia definition of Cryptocurrencies
2. https://en.wikipedia.org/wiki/Cryptocurrency
3. The Bitcoin Project -- https://www.bitcoin.com
4. 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
5. Irwin, A.S.M. and Turner, A.B. (2018), "Illicit Bitcoin transactions: challenges in getting to the who, what, when and where", *Journal of Money Laundering Control*,