Linköping University | Department of Computer and Information Science

Bachelor's thesis, 15 ECTS | Information technology

2022 | LIU-IDA/LITH-EX-G--2022/075--SE

Characterizing Bitcoin Spam Emails

– An analysis of what makes certain Bitcoin spams generate millions of dollars

Axel Flodmark
Markus Jakum

Supervisor : Niklas Carlsson
Examiner : Marcus Bendtsen

Linköpings universitet
SE–581 83 Linköping
+46 13 28 10 00 , www.liu.se

Abstract

Bitcoin scams cause billions of dollars worth of damage every year, targeting both large corporations as well as individuals. A commonly used method for these scams is spam emails. These emails all share the same intention of trying to trick people into sending Bitcoin to the address attached in the emails, which can be done using various methods like threats and social engineering. This thesis investigates Bitcoin spam emails and tries to distinguish the characteristics of the successful ones. The study was conducted by collecting data on 250,000+ Bitcoin addresses from emails that have all been reported as spam to the Bitcoinabuse website. These addresses were analyzed using their number of transactions and final balance, which were extracted with a Python script using Blockchain's public API. It was found that the successful Bitcoin spam emails only made up a tiny percentage of the entire data set. Looking at the most successful subset of spams, a few key aspects were found that distinguished them from the rest. The most successful spam emails were using blackmail techniques such as sextortion and ransomware to fool their victims. This method is believed to work so well because of the emotional response it invokes from the victims, which in many cases is enough for them to fold. In addition, luck seemed to play a rather big role for the scams to work. The emails had to reach the perfect target: a person that would fall for the trick, have money to send as well as the knowledge to buy and transfer Bitcoin. To increase the odds of finding these types of people, the scammers send emails in large volumes.

Acknowledgments

We would like to express our deepest appreciation to those who provided us the possibility to complete this report. A special gratitude we give to our project supervisor, Niklas Carlsson, whose contribution in stimulating suggestions and answering questions helped us to coordinate our project. We would also like to thank former student Vera Antonov, whose previous work in the area provided us with insights on how to construct our methodology and especially our code.

Contents

Abstract **iii**

Acknowledgments **iv**

Contents **v**

List of Figures **vi**

1 Introduction **1**
1.1 Aim . . . 1
1.2 Research questions . . . 2
1.3 Delimitations . . . 2
1.4 Contributions . . . 2
1.5 Thesis outline . . . 2

2 Background **3**
2.1 The blockchain . . . 3
2.2 Types of Bitcoin spam . . . 4
2.3 Spam . . . 5

3 Method **7**
3.1 Tools . . . 7
3.2 Data collection . . . 7
3.3 The data set . . . 8
3.4 Data analysis . . . 9

4 Results **10**
4.1 Scam types . . . 10
4.2 The distribution of balance and transactions . . . 12

5 Discussion **16**
5.1 Results . . . 17
5.2 Method . . . 18
5.3 Countermeasures . . . 18
5.4 The work in a wider context . . . 19

6 Related work **20**

7 Conclusion **21**

Bibliography **23**

List of Figures

2.1 Example of a typical Bitcoin spam email. 6

4.1 The amount of reports for each abuse type. 10
4.2 The average amount of transactions for each abuse type. 10
4.3 The amount of reports for each abuse type over time. 11
4.4 The abuse types and the respective percentages of emails that used email spoofing. 11
4.5 The total number of reports on Bitcoinabuse for the years 2017-2022. 12
4.6 All addresses ranked by amount of transactions on a log-log scale. 13
4.7 All addresses ranked by balance on a log-log scale. 13
4.8 The top 500 addresses by amount of transactions and their amount of reports on Bitcoinabuse. 14
4.9 CDF showing the distribution of all addresses with more than 0 transactions. . . . 14
4.10 The correlation between the balance and amount of transactions for the addresses. The orange dots show the average balance of periodical groups of transactions. . . 15

Chapter 1

Introduction

Bitcoin amongst other cryptocurrencies has gained popularity over the last decade, reaching its peak market value of 2.9 trillion USD in November 2021 [1]. This market expansion has created opportunities for lucrative scams to arise that use techniques such as spam emails and phishing websites to defraud victims out of their digital money. Cryptocurrency scams work particularly well because it is a decentralized currency. The decentralized aspect provides anonymity to its users combined with the absence of some countries requirements for know your customer, also referred to the KYC process [2], enabling and giving more people access to get away with malicious activities such as scamming and money laundering. Billions of dollars in cryptocurrency is stolen each year in the cryptocurrency market and in recent years the magnitude of this has caught more eyes from authorities. Thus, authorities have made forceful attempts to regulate the cryptocurrency market in order to prevent illegal activities such as scams and money laundering. They have also been more tough and strict toward exchanges where criminals ultimately can trade their cryptocurrency for money issued by the government, also referred to as fiat. Rules for the KYC process is one of the regulation methods that has been tightened, enabling different countries' authorities to be able to receive information about their citizens' activities and exchanges transaction histories. Regulating cryptocurrencies and its activity is complicated. However, because Bitcoin and hundreds of other cryptocurrencies have been decentralized, it allows people to be able to stay anonymous, removing the middleman such as a bank interfering with its network's users and activities.

The adoption of cryptocurrency keeps expanding, providing people with an alternative option to the traditional banking system that historically has had a monopoly in controlling their money. This growing adoption however comes with the drawback that new and inexperienced users are particularly at risk of being exposed to scammers where banks and other middlemen in the traditional banking system would have provided more protection. In order to get a deeper understanding of how and why Bitcoin scams are a big issue, one must analyze the money propagation through scam addresses and characterize the frameworks in which they are used.

1.1 Aim

The aim of this study is to characterize Bitcoin spam emails. This includes how the scammers operate and send money through the decentralized network, and why some frameworks are more successful than than others.

1.2 Research questions

1. What distinguishes successful Bitcoin spam emails from non successful ones?
2. What measures can be taken to track illicit Bitcoin addresses as well as prevent scammers from cashing out?

1.3 Delimitations

There are similarities between Bitcoin and other cryptocurrrencies in the way that scams occur. The research conducted in this thesis is delimited to Bitcoin only, but several of the conclusions overlap with a number of other cryptocurrencies.

1.4 Contributions

Previously, a lot of research in the field has gone into exploring how stolen Bitcoin propagate on the blockchain. However, not as much work has been done on Bitcoin spam, especially on the factors that characterize successful spam. This paper makes an attempt shed some light on the topic, and in that way lay the groundwork for countermeasures to be developed as well as for future research in the area.

1.5 Thesis outline

This thesis starts with an introduction to the subject followed by necessary background information that is important to know in order to understand the purpose of the study. The methodology is then described thoroughly, going through the data collection, the data analysis as well as the main tools that were used. Afterwards, the results are visualized in various tables and graphs with provided insights and discussion for each figure. The discussion section summarizes the results and puts them in a broader context. The methodology, potential sources of error and the validity of the results are also discussed. The thesis ends with a conclusion chapter in which the final conclusions are stated along with thoughts on future work on the subject.

Chapter 2

Background

Bitcoin is a form of money - digital money. Bitcoin operates in a network where people can send money to one another without having any form of middleman[3]. This allows it to be an effective payment method that can be used for trading goods, since the seller is unable to hide any fees or unexpected costs. The network does not require any personal information about its users and is available to anyone with a computer and an internet connection anywhere in the world. Since the middleman is cut out, Bitcoin secures its network through something called the blockchain. The blockchain is a large, shared and encrypted list of all Bitcoin addresses and balances[4]. It keeps track of every transaction made on the network. In short, Bitcoin is a peer-to-peer network that does not reveal the users identities[5].

2.1 The blockchain

The blockchain ledger is a record that everyone has access to. It contains every transaction sent on the network, how many Bitcoins have been sent and the date of every transaction. The ledger is built to ensure that every user has the same information they can access on the ledger. The blockchain is constantly being updated with new transactions in bundles together with the hash of the previous bundle. The bundle is then put on the ledger and is available to the public to find a "proof-of-work", which is a chain of characters that gets inserted at the end of a bundle. Combined with the bundle, it accords the hashed output of the current block depending on the amount of zeros at the start of the hash-string. This work-of-proof model can only be found by trial and error. Bitcoin miners set up computer rigs that constantly work in order to find the first proof-of-work, which is then awarded with an amount of newly acquired Bitcoin. The proof-of-work secures the system and prevents criminals from corrupting and stealing Bitcoin on the network [6].

It is the fact that it's not possible to directly see who is the actual person behind an address that enables the downside of more criminals being attracted to Bitcoin. Authorities and companies have worked to find ways to be able to find out who the actual people behind addresses are when the activity is suspicious and could be of criminal nature [7]. Techniques that can be used to identify users could be to scan websites and forums to see if the users have published their name or email together with the address somewhere on the internet. Other measures involve strategies such as working together with email and web-hosting providers to see if the user has bought a domain or hosting in their legal name and to see if the address could be found through there.

For instance, there are companies that use clustering algorithms to find addresses that suggest that the multiple addresses are used by the same physical person. This phenomenon is called the "wallet cluster" [8]. Algorithms designed and developed by authorities and companies can find patterns where multiple wallet clusters send Bitcoin to one another, and draw conclusions about how the people behind the wallets operate. This can be helpful in finding out about criminal behavior on the ledger as well as discovering who the people behind it are.

2.2 Types of Bitcoin spam

There are many different types of Bitcoin scams. One common denominator regarding Bitcoin spam is that most take advantage of the victim's emotional response to messages. The scammers goal is that they hope that the victims act irrationally after receiving a threatening and sending away money due to fear for instance.

Sextortion is one type of scam is sextortion which is a type of threat where the perpetrator threatens to leak sexual material of the victim unless he or she complies with the criminal's demands [9]. Regarding sextortion linked to financial scams, the perpetrator's threats can be based on nothing but still be successful. The criminals behind these types of scams exploit people's emotional reaction to the threats and false claims. An example of a false claim is that the scammer claims to have found nude pictures of the victim and threatens to leak them unless he or she sends money to the scammer.

Blackmail

Another type of Bitcoin spam contain blackmail, which is very similar extortion method to sextortion. The difference is that blackmail threats can consist of a lot of different types of threats and is not necessarily linked to sexual images [10]. Blackmailing refers to criminal action where the perpetrator threatens to leak private and sensitive information in exchange for money or other benefits. Blackmail in regard to Bitcoin spam works in the same manner as sextortion in terms of playing on the victim's emotional response after he or she receiving a threat. It could be that the perpetrator for example has information about an affair in a relationship, and threatens to leak that information unless he or she agrees to pay Bitcoin.

Ransomware

Ransomware is a type of software that gets installed on a victim's computer that then encrypts the information on resulting in the company or individual not being able to access their files [11]. This often results in the victim having to pay the criminal in order to be able to access their files again. Ransomware could be deployed on one employee's computer in a company that afterwards sends the ransomware to the other employees causing the entire company to stop their operations in the worst case scenario. The price to pay in order to get rid of the ransomware can be very large depending on the business or individual it attacks. Ransomware attacks can also be carried out when the perpetrator claims to have locked the files of an individual's computer. This might despite not being the case still be effective and result in the victim giving an intense emotional response. In Bitcoin spam, it is always the case that the scammer claims that he or she has encrypted the victim's data.

Social engineering

Another type of scam technique is social engineering. This is where a person or organization trick the victim into revealing private information about themselves to the perpetrator[12]. Regarding Bitcoin, social engineering occurs in many different areas. For example, a criminal can put up a fake charity website that tricks victims into sending Bitcoin with the belief that the money will be going to a good cause. Another example is where a colleague or friend pretends to help a victim, but instead the victim reveals too much sensitive information, enabling the fake "friend" to be able to login and access the victim's bank account. Social engineering can in some cases be difficult for the victim to detect since the scammer can put up a facade, gaining the victim's trust for a longer period of time which makes it difficult to see what is actually going on.

Bitcoin tumbler

Bitcoin tumbler also referred to as cryptocurrency mixing service is a fraudulent service that mixes cryptocurrency funds together, thus making it very difficult to find the original source of the funds. This type of service often helps criminals that have received illicit Bitcoin from scams [13]. Bitcoin tumblers are often used in order to launder money and make it very difficult to trace the money.

Darknet market

Darknet marketplaces are commercial websites that operate through darknet onion browsers such as TOR. They facilitate trading of illegal goods. Bitcoin and other cryptocurrencies are often used as payment methods on these sites, and while many of them are serious businesses, many of them are scams[14].

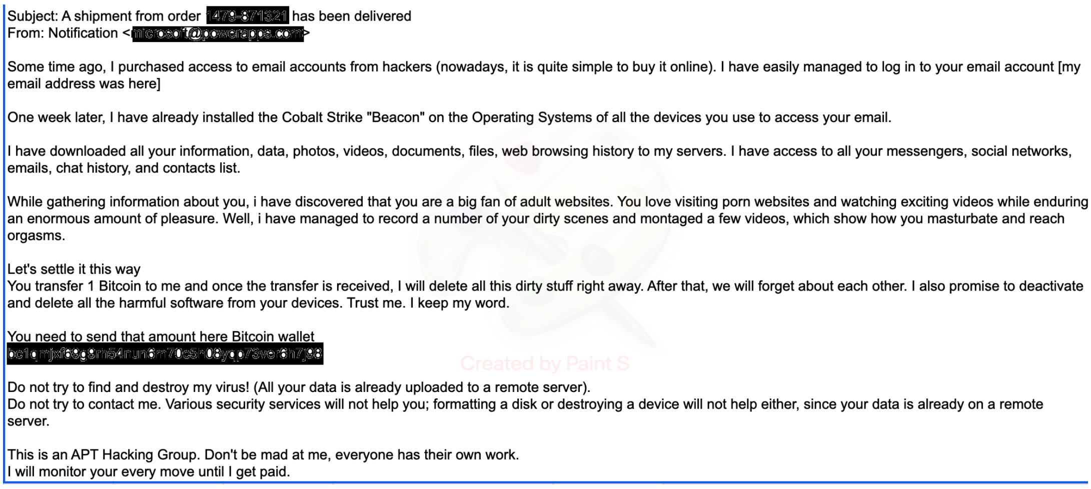
Email spoofing

Email spoofing is a technique where the scammer impersonates an organization or a person by using a fake domain name in the email address used to send the email [15]. The fabricated legitimacy creates a sense of trust which increases the chances that the receiver opens the email, furthermore potentially believing the content of it. Email spoofing can be used together with social engineering for example. An example is that a scammer could claim to be a charity helping people in need and using an email from a well known entity that could help persuading the victim into believing that the spam email is legitimate.

2.3 Spam

With increased attention and adoption of Bitcoin, the number of scams, especially spam emails, have increased. Large sums of money gets stolen each year by cybercriminals in potentially untraceable scams [16]. There are many different types of scams that occur. The scams have also become more advanced and the range of how advanced they are can vary greatly. The hackers target large companies as well as individuals through various methods. One reason why there has been an uptick in the number of Bitcoin scams and the severity of how much money is involved is due to the lack of "KYC" that some cryptocurrency exchanges are missing. This gives scammers the ability to keep their real identity hidden while selling and trading cryptocurrencies. The possibility of being anonymous is an aspect that has given scammers an advantage.

Spam refers to any kind of unwanted information sent to a person that he or she has no interest in receiving. Spam emails is a method used by criminals, where they send large volumes of emails to as many people as possible in the hope that some will accidentally click on the malicious links provided or give out sensitive information about themselves. Spam emails can also contain content that purposefully tricks people into sending their Bitcoin away. An example how they can achieve this is by pretending to be charity organizations seeking donations [17]. Figure 2.1 shows an example of a Bitcoin spam email. This email uses the method of sextortion in an attempt to scare the victim.



Subject: A shipment from order [redacted] has been delivered
From: Notification <[redacted]>

Some time ago, I purchased access to email accounts from hackers (nowadays, it is quite simple to buy it online). I have easily managed to log in to your email account [my email address was here]

One week later, I have already installed the Cobalt Strike "Beacon" on the Operating Systems of all the devices you use to access your email.

I have downloaded all your information, data, photos, videos, documents, files, web browsing history to my servers. I have access to all your messengers, social networks, emails, chat history, and contacts list.

While gathering information about you, i have discovered that you are a big fan of adult websites. You love visiting porn websites and watching exciting videos while enduring an enormous amount of pleasure. Well, i have managed to record a number of your dirty scenes and montaged a few videos, which show how you masturbate and reach orgasms.

Let's settle it this way
You transfer 1 Bitcoin to me and once the transfer is received, I will delete all this dirty stuff right away. After that, we will forget about each other. I also promise to deactivate and delete all the harmful software from your devices. Trust me. I keep my word.

You need to send that amount here Bitcoin wallet
[redacted]

Do not try to find and destroy my virus! (All your data is already uploaded to a remote server).
Do not try to contact me. Various security services will not help you; formatting a disk or destroying a device will not help either, since your data is already on a remote server.

This is an APT Hacking Group. Don't be mad at me, everyone has their own work.
I will monitor your every move until I get paid.

Figure 2.1: Example of a typical Bitcoin spam email.

Chapter 3

Method

This section explains the necessary tools, as well as specify the methodology for data collection and analysis.

3.1 Tools

These are the tools that were used to perform the data collection and analysis.

Blockchain API

Blockchain is a website offering a large variety of trusted blockchain web services, such as for buying, selling and trading Bitcoin, as well as for searching the blockchain for information about transactions and addresses. The service that was of interest to us was their public API. The API let us access useful information about the addresses such as the transaction history and balance. Blockchain's API allowed up to 120 requests per minute, but they offered a way to bypass the waiting time by piping several URLs at once and send them as one request, which ultimately saved us a lot of time [18].

Selenium

Selenium is a browser automation tool that was used for collecting data about phishing domains. It ran with Python code, initially written by student Sebastian Frisenfelt, but slightly modified by us in order to derive the desired information for this collection. The output CSV files contain a variety of columns with useful information about the websites such as content type, status code response and domain. By using a regex for Bitcoin address identification in the Python code, we could also include columns with Bitcoin information in the CSV files, in the case that addresses showed up on some of the websites that we were looking at.

R Studio

For all of the graphs we used R Studio. With the many libraries and functions available with this program we could easily produce graphs like CDF and log-log plots to help us understand the data.

3.2 Data collection

Over 250 000 Bitcoin addresses were downloaded from the Bitcoinabuse database using their public API. This database keeps track of Bitcoin addresses used in emails that have been reported as spam. The addresses were downloaded as a CSV file that contained multiple headers which are explained in 3.3. The column containing the addresses was exported to a separate text file which would be the foundation of our final data set. This text file was imported to a Python script which read the file line by line using the readlines() function. The script took advantage of the public API from Blockchain.info in order to gather information about the balance and amount of transactions for each Bitcoin address in a loop, putting the results in another text file. Addresses with a small transaction history were less time consuming to run, while addresses with a large transaction history were dealt with separately. The script used urllib3's pool manager in order to pool connections and send HTTP "GET" requests to the URL of each bitcoin address on Blockchain.info.

Additional addresses were gathered using Selenium running on Python code, where a large set of phishing domains from the Openphish database were investigated. In addition to phishing domains, regular domains as well as malicious and spam domains were also included in the data collection for the purpose of comparisons. These domains were taken from the databases Tranco, Alexa, Urlhaus, Netcraft and Joewein. With the Netcraft database we could separate the domains for different countries. In the case that one or multiple Bitcoin addresses showed up on one of the websites, they were stored in the resulting CSV file along with other data describing the infrastructure of the website. This data was intended for later characterization of successful phishing websites, looking at the balance and amount of transactions connected to the addresses. To further investigate and characterize domains related to Bitcoin, we looked at the email addresses that were used to send the scam emails in the CSV file from Bitcoinabuse. With a Python script we could parse the email addresses and gather only the domains, where possible. These domains were later examined with Selenium.

For the data collection of the phishing websites, a virtual machine running Ubuntu was used to prevent any malicious data from downloading on our personal computers. Ubuntu was found to be the most suitable operating system to use for all the tools. It facilitated the download and use of both OpenSSL and GNU in parallel. Similar for every tool was the use of a parallel extension, making it possible for us to run the tools on a different number of threads. Using a bash script, the tools could run simultaneously. The outcome was in the form of a set of CSV files that were later merged into one big CSV file.

3.3 The data set

The data set downloaded from the Bitcoinabuse database contained nine headers:

- id
- address
- abuse type
- abuse type other
- abuser
- description
- from country
- from country code
- created at

The id was simply a unique identifier for each report, and the address header contained the Bitcoin address that was used in the specific email. The abuse type header described the type of scam used in the email using six different numbers for each category:

- 1: Ransomware
- 2: Darknet market
- 3: Bitcoin tumbler
- 4: Blackmail scam
- 5: Sextortion
- 99: Other (e.g. fake charity, social engineering)

These different types of scams were described in Chapter 2. The third column, "abuse type other", often contained nothing and was there just in case the one sending in the report wanted to elaborate on the abuse type. "Abuser" contains information about the sender of the email, either in the form of an email address, name or organization, if available. The body text of the email could be found in the "description" column. The last three columns, "from country", "from country code" and "created at", name the country in which the report was made, its country code and the date of the report.

This data set together with the text file of collected data from Blockchain.info made up all of the data used in this study.

3.4 Data analysis

In order to analyze the data, the CSV file from Bitcoinabuse and the text file with transactions and balances derived from Blockchain.info had to be merged. With R Studio, the tool used to create all the plots, the merge function could be used to create a combined data file with the selected headers. This combined text file consisted of the following columns: address, transactions, balance, amount of reports and type of scam. The type of scam was derived from the abuser type number in the CSV file, while the amount of reports for each address had to be calculated using a Python script that read a text file with the 250 000+ addresses listed, and used the count function to count the amount of times that each address had been listed. The abuser column from the CSV file was put in another text file along with all of the corresponding Bitcoin addresses, so that the domains in the email addresses could be studied separately. To facilitate the making of certain plots and analysis, a separate file was created that was stripped of all duplicate addresses, leaving roughly 80 000 unique addresses.

The data manipulation was done in R Studio. For the purpose of finding all possible patterns and visualizing them in separate plots, two columns from the data file were used at a time as the x and y values. This could easily be done in R Studio by simply selecting the column to be used for which axis, that way we could import the whole file and did not have to deal with multiple split up files. To be able to look at attributes for the different abuse types separately, the file was split by abuse type, creating one file each for blackmail, ransomware, sextortion, Bitcoin tumbler, darknet market and other.

The addresses that were scraped from phishing domains were also analyzed in a similar way, but instead of ranking the addresses we ranked the domains by the total amount of transactions. This made it possible to categorize the domains, looking at key factors and approaches that may have contributed to making some domains more profitable than others.

Chapter 4

Results

Here we will present the results conducted from the research using multiple figures.

4.1 Scam types

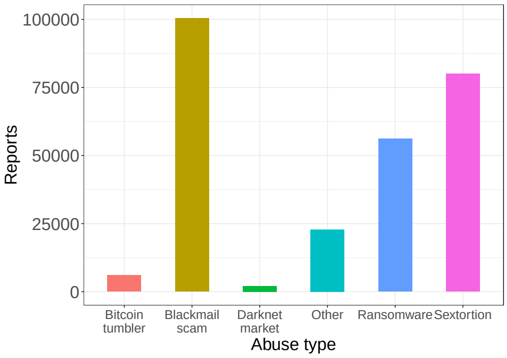


Figure 4.1: The amount of reports for each abuse type.

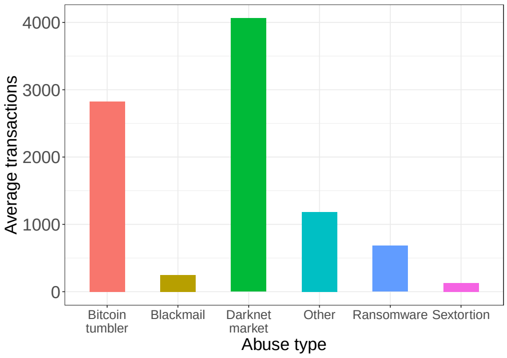


Figure 4.2: The average amount of transactions for each abuse type.

Figure 4.6 shows how many times each abuse type had been reported to the Bitcoinabuse database on the Y-axis, and the abuse types on the X-axis. From Figure 4.1 we can deduct that blackmail scams were the most reported type on the Bitcoinabuse website. Sextortion and ransomware scams came in a close second and third, while the gap was large to darknet market, Bitcoin tumbler and "other". Blackmail is a collective name for all types of extortion, including the ransomware and sextortion categories. To generalize, blackmail in all of its forms made up for the vast majority of reported scams. It is possible that some people mislabeled their reports as blackmail, when in reality it was ransomware or sextortion that they had encountered, which would imply that an unknown portion of the reported blackmail scams actually belong to the other two. This however does not make a big difference since they all cover the same subject.

Figure 4.2 shows the average number of transactions on the Y-axis, and the abuse types X-axis. In Figure 4.2 we can see that the average amount of transactions varies a lot for the different abuse types. Blackmail, ransomware and sextortion scams were the top three reported scams, as seen in 4.1, however it seems that they are at the bottom when it comes to average transactions. The scams labeled "other" remain in the middle, while darknet market and Bitcoin tumbler scams both have a significantly high average amount of transactions compared to the rest. It seems that there is an inverse relationship between reports and average transactions. One way to see it is that Bitcoin tumbler and darknet market type emails had the highest average amount of transactions because their reports were so few, which limits the long tail of smaller to zero transactions that the other abuse types showed. This can in turn be due to limited knowledge of these more unusual scams among the people on the receiving end, giving them less recognition as spam.

Furthermore, an important thing to point out about these two abuse types is that the addresses included in these emails are not unlikely to have been involved in other scams. We can not say this for certain, but after having looked a smaller sample of these types of reports we could see that the contents did not regard emails at all, but rather flagging for illicit involvement in Bitcoin tumbler services or darknet markets. The people that reported the addresses could either have been scammed by one of these websites/services or been exposed to another type of scam, and tracked the addresses back to these organizations. Bitcoin tumblers often serve as an end point that scammers use to mix up the earnings with Bitcoin stolen from other places in an attempt to launder the money and make it harder to track. In addition, darknet markets are illegal businesses that often operate using Bitcoin, where the opportunity for scams to occur is big. In the case that people reported addresses to Bitcoinabuse that were not included in email spam, but instead involved in one of these two, that could explain the high average transaction numbers.

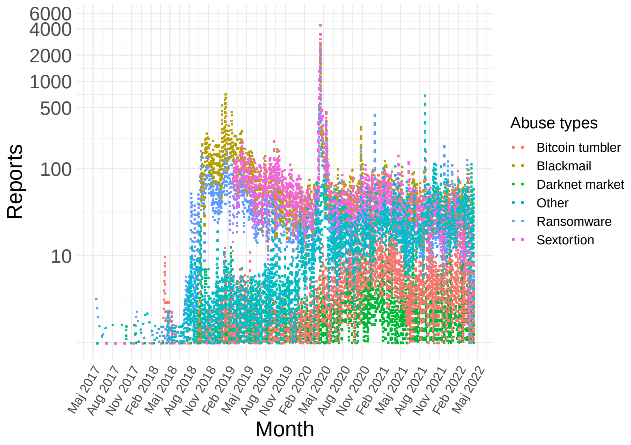
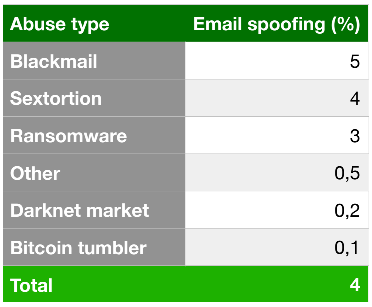


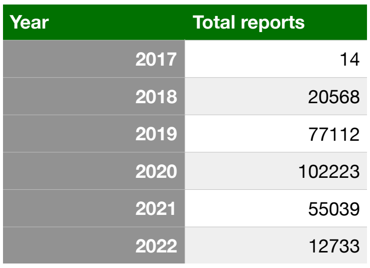
Figure 4.3: The amount of reports for each abuse type over time.



Abuse type	Email spoofing (%)
Blackmail	5
Sextortion	4
Ransomware	3
Other	0,5
Darknet market	0,2
Bitcoin tumbler	0,1
Total	4

Figure 4.4: The abuse types and the respective percentages of emails that used email spoofing.

Figure 4.3 shows the reports for each abuse type on the Y-axis, and the dates on the X-axis, starting from the first report on Bitcoinabuse, that was made in May of 2017, to the latest one in May of 2022. The five-year period between the first and last report is shown on the X-axis with three month intervals between the ticks. The abuse types are represented using different colors, with sextortion being pink, ransomware as dark blue, other as light blue, darknet market as green, blackmail as light brown and Bitcoin tumbler as red. The dotted lines of the different colors contain one data point of the total amount of reports for the respective abuse type for each day that reports were seen for that type.



Year	Total reports
2017	14
2018	20568
2019	77112
2020	102223
2021	55039
2022	12733

Figure 4.5: The total number of reports on Bitcoinabuse for the years 2017-2022.

Adding up the total amount of reports for each year from the figure, we end up with the numbers seen in 4.5. The reports were very low in 2017 and increased drastically during 2018 and 2019, reaching a peak of 100,000+ reports during 2020. After 2020, the number of reports decreased the next year and as of May 2022 the number has reached 12,733. The reports seem to have been less diverse when it comes to abuse types during the 2017-2018 period. Bitcoin tumbler and blackmail reports were first seen in May and October of 2018 respectively. Likewise, sextortion reports were not seen at all at first, and then had a huge spike in March of 2019. Sextortion reports also had the biggest spike of all of the abuse types with over 5000 reports in a single day, sometime in April of 2020. Looking at trends for the entire time period, we find that reports within the "other" category have increased continuously, while the other types have had a more volatile progress. Blackmail, sextortion and ransomware reports have been the most reported abuse types quite consistently until the beginning of 2020, when "Other" started to catch up. Reports of Bitcoin tumbler and darknet market also started to increase at that same time, but never reached the same levels.

In early 2020 the Bitcoin market cap value had a big spike, which could possibly correlate to the increase of around 5-10 reports a day to 50-500 reports a day for many of the abuse types at that same time. With the market value of Bitcoin increasing, it is not odd to see that the amount of Bitcoins scams would increase with it. It can not be said for certain what the underlying factor of occasional spikes in reports is.

Figure 4.4 conveys how often email spoofing was used. The left column represents each abuse type and the column to the right represent what percentage of the emails in each abuse type that used spoofed emails. The figure shows that only a small percentage of emails within each abuse type used the concept of email spoofing. Especially surprising is the 0.5 percentage in the "Other" category that includes methods such as faking a charity and social engineering, both of which one might think could benefit from spoofed emails in order to impersonate a trustworthy entity. Blackmail scams have the highest percentage of 5. This type of scam does not benefit from email spoofing in the same way as the previously mentioned scams, but since the number of reported blackmail scams is so high it invites a larger variety of techniques. There is a possibility that the actual number of emails that used this approach was higher than what is shown in the figure. To find the spoofed emails, we filtered the reports by descriptions containing the word "spoof". This means that the person had to include the word "spoof" in some form when creating the report, hence reports using synonyms of this word, such as "stolen email", "impersonating", or even the cases when the email was in fact spoofed but the person writing the report did not mention it, were not included. Our results very much rely on the reports on Bitcoinabuse, thus there is a high possibility of inaccuracies in the results if a large amount of the reports were either misleading or incomplete.

4.2 The distribution of balance and transactions

Figure 4.6 shows a rank plot of the number of transactions per Bitcoin address. Using log-scale on both axes we observe that the data points get more dense as they move towards

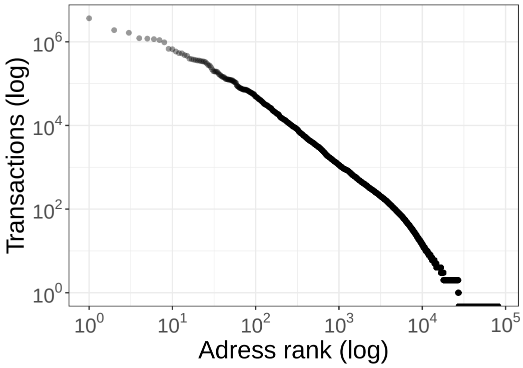


Figure 4.6: All addresses ranked by amount of transactions on a log-log scale.

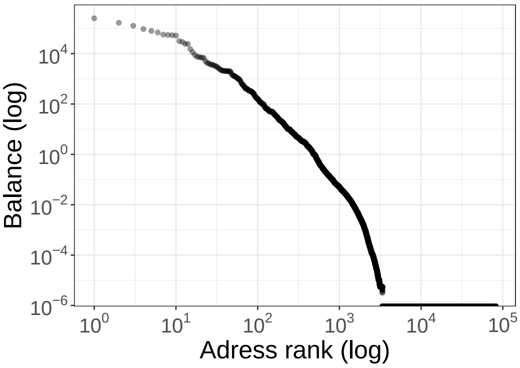


Figure 4.7: All addresses ranked by balance on a log-log scale.

the higher ranks. This behaviour is somewhat in terms with Zipf's law [19], which in our case translates to a small number of the addresses looked at having the highest amount of transactions, while the majority of addresses have a lower amount. This pattern is quite intuitive and tells us that there are only a few scams that successfully generate cash.

Figure 4.7 shows the addresses on the X-axis, ranked by their balances on the Y-axis on a log-log scale. The different shading of the data points represent density. We can see a similar pattern as in 4.6, with the recorded data being thinned out towards the lower ranks. The curve is steeper in this plot, implying that the transactions of the addresses go towards zero faster. There is also a key difference in the amount of addresses with the value zero on the y-axis. There are more addresses that have zero balance than addresses that have zero transactions. The balance does not say as much as the amount of transactions as to whether or not the address has been successful. This is because the balance, for many addresses, is very temporarily more than zero, before the money is passed on to other addresses. The address included in the email is quite exposed, and thereby prone to flagging and reports, which is why scammers use a cluster of addresses to hide the money instead of only one. Roughly 96% of the addresses have zero balance. For the addresses that do contain Bitcoins, it could simply be the case that not all scammers use the previously mentioned technique, instead leaving the money on the address used in the email. It could also be that some of the addresses were not reported for email spam, but some other scam. From looking closer at the reports on Bitcoinabuse, we could deduct that some of them regarded illicit use only, and did not mention en email. Therefore, a small subset of the addresses could possibly be "endpoints" in clustering networks, which explains the high balances.

In Figure 4.8, the addresses included are within the top 500 in terms of transaction amount, i.e. they all have significantly high amounts of transactions in relation to the entire data set. The colors represent density, with yellow being high density and purple low density. We can see that the most reported address, with close to 200 reports, has roughly 1,300,000 transactions. On the contrary, the address with the highest amount of transactions of close to 4,000,000, has only been reported 2 times. The density coloring shows that the majority of the addresses have around 3600-35000 transactions and have been reported less than 5 times.

There seems to be no correlation between addresses having been reported to Bitcoinabuse numerous times and them having a high amount of transactions. Instead, the figure tells us quite the opposite, i.e. that these addresses have been reported only a few times. While it might be more intuitive to think that the scams that have resulted in more transactions would be reported more, one could make an argument for it being the other way around. The scams that were the most successful might not have gotten their addresses reported as often because

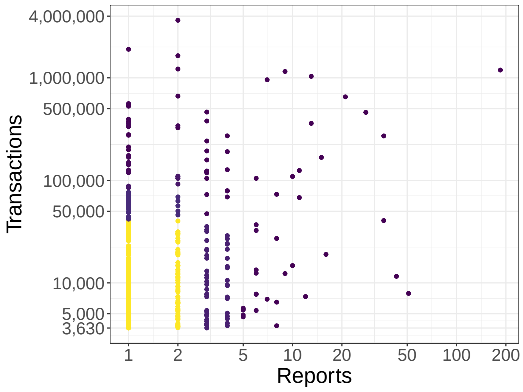


Figure 4.8: The top 500 addresses by amount of transactions and their amount of reports on Bitcoinabuse.

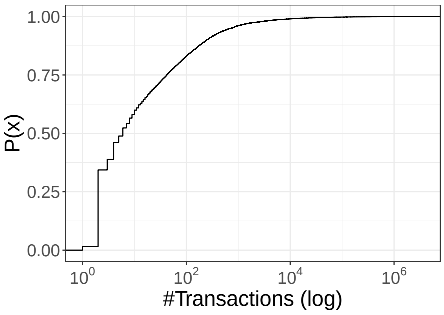


Figure 4.9: CDF showing the distribution of all addresses with more than 0 transactions.

the content of the emails was more believable. Looking at the emails containing the top 500 addresses, we did not see a pattern of particular types of scams being used, but rather that the emails generally were better designed than others in the data set. This could have caused the victims to disregard the emails as spam, and therefore not report them.

Figure 4.9 shows a CDF plot, where the amount of transactions for the entire data set is shown on a log-scaled X-axis, and the probability that a random chosen value for x is less than or equal to x on the Y-axis. Since a very large amount of addresses contained zero transactions, they were excluded from this plot in order for better visualization. This gives an overview of how the addresses were distributed in terms of transactions. CDF shows that roughly 75% of the addresses included had less than 50 transactions. We can also see that roughly 90% of the addresses had less than 1000 transactions. These numbers would naturally increase had we also taken the addresses with zero transactions into consideration in this plot. This shows that the distribution of transactions is quite long-tailed, i.e. that our data set of Bitcoin addresses consists mostly of addresses with few transactions. This could mean that the scammers do not rely on a high success rate overall, but instead try to increase the quantity of emails in order to better the odds that a couple of them are successful.

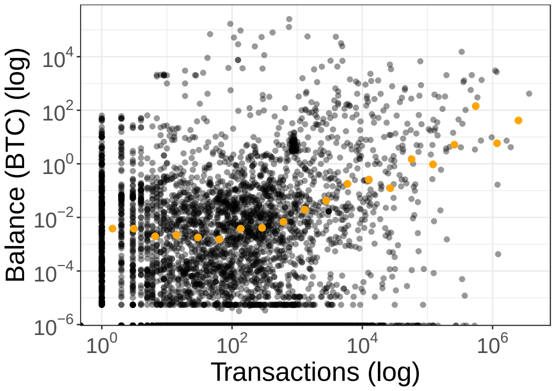


Figure 4.10: The correlation between the balance and amount of transactions for the addresses. The orange dots show the average balance of periodical groups of transactions.

In Figure 4.10 the 20 equally spaced orange dots represent the balance mean for the interval of transactions between the placement of the dot itself and the previous one. Looking at the graph, it seems that the balance mean increases with the amount of transactions, especially after the 1000 transactions mark. However, since the amount of addresses in the data set with over 1000 transactions is significantly smaller than the amount of addresses with less, we can not say that this pattern is truly valid. If we look at the data points in the graph at the 1M transactions mark, there are only a few of them, and they are quite well distributed along the balance axis. The trend that instead seems to be right is that the addresses with fewer transactions have a low balance for the most part, and when we get towards the ones with more transactions the balance is spread out.

Chapter 5

Discussion

A pattern discovered was that the balance of the majority of the addresses was zero. This can be interpreted as the scam attempts being unsuccessful, but that might not necessarily be the case. From taking a closer look at the addresses, several of them were found to have had extensive transaction histories at the same time as zero balance. One reason why this could be the case has to do with the fact that there are several chain-analysis companies that try to identify scams and addresses that have been involved in criminal activities [20]. The scammers run the risk of their addresses being connected to malicious activity that can then result in cryptocurrency exchanges flagging their addresses, and in some cases banning the addresses from being able to convert their cryptocurrency to FIAT money. This is a major issue for scammers, since the cryptocurrency in this case would be worthless. Therefore, it is in the criminal's best interest to spread out the money to multiple different addresses, thereby minimizing the damage in the case that one of the addresses gets flagged. This seemed to be a technique that scammers used for both addresses that had received a lot of money and ones that had not received a lot.

Another key factor for whether a Bitcoin address used in spam is successful or not is how many people the email manages to reach. The quantity of email spam is often very large since the emails themselves are sent in bulk [21]. Determining which people are more likely to fall for a scam is difficult. However, what is known is that a person who is aware of the concept of Bitcoin spam and can somewhat recognize spam emails, is less likely to fall for the scam than a person who is not aware [22]. Therefore the odds increase for the scammers if they manage to send their spam emails to as many people as possible.

Although we managed to find trends with regards to what types of spam methods that seemed to be the most popular, we still were not able to comfortably state which type of characteristics that determined a Bitcoin address' success. The pattern we saw was that the average number of transactions of each abuse type seemed to be lower the more the abuse type had been reported to the Bitcoinabuse database. This result was the opposite to what we thought would be the case, since we had imagined that the abuse types that were the most popular would also be the more successful ones on average. However, it might still be the case that the abuse types reported the most times as spam were the most successful, since the results might have been affected by a couple of factors. Perhaps blackmail spam, the abuse type that was the most reported, were easier for the general public to detect as spam and thereby report the emails, at the same time as the scams worked really well and generated lots of money on the few occurrences that they succeeded. It could also have been the case that the more common abuse types were the most popular ones to be picked up by criminals new to email spam. Many factors could have affected their results in a bad way, such as not sending enough emails, or not being able to dodge the email filtering systems. These factors could have contributed to lowering the average transactions of blackmail. With regards to this, it is hard to determine what truly characterizes successful Bitcoin spam. However, what can be said is that only a small percentage of emails are successful, and the factors that contribute to differences in success between the abuse types seem to be randomly based and have a lot to do with the receivers rather than the senders. Another aspect worth considering is that an email reported to the Bitcoinabuse database for one type of spam might have used multiple different spam methods with the same Bitcoin address. Overall, it seems to be a large luck factor involved with spam in general. What decides if a scammer is successful or not can depend on if he or she manages to hit the right person at the right time, and the scammers seem the increase the odds of this happening by sending large volume of emails.

Considering the entire data set, we could see in the results that the distribution of transactions and balances was very uneven. This further supports the argument that in order for a scam to be successful, it needs to catch the few people that are willing to pay a lot of money. It is not as important to obtain a good success rate overall by receiving small amounts of money from a lot of emails. This pattern has also been found in Bitcoin scams that do not operate using emails, such as fake exchanges, mining investment scams, scam wallet services and high-yield investment programs [23]. Using this logic, blackmail spam can be considered as the most successful type. Without looking at the amount of Bitcoin that these scams received in total, we can say that it was very likely the highest of all of the abuse types because of the big difference in number of reports between blackmail and the others. The low average amount of transactions is a consequence of sending plenty of emails, and as we know most of them fail.

Whether Bitcoin spam has an impact on the market price of Bitcoin is difficult to say since it does not exist much data on the topic. However, we find it very unlikely, especially today when the daily volume of Bitcoin trades is in the tens of Billions USD. The data set studied in this thesis only contained a small amount of addresses with significant amounts of money and transactions, which implies that these addresses could not single-handedly have impacted the price of Bitcoin. In contrary, there is a possibility that it could work the other way around. The expansion and increased adoption of Bitcoin as a currency has contributed to a high market capitalization. This means that Bitcoin has become more popular and gained more users, which gives the scammers more people to work with that know how to manage and send Bitcoin. This could explain why the amount of reports increased when the market cap was at its highest. More widespread knowledge of the subject could also have contributed to greater awareness of Bitcoin spams.

5.1 Results

Looking at the addresses with the highest amount of transactions, the total amount of money sent/received was remarkably high. The top addresses had moved billions of dollars in BTC, most often through thousands of transactions. With sums like these, it is hard to think it could all be generated through spam emails alone. After looking further into the reports for these addresses on the Bitcoinabuse website, we found that some of them were connected to what seemed to be black market websites. This finding could account for the large sums of money in the case that these addresses in some way were also used for black market scams, although it seems a bit odd that the scammers would use the same addresses for different types of scams. In addition, letting that much money flow through a single Bitcoin address draws a lot of attention and runs a high risk of getting the address flagged. With the amount of money these addresses moved, and the fact that they were involved in several areas of scamming tells us that we were dealing with some sort of organization or large scam operation rather than an individual working alone from their computer.

5.2 Method

The script that was developed retrieved both the balance of the addresses as well as the amount of transactions that had been made in total. Only using those two aspects when analyzing which addresses were successful and why is not sufficient for obtaining the whole precise picture, but it is good enough to see some patterns and draw conclusions. Considering the time frame for this study, our ability to conduct an ideal data collection was limited. In order to get a more valid result, one would also need to collect the entire transaction history for each address. This would be very time consuming, but with this data in hand, one could look into the actual BTC amount of the transactions, and distinguish between addresses that actually move considerable amounts of money and the ones that do not. In our study, we consider a high amount of transactions as a sign of an address being successful. This is not wrong for the addresses in general, but can sometimes be a bit deceiving.

With the methodology used in this study, the amount of headers used in the final data set were limited. There is plenty of room for more extensive research on the subject. One could include the dates of the reports, and from which country they were made, both of which are available in the CSV file from Bitcoinabuse, in order to find further patterns and analyze the addresses more in depth. With more time, the data collection could be expanded using a different API to include full transaction histories of the addresses, as mentioned previously.

This study was also supposed to include some characterization of phishing websites where Bitcoin addresses could be found. However, the data collection of phishing websites did not end up with enough data to conduct a proper analysis. The cases where Bitcoin addresses showed up on one of the websites were so rare that we could not draw any conclusions about the characteristics. This was also the case with the domains of the email addresses that were used to send the spam emails reported to Bitcoinabuse. Running these domains in Selenium did not result in any significant findings, as the majority of domains were invalid. The valid domains belonged to spoofed addresses, thus giving us information about real websites that in reality had nothing to do with scams and did not have to be characterized. For these reasons, we did not include this part of the study in the results and instead switched the focus fully to the Bitcoin spam emails.

5.3 Countermeasures

Due to Bitcoin addresses not being linked to the physical person of each respective address, it makes it a difficult task to identify and punish people for criminal activity such as email spam. One aspect that aids criminals who send Bitcoin spam emails is that email services allow large quantities to be sent at once. This area is difficult to restrict since there are many businesses that operate by sending a lot of emails to customers and potential customers for legitimate reasons. Something that can be done to reduce the number of spam emails that reach innocent people however, is to keep developing new smart email filtering systems that can detect Bitcoin spam and prevent them from reaching potential victims.

Another thing that can be done to make life more difficult for the people responsible for Bitcoin spam emails is to make it difficult for criminals to be able to trade their cryptocurrency into FIAT money. Authorities across the world have implemented ambitious regulations to demand mandatory KYC processes on cryptocurrency exchanges [24]. Despite this, there are still loopholes that allow criminals to be able to find a way around this problem and be able to trade stolen cryptocurrency for FIAT money. Therefore we suggest authorities keep working on this issue, which enables legal authorities in each respective country to receive information about its citizens actions on the exchanges, and enables law enforcement to take legal action against criminals. This is not an easy task however since it requires jurisdiction to be set in place across the world, since it otherwise will create opportunities for scammers to find loopholes to in the system[25].

5.4 The work in a wider context

Bitcoin spam causes a lot of damage to innocent people every year. They generally affect people that are unaware of the existence of these types of scams. With the increasing adoption of Bitcoin across the world, it is likely that Bitcoin spams will multiply in the future. We believe that a way to limit the damage is to bring awareness to people about the scams and how they work. This thesis summarizes what types of Bitcoin spam emails generate the most money, and we hope that email services keep developing their filtering systems with regards to Bitcoin spam, especially when it comes to threat emails involving blackmail and sextortion, which were found to be the most reported types of scams. By counteracting the most effective methods in Bitcoin spam, there is hope that the amount of Bitcoin spam emails will decrease in the future as the criminals find them to be less lucrative.

One risk with cryptocurrency regulation is that by regulating a specific area in an attempt to make it difficult for scammers, it might not actually lead to less criminal activity. The risk is that the scammers adapt and change their ways of scamming and move to a different area.

Chapter 6

Related work

A lot of work has gone into investigating capabilities for money laundering, Ponzi schemes, ransomware payments and tax evasion on the blockchain [26][27]. There is a lack of research in the field about Bitcoin spam emails precisely. However, other areas of Bitcoin scams including fake exchanges, mining investment scams, scam wallet services and high-yield investment programs have been explored more thoroughly [28].

Bitcoin gets referred to as pseudo-antonymous due to the addresses are not directly linked to a physical person, but all the transaction data gets stored on the ledger. Research has gone into identifying ways that use machine learning to group addresses by ownership. This strategy is also known as address clustering and by using behavioral patterns and public information stored on the blockchain can identify an owner of multiple different addresses[29].

There have also been several works in the email spam detection field that have lead to machine learning technology and algorithms that help detect and prevent email spam [30]. While many different types of email spam have similarities, differences can still be found in different sectors where spam occur.

Due to cryptocurrency being a relatively new sector, authorities are actively looking to regulate it[31]. These regulations could rapidly change the climate of Bitcoin in the countries where authorities deploy strict regulations, which would then create a big impact on the users [25]. The regulations will not necessarily only have an impact on ordinary users, but how scammers operate as well.

This thesis tries to characterize successful Bitcoin spam emails. While there have been plenty of research on Bitcoin as a currency, the blockchain and Bitcoin scams, there is a lack of studies on Bitcoin spam in particular. This paper differs in the way that it looks more in depth into the underlying ways that scammers using this method operate, and how some of them manage to succeed better than others.

Chapter 7

Conclusion

After investigating the characteristics of different types of Bitcoin spam and analyzing the results, a few aspects that distinguished successful Bitcoin spam were found. A major factor for success is how many people the spam emails manage to reach. This also includes how well they can bypass the email filtering systems in order to avoid ending up in the spam folder instead of the inbox. We found that threats in general, including blackmail, ransomware and sextortion were the most common types of spam. We found that these abuse types did not contain the most transactions however since the average Bitcoin address attached to Bitcoin tumbler addresses and darknet marketplace addresses contained a substantial amount of more transactions on average.

Another conclusion drawn was that the scam business itself works in a similar way to many other markets when it comes to the success ratio. The majority of addresses had received zero Bitcoin, suggesting that they had failed. Our final conclusion is that one of the largest factors if not the largest factor is how lucky the criminals sending email spam are. What decides if certain Bitcoin spam is successful or not can come down to if or not the spam email manages to reach an unsuspecting and somewhat naive person with a lot of money. This makes it difficult to determine specific characteristics of an email that would increase the odds of an email being successful, since it appears that how lucky the scammers are in finding the people who get tricked is the most important factor deciding how successful certain Bitcoin spam is.

To extend further knowledge in this area it would be interesting to see more research go into exploring and characterizing successful Bitcoin phishing websites such as fake exchanges. From seeing how much money some of the scammers are generating, it is important to try to develop applicable countermeasures for Bitcoin scams in the future. In order to do this, one needs to look more closely into how the stolen Bitcoin propagates and moves on the blockchain through different clusters of addresses to ultimately be exchanged into FIAT. We believe that making it difficult for scammers to cash out the stolen Bitcoin into FIAT is the most efficient way to decrease Bitcoin spam.

It would also be interesting to do a deep dive on how the emails are designed and worded. Due to the large amounts of emails that were investigated in this thesis, we were not able to take a closer look at the contents of the emails themselves. We suggest using a smaller sample of successful emails and comparing them to a smaller number of unsuccessful emails, to see if there are any characteristics that stand out within the successful ones. This does not guarantee any further concrete discoveries, especially since we in this thesis argue that the emails just have to be sent to the right people. However, there might be ways that the scammers can sort out these types of people and target them. In the event that a certain style or design of email would be found to contribute to a higher success rate, perhaps the email filtering systems more directly could adapt to filtering out these type of techniques.

Bibliography

[1] CMC. *Global Cryptocurrency Charts Total Cryptocurrency Market Cap*. URL: `https://coinmarketcap.com/charts/`. accessed: 04.03.2022.

[2] Yaya J Fanusie. "Financial Authorities Confront Two Cryptocurrency Ecosystems". In: *Global Governance to Combat Illicit Financial Flows* (2018), p. 56.

[3] Matthias Lischke and Benjamin Fabian. "Analyzing the Bitcoin Network: The First Four Years". In: *Future Internet* 8 (Mar. 2016). DOI: `10.3390/fi8010007`.

[4] G. Karame and S. Capkun. "Blockchain Security and Privacy". In: *IEEE Security Privacy* 16.04 (July 2018), pp. 11–12. ISSN: 1558-4046. DOI: `10.1109/MSP.2018.3111241`.

[5] Ryan Henry, Amir Herzberg, and Aniket Kate. "Blockchain Access Privacy: Challenges and Directions". In: *IEEE Security Privacy* 16.4 (2018), pp. 38–45. DOI: `10.1109/MSP.2018.3111245`.

[6] Satoshi Nakamoto. "Bitcoin: A peer-to-peer electronic cash system". In: *Decentralized Business Review* (2008), p. 21260.

[7] Martin Harrigan and Christoph Fretter. "The Unreasonable Effectiveness of Address Clustering". In: *2016 Intl IEEE Conferences on Ubiquitous Intelligence Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*. 2016, pp. 368–373. DOI: `10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0071`.

[8] Hyochang Baek et al. "A Model for Detecting Cryptocurrency Transactions with Discernible Purpose". In: *2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN)*. 2019, pp. 713–717. DOI: `10.1109/ICUFN.2019.8806126`.

[9] Roberta Liggett O'Malley and Karen M Holt. "Cyber sextortion: An exploratory analysis of different perpetrators engaging in a similar crime". In: *Journal of interpersonal violence* 37.1-2 (2022), pp. 258–283.

[10] Jonathan Yorke, Lesley Sefcik, and Terisha Veeran-Colton. "Contract cheating and blackmail: a risky business?" In: *Studies in higher education* 47.1 (2022), pp. 53–66.

[11] Philip O'Kane, Sakir Sezer, and Domhnall Carlin. "Evolution of ransomware". In: *Iet Networks* 7.5 (2018), pp. 321–327.

[12] Sven Uebelacker and Susanne Quiel. "The social engineering personality framework". In: *2014 Workshop on Socio-Technical Aspects in Security and Trust*. IEEE. 2014, pp. 24–30.

[13] David Buil-Gil and Patricia Saldaña-Taboada. "Offending Concentration on the Internet: An Exploratory Analysis of Bitcoin-related Cybercrime". In: *Deviant Behavior* (2021), pp. 1–18.

[14] Julian Broséus et al. "A geographical analysis of trafficking on a popular darknet market". In: *Forensic science international* 277 (2017), pp. 88–102.

[15] Hang Hu and Gang Wang. “End-to-End Measurements of Email Spoofing Attacks”. In: *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 1095–1112. ISBN: 978-1-939133-04-5.

[16] Massimo Bartoletti et al. “Cryptocurrency scams: analysis and perspectives”. In: *IEEE Access* 9 (2021), pp. 148353–148373.

[17] BA. *Bitcoin Abuse Database*. URL: https://www.bitcoinabuse.com/reports/bc1q8y2tf9kcmtn6v9wtmjw08rc5pygackkzux0p2n. (accessed: 07:03:2022).

[18] Blockchain.info. *Blockchain Data API*. URL: https://www.blockchain.com/api/blockchain_api.

[19] Seung Ki Baek, Sebastian Bernhardsson, and Petter Minnhagen. “Zipf’s law unzipped”. In: *New Journal of Physics* 13.4 (2011).

[20] CoinDesk. “Leaked Slides Show How Chainalysis Flags Crypto Suspects for Cops”. In: (). URL: https://www.coindesk.com/business/2021/09/21/leaked-slides-show-how-chainalysis-flags-crypto-suspects-for-cops/. accessed: 2022-05-15.

[21] Emmanuel Gbenga Dada et al. “Machine learning for email spam filtering: review, approaches and open research problems”. In: *Heliyon* 5.6 (2019), e01802.

[22] Steve Sheng et al. “Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions”. In: *Proceedings of the SIGCHI conference on human factors in computing systems*. 2010, pp. 373–382.

[23] Marie Vasek and Tyler Moore. “There’s No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams”. In: *Financial Cryptography and Data Security*. Ed. by Rainer Böhme and Tatsuaki Okamoto. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 44–61. ISBN: 978-3-662-47854-7.

[24] Yaya Fanusie and Tom Robinson. “Bitcoin laundering: an analysis of illicit flows into digital currency services”. In: *Center on Sanctions and Illicit Finance memorandum, January* (2018).

[25] Misha Tsukerman. “The block is hot: A survey of the state of Bitcoin regulation and suggestions for the future”. In: *Berkeley Technology Law Journal* 30.4 (2015), pp. 1127–1170.

[26] Yining Hu et al. “Characterizing and detecting money laundering activities on the bitcoin network”. In: *arXiv preprint arXiv:1912.12060* (2019).

[27] Massimo Bartoletti, Barbara Pes, and Sergio Serusi. *Data mining for detecting Bitcoin Ponzi schemes*. 2018. DOI: 10.48550/ARXIV.1803.00646.

[28] Pengcheng Xia et al. “Characterizing cryptocurrency exchange scams”. In: *Computers & Security* 98 (2020), p. 101993.

[29] Dmitry Ermilov, Maxim Panov, and Yury Yanovich. “Automatic Bitcoin Address Clustering”. In: *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*. 2017, pp. 461–466. DOI: 10.1109/ICMLA.2017.0-118.

[30] Hekmat Mohammadzadeh and Farhad Soleimanian Gharehchopogh. “Feature selection with binary symbiotic organisms search algorithm for email spam detection”. In: *International Journal of Information Technology & Decision Making* 20.01 (2021), pp. 469–515.

[31] Galang Prayogo. “Bitcoin, regulation and the importance of national legal reform”. In: *Asian Journal of Law and Jurisprudence* 1.1 (2018), pp. 1–9.