NTNU
Norwegian University of
Science and Technology

Cybercrime Economy

A Netnographic Study on the Dark Net
Ecosystem for Ransomware

Yara Bayoumy

Master in Information Systems	
Submission date:	June 2018
Supervisor:	Guttorm Sindre, IDI
Co-supervisor:	Per Håkon Meland, SINTEF

Norwegian University of Science and Technology
Department of Computer Science

Summary

Black hat hackers are far more shrewd than the public's stereotypical perception of them. They are no longer script kiddies who are trying to impress their social circles, but skilled businessmen with the general aim to profit from exploitative attacks. Very little research has been done on how the cyber-criminals involved make decisions based on profit margin calculations.

The dark net provides the perfect environment to commit cyber crimes without being tracked down by law enforcement. An entire economy has emerged in the dark net as a result of transactions of illegal goods and services supported by cryptocurrencies. The social structure of the members in the dark net is strong enough to survive any intrusions made by law enforcement.

The dynamic shifts in the field of cyber security has encouraged many researchers to propose different methodologies that capture the true intent of an attacker. In this report, a netnographic study was done to obtain data useful for threat predictions and attacker profiling. This included observations of the online marketplaces in the dark net and the researcher's reflections on the social communications between the different actors involved in the creation and distribution of ransomware. Data collected from this study was also used to deduce a cost-benefit framework.

Acknowledgement

First and foremost, I would like to express my sincerest gratitude to my co-supervisor Per Håkon Meland for his continuous help and support. Thank you for offering me an opportunity to attend and speak in academic conferences and introducing me to many experts in the field. Thank you for creating an environment of enthusiasm for learning, appreciation for growing, and room for making mistakes along the way. Without your guidance this dissertation would not have been possible.

I would also like to thank Professor Guttorm Sindre for his contribution in the supervision of this work. The door to Professor Guttorm's office was always open when I needed help. I truly appreciate your effort in answering my questions and offering advice when needed.

A special thanks to my family, especially my father Fareed, my mother Omnia and my sister Sara for their emotional and financial support. Thank you for encouraging me to pursue my Masters abroad.

My gratitude also goes to the friends I have made during my stay in Norway, especially to the girls of Computer Science, Class of 2018. Thank you for your welcoming hospitality. Lastly, I would like to thank all the tutors that lectured me during my Masters degree at NTNU. I apologize to anyone I overlooked. To you all, I express my deepest appreciation.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Abbreviations

DDoS	=	Distributed Denial of Service
FUD	=	Fear, Uncertainty and Doubt
FE	=	Finalize Early
ISP	=	Internet Service Provider
IRC	=	Internt Relay Chat
NiRWebs	=	Netnographic Interactive Research Websites
OPSEC	=	Operation Security
PGP	=	Pretty Good Privacy
RaaS	=	Ransomware-as-a-Service
Tor	=	The Onion Router
VM	=	Virtual Machine
VPN	=	Virtual Private Network
XMPP	=	Extensible Messaging and Presence Protocol

Glossary

Bitcoin : A type of cryptocurrency.

Carding : The practice of stealing and selling credit card information

Botnet : Network of connected devices that coordinate together to perform a task

Clearnet : Segment of the World Wide Web that is accessible

Cryptocurrency : A currency that uses decentralized blockchains to avoid surveillance. Used by dark net members for transactions and to receive ransom

Cryptomarket : Online marketplace that uses cryptocurrencies as the media for transactions

Cybercrime : Computer-mediated crime

Dark Net : A segment of the deep web that is used for to host hidden services

Deep Web : A part of the World Wide Web that is not indexed, therefore not discoverable by search engines

Doxx : Giving out personal information

Drops : Locations to meetup to receive illegal packages, not the place of residence

Escrow : The involvement of a neutral third party to make sure that the purchase money will reach the vendor when the buyer has fully received the product or service

Finalize Early (FE) : Release of escrow funds before buyer conditions have been met. This only benefits the vendor as it avoids the risk of cryptocurrency influx

Fullz : A person's entire data cluster (Name, address, SSN, DOB, Phone, Email etc.)

Multisignature : Multisig for short, is an authorization method in which requires multiple keys to authorize a transaction.

Malware : Software created to maliciously disrupt activity and access to a device.

Netnography : Ethonographic research methodology taking place on the internet

Ransomware : Type of malware that blocks access to a device, the perpetrators promise to unlock it in exchange of a ransom.

Ransomware-as-a-Service : Type of Software-as-a-Service with support for malicious ransomware instead of a software

Script Kiddies : Premature individuals with basic hacking skills. Are capable of coding, but can only write weak malicious software

Surface Web : Another term for clearnet

1

INTRODUCTION

This Chapter presents the motivation behind this research study, the questions imposed and the methodology used to answer these questions. The end of this chapter summarizes the structure of this thesis.

1.1 Motivation

> *There are over 100 different sources of data on cybercrime, yet the available statistics are still insufficient and fragmented; they suffer from under- and over-reporting, depending on who collected them, and the errors may be both intentional (e.g., vendors and security agencies playing up threats) and unintentional (e.g., response effects or sampling bias)*
>
> – Anderson et al., *Measuring the Cost of Cybercrime* [4]

Security threats have evolved throughout the years as enterprises and individuals are increasingly relying on computer-based systems. The internet and modern day digital currency also offer a safe network for cybercriminals to carry on with their illegal activities unidentified. Observing these activities up close can help identify cost trend analysis of the services provided by the cybercriminals in the hidden segment of the internet. The latest service being Ransomware, a malware used to extort victims into giving money in exchange for access to their files on the hacked device. Ransomware spread globally at unforeseen heights and was labeled as one of the greatest threats in cybersecurity. The miscreants behind the malware work in an organized manner in the hidden *dark net*.

The *dark net*, or *dark web* is a subset of the *deep net/web*. What distinguishes any website in the deep web from that on the surface web is that it is not indexed, and therefore, cannot be accessed through most commercial search engines such as Google. The *dark net* includes websites that are intentionally created in this secret space on the grounds of privacy. *Surface web* or *clearnet* refers to the segment of the internet that includes indexed websites. Indexed websites can be easily tracked and the location of the hosting servers are open for the public. Individuals or organizations who wish to conceal their identity or location would host their websites in the dark net as a hidden service with a URL ending with *.onion*.

Criminals have taken benefit of the anonymity feature of the dark net to hide their illegal activities. The criminal acts offered through hidden services range from drug trafficking to hacking services. Transaction funds are channeled with the help of cryptocurrencies such as Bitcoin due to its anonymity. In 2001, Silk Road was hosted as a hidden service on the dark net as the first underground marketplace, also known as *cryptomarkets* for its reliance on cryptocurrency. It took the same format as commercial e-shopping websites on the clearnet such as e-Bay and Amazon, but instead, sells drugs, narcotics, fake IDs among other illegal products with prices listed in Bitcoins. When Silk Road was shutdown by law enforcement agencies, other marketplaces were created with the same business model and infrastructure.

The rise of cryptomarkets triggered interest in cybercriminal enterprise taking place in the dark net. Analysis of dark net markets has offered a better understanding of underground ecosystem and its social structure. Examples of such research is [14], who used crawling mechanisms to collect data from the now terminated Silk Road. Analysis of the gathered data presented insight on the categories sold in the marketplace, popularity of vendors and their products and also regional distribution of product shipment. This research was then sought as a point of reference for other studies centered around cryptomarkets which also used crawling as method of collecting data [20], [18]. More external shocks began to emerge, which involved exit scams by cryptomarket owners [41].

What is even more intriguing is the resilience of dark net marketplaces. Silk Road has been a very successful trade in the dark net community and many other marketplaces started to follow the lead. When Silk Road was shut down, the activity in the dark net was not hindered. Members in Silk Road migrated to another marketplace called *Silk Road 2.0*. This was not managed by the same board that controlled Silk Road, but a new board of administrators that seized the opportunity prior to Silk Road's termination. Research has shown that this phenomena occurred several times in many other shut downs [51].

Professional cybercriminals' main incentive behind their attacks is to gain substantial profits. An attack is not worthy of developing and distributing if it is not a profitable exercise. Ransomware became a successful phenomena as a means of extortions. Hospitals and government offices were targeted, leaving them with no choice but to pay the ransom. Ransomware threats are on the rise and new variants of the malware are continuously discovered. Unfortunately, many organizations that have been attacked by ransomware refuse to publicly share vital information due to several reasons. Bad publicity can have a negative influence on their position in the financial market. Organizations may also have weak legislative action to defend the firm from consumer right breach. Nevertheless, economic analysis of ransomware and cybercrime have been presented before in research. An economic model was put forth based on the victim's willingness to pay [27]. In another study, the cost of ransomware was determined based on the complexity of the vulnerability the malware is exploiting [39].

Seldom has the issue of the ransomware economy in the dark net been raised by the research industry. Cyber security firms and law enforcement agencies dominate research in ransomware-as-a-service provided in the dark net. This results in statistics and figures presented with some bias. Take for instance, in October of 2017, a prominent cyber security firm called Carbon Black issued a report claiming that the sales of ransomware in the dark net will increase by 2500% [8]. The legitimacy of these numbers are in part questionable. The vast amount of information available on the dark net makes it difficult to give out precise analysis. In addition to that, the volatility of cryptocurrencies leads to miscalculations of profits and costs incurred. As a consequence, the possibility and scalability of future attacks can be challenging to estimate.

This claim has been supported by other empirical studies about the economy of cybercrime. Many of them call attention to the importance of cryptomarket research [6, 4, 49, 14]. Offering a more precise and unbiased representation of the cybercrime economy with respect to ransomware is the main motivation behind this research. This can contribute to the field of threat intelligence by apprehending the attacker's incentives and actions.

Ritter [49] presented five approaches to examine the drug market. These included netnographic, economic, psychological and survey research. From each approach, the benefits and expected outcomes were presented.

Observational study of online communities is known as *Netnography* [34]. This method of research is good for understanding the social structure of members of the dark net, and their responsibilities behind the creation and distribution of ransomware.

Netnography could also fulfill the necessary factors that make up a business model listed as follows [11]:

- Understand the attackers, their incentives and risks
- Estimate the social cost losses due to cybercrime
- Identify the resources needed to combat cybercrime

Netnographic study has been done before in a study on the activities on Silk Road [6]. The study documented the social structure of Silk Road members, but was discontinued once the website was shut down by law enforcement. Bakken's research did not focus on a particular category of items sold on the cryptomarket. However, drug related items were the dominant category in number of items, and therefore, were mentioned frequently throughout the report. In addition, the study applied a Deleuze-Guattarian approach to capture how the cryptomarket functions. This approach is irrelevant for the aims of this research, hence disregarded.

In August 2017, a preliminary study was performed on the dark net for the objective of creating an attacker-centric threat model [7]. The study only identified three stakeholders behind the creation and distribution of ransomware from cybersecurity reports. These actors are *Authors* who write the code which makes up the ransomware, *Vendors* who sell the ransomware on cryptomarkets and *Distributors* that infect devices.

Netnography is a suitable methodology for this research since it can capture clusters and typologies in an online community [49]. Netnographic fundamentals include immersion of the researcher in the online community and prolonged observations of the activities taking place. This eventually offers a rich picture of organizational hierarchy of the online community and its communication channels. In addition, we can grasp the economic aspects through observations of the supply and demand value chain in dark net cryptomarkets. Lastly, netnographic methodology is not strictly conformed to one type of online community. It is applicable to any as long as it as the community has a substantial userbase and is rich in content.

1.2 Research Questions

The research questions listed below concern two discrete but loosely entwined phenomenon which is *ransomware-as-a-service* and the *dark net.* The first research question hopes to present a better understanding of the devised social infrastructure of the dark net and the second research question aims to express the economic turnover of ransomware-as-a-service

- **RQ1** What are the behavioural aspects of members involved in the underground economy of ransomware in the dark net?
  - *RQ1.1* What is the nature of the activities practiced by the online community within the dark web market forums?
  - *RQ1.2* What are the economic incentives and risks behind the actions of dark net members?
- **RQ2** What is the business model of Ransomware-as-Service?
  - *RQ2.1* What are the cost-benefit estimates of ransomware sold on the dark net?
  - *RQ2.2* What is the organizational structure of the economy of Ransomware-as-a-Service?

1.3 Research Approach

The approach used in this research is mixed, i.e. both qualitative and quantitative methods are used to collect and analyze data. The qualitative methods involved an extensive netnographic study on pre-selected dark net markets active on the Tor network. The type of netnography will mostly be semiotic in the sense that the researcher will not emphasize with the subjects but inspect the intentions and behaviours of the users [45]. The expected outcome is a general understanding of the attacker incentive's and possible organization structure of cybercrime.

The quantitative approach used was inspired by the earlier research done on cryptomarkets. The aforementioned research papers that involved extensive studies on cryptomarkets have used crawling mechanisms to collect huge sums of data. Crawling data will help capture the dynamic and growing content in cryptomarkets. Since our main objective is to achieve precision and reliability, a triangulation of cryptomarket records (via observations and crawling) could help strengthen the validity of our data. Added to that, capturing records of data from earlier years, can support analysis through time and major events.

The netnographic strategy involves the researchers understanding of the social activities between the hackers that develop the ransomware, the vendors that sell them, and the consumers that buy them. Therefore it has a strong connection to constructivist/interpretive paradigm. Despite the fact that there is very little researcher involvement, it still does not relate to a critical research paradigm because the observations will be presented from the researcher's personal perspective. The conversations between the different users in the dark net will be an important source for qualitative data analysis, and researchers may have different interpretations of the motives of the users involved.

1.4 Literature Review

A background study of similar dissertations was performed prior to the research. The outcome of the literature review is to connect some of the findings and methodologies presented by other researchers to the study and its empirical analysis. The sources were retrieved from *Google Scholar* [1], *Scopus* [3] and *Mendeley* [2]. When searching for articles the following tags were used:

- Cryptomarkets
- Cybercrime
- Ransomware
- Economy
- Dark Net

There is a never-ending list of research articles relevant to the aforementioned research questions. To evade any irrelevant literature with similar keywords, research papers were filtered based on the research questions.

1.5 Structure of the Report

Chapter 2 Literature Review offers a brief summary of the relevant literature used as references for this study. It covers the basic facts of ransomware, ecosystem and social structure of cybercrime, and the stakeholders classified by other studies.

Chapter 3 Netnographic Study explains the *Netnography* methodology used in this research.

Chapter 4 Data Collection includes a brief explanation of the strategy used to collect the data, and the type of data that needs to be collected for this research.

Chapter 5 Results and Analysis presents the findings of the dark net observations and empirical analysis on the data collected, including attacker profiles for an attacker model.

Chapter 6 Discussion is a personal reflection of the research process, mentioning the limitations faced and what were the attempts to resolve them.

Chapter 7 Conclusion and Future Work concludes this report with suggestions for future work.

Appendix Includes interviews of dark net members extracted from external sources [17], excerpts of leaked conversations between dark net and additional screenshots from the dark net.

2

LITERATURE REVIEW

Research on the financial and organizational aspects of the cybercriminal communities involved in the development and distribution of ransomware was not prevalent in the academic community prior to this study. However, previous studies on the ecosystem of cryptomarkets and their economic prospects are a relevant source of reference for this research. Other reads included studies on the financial incentives of cybercrime. In this Chapter, these studies have been summarized and the most important findings and research methods are highlighted.

2.1 Cybercrime Ecosystem

According to the European Commission, the term *cybercrime* can be defined as "*criminal acts committed using electronic communications networks and information systems or against such networks and systems*" (European Commission [22]). What differentiates cybercrime from any other crime is that it is *computer-mediated*, i.e. the crime is committed with the use of a software or electronic device.

As cybercriminal offences continue to evolve and more sophisticated branches of cyber attacks begin to emerge, it becomes difficult to identify the nature of the crime, and prosecute the perpetrators accordingly. The rate at which criminals are prosecuted is very slow compared to the growth of cybercriminal offences. In current practice, organized criminal groups can be distinguished into three categories in [13, 22]:

- **Traditional organized criminal groups:** Crimes facilitated with the use of ICT components e.g. identity theft
- **Organized cybercrime groups:** Crimes committed solely online e.g. Banking fraud
- **Ideologically and politically motivated criminal groups:** These groups use internet platforms to incite terrorism and violence or spreading of illegal content

Traditional organized and ideologically and politically motivated criminal groups have been going on long before the commercialization of the internet. Thanks to the anonymity feature of the dark net, these groups are now more actively involved in the cyber space than ever before. The dark net offers a safe environment for members of all the three groups to communicate and exchange ideas and thoughts. The ecosystem in which these cybercriminals perform their activities has proven to be resilient [12, 51]. Taking down a server that hosts the illegal activity will not be an obstacle for these cybercriminals, they will instead migrate to other organized groups.

It is essential to identify the core elements of the cybercrime ecosystem to understand the reason behind its ability to tolerate any external disturbances such as exit scams, or arrests made by law enforcement. The core elements are provided by Kraemer-Mbula et al. [35] and listed as follows:

- International value chains (networks) which link activities and actors
- The changing capabilities that underlie the ecosystem
- The business models that arise from the changing capabilities and concomitant innovations and strategies

For the rest of this section, each element is mapped to concepts introduced in previous cybercriminal research. The global value chain inhibited in modern day cybercrime can be illustrated by classifying the stakeholders. The capabilities of these stakeholders are based on the social structure and how individuals with different levels of skill interact with each other. Lastly, the business model is drawn based on a defined framework for cost-benefit analysis on cybercrime.

2.1.1 Stakeholder Classification

The actors involved in the underground economy have different responsibilities and expose themselves to different types of risks. Several research papers have modelled value chains that illustrate the roles involved and the direction of communication and responsibility. In 2007, Zhuge et al. [59] modelled the underground economy by distinguishing the individual actors involved in the underground market economy of China. Their measurements indicated a direct link to public virtual assets such as video games. The model presented is not specific to China but could also be extended to other countries.

The underground value chain was also further enhanced with the inclusion of the type of other roles that facilitate the process of attaining specific services and products such as the design of a faux website [57]. Figure 2.1 shows the general mapping of the value chain of Chinese underground economy created by Yip [57]. The diagram does not conform to a particular threat modelling technique, but simply defines the flow of demand and potential influence among members. The traditional organized criminal groups are only involved in activities that involve physical interaction. The remaining roles are distinguished into several organized cybercriminal groups.

Yip [57] states that the underground economy has a chain of needs that are satisfied by the different skills each group offers. The chain of needs differs based on the type of good and service being offered. An example presented was that of carding services, i.e. credit card frauds. A carder first requests from the *bank data stealer* to commit identity theft. The bank data stealer hires a *malware author* to create a malicious software that can steal confidential data from a device. To distribute the malicious software across multiple devices, a *botnet herder* is asked to employ a series of botnets for malware installs. Once the data has been attained and offered to the carder, the money stolen from the malware victims is transferred or cashed out with the help of a *mule* or *drops*. The term *drops* is also used for individuals that send or receive mail with illegal products such as drugs or guns and weapons.

Another stakeholder classification of the underground economy was presented by Cárdenas et al. [11]. No value chain was provided in this research and most roles mentioned are included in Figure 2.1. One additional role was identified as *Malware Distributors* who use exploit tools to search for vulnerable devices [11]. The identified incentives can be financial, ideological, political or accustomed to an online pedophile rings [13]. However, cybercriminals today have more financial incentives than political or ideological. This mainly stems from the lack of employment opportunities or low income wages [36].

For this research, the focus is centered around the spread of ransomware via the means of the dark net. Including other services such as carding or distribution of game login accounts is irrelevant to the research questions imposed in Chapter 1. The list of responsibilities provided in Table 2.1 include the roles mentioned in the three studies and are tightly coupled with this research.

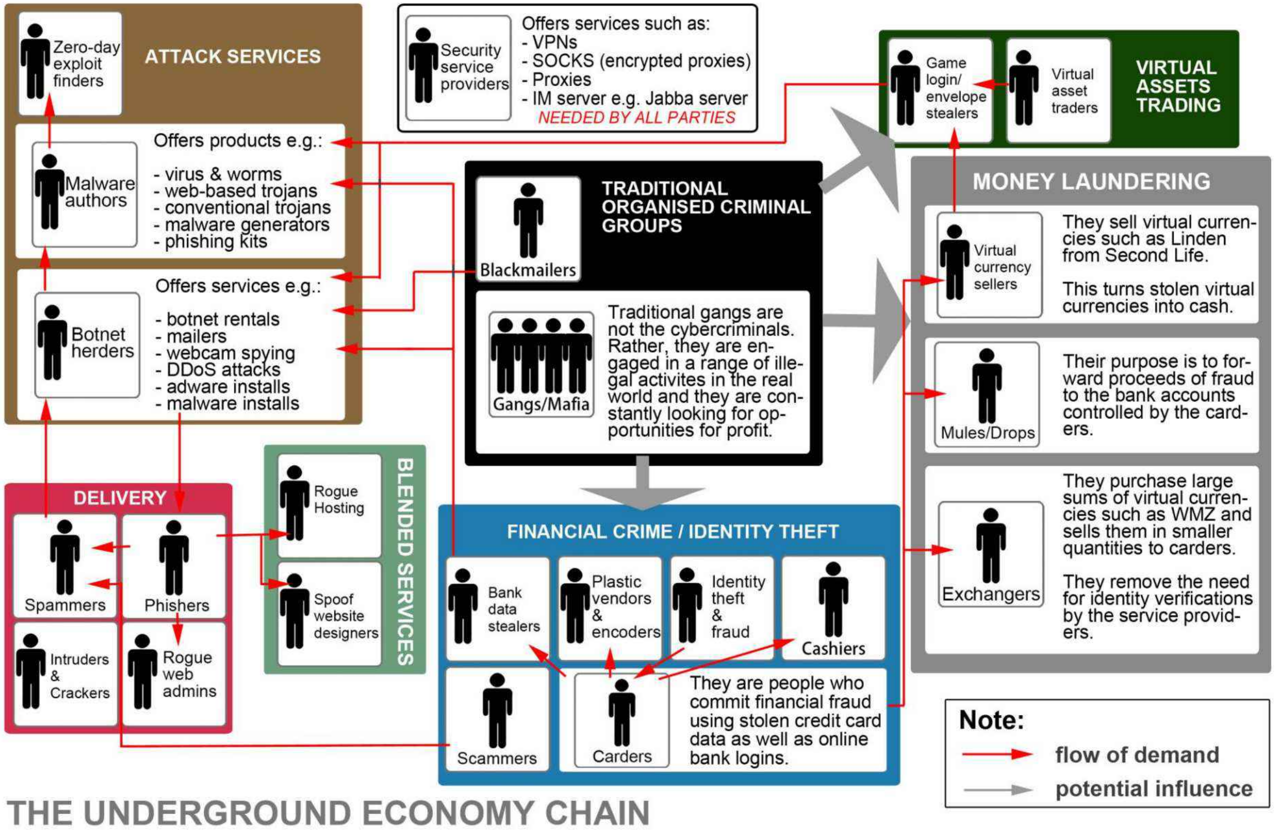

ATTACK SERVICES
Zero-day exploit finders
Malware authors
Offers products e.g.:
- virus & worms
- web-based trojans
- conventional trojans
- malware generators
- phishing kits
Botnet herders
Offers services e.g.:
- botnet rentals
- mailers
- webcam spying
- DDoS attacks
- adware installs
- malware installs
Security service providers
Offers services such as:
- VPNs
- SOCKS (encrypted proxies)
- Proxies
- IM server e.g. Jabba server
NEEDED BY ALL PARTIES
TRADITIONAL ORGANISED CRIMINAL GROUPS
Blackmailers
Gangs/Mafia
Traditional gangs are not the cybercriminals. Rather, they are engaged in a range of illegal activites in the real world and they are constantly looking for opportunities for profit.
VIRTUAL ASSETS TRADING
Game login/ envelope stealers
Virtual asset traders
MONEY LAUNDERING
Virtual currency sellers
They sell virtual currencies such as Linden from Second Life.
This turns stolen virtual currencies into cash.
Mules/Drops
Their purpose is to forward proceeds of fraud to the bank accounts controlled by the carders.
Exchangers
They purchase large sums of virtual currencies such as WMZ and sells them in smaller quantities to carders.
They remove the need for identity verifications by the service providers.
DELIVERY
Spammers
Phishers
Intruders & Crackers
Rogue web admins
BLENDED SERVICES
Rogue Hosting
Spoof website designers
FINANCIAL CRIME / IDENTITY THEFT
Bank data stealers
Plastic vendors & encoders
Identity theft & fraud
Cashiers
Scammers
Carders
They are people who commit financial fraud using stolen credit card data as well as online bank logins.
Note:
flow of demand
potential influence
THE UNDERGROUND ECONOMY CHAIN

Figure 2.1: Stakeholder mapping of the underground economy chain as presented by Yip [57]

Actor	Description
Zero-day exploit finders	Also known as *Vulnerability Researchers* [11]. Responsible for discovering zero-day vulnerabilities and selling information about the exploit to others who can write the exploit code
Malware Authors	These individuals extend what has been presented by the vulnerability researchers. They are professional full-time developers that manage to create the malware that takes advantage of an exploitation. They market they release their malware in online discussion boards. There is also a fierce competition between malware authors [57].
Malware Distributors	The distributors mainly look for computers with the vulnerabilities needed for the malware to work. Vulnerable devices can be identified either by probing the network or employing web-based malware through emails or faux websites (*spamming and phishing*). The latter requires more sophisticated technical skills and costly resources such as C&C servers [11].
Website Designers	They are the administrators of websites that attempt to attract users to download the malware. They also try to take advantage of well-known websites with vulnerabilities.
Botnet Herders	They compromise computers to create a network of bots or botnet. Once compromised, these bots receive commands from a C&C server to
Rogue Hosting	Provide hosting services on bulletproof services to reduce the risk of getting caught [11].
Money Mules / Drops	Transactions received from victims are transferred through an intermediary. This intermediary can either be *innocent*, forwards the funds unknowingly or *professional* who is clever enough to obscure their identity in the process.
Exchangers	Exchanging large sums of cryptocurrency to the local currency can alarm authorities of a suspicious attempt. Exchangers own verified accounts and use their immunity to offer currency exchange services to cybercriminals.

Table 2.1: Modelling of individual actors in the cybercrime economy

Actor Profiling

The method used to model the underground value chain in Figure [57] does not mention factors that provide a basic profile for the actors involved the distribution of cybercrime. The estimated attacker behaviour can be applied to an attacker profile template. Templates have attributes/properties that characterize the attackers. A suitable example of an attacker profile template is proposed by (Irwin [31]). It offers a detailed list of characteristics such as attacker intent and objective that can help assume a unique persona for every actor. The characteristics are listed as follows:

- *Unique ID*
- *Name:* Standardized name for the attacker
- *Description:* General characteristics of the actor
- *Relationship:* The actor either has an external or internal relationship with an organization
- *Region of Operation:* The geographic position of the actor and their activities
- *Motive:* The actor may have a specific motive or no motive
- *Intent:* The actor's intent may be deliberate, malicious, competitive or accidental reasons
- *Capability:* Technical strength and skills of the actor
- *Target Victim:* The type of the industry/individual targeted by the actor
- *Action:* Description of the tools and methods of the attack used by the actor
- *Target Asset:* Assets the actor tries to obtain such as intellectual property
- *Objective:* The ultimate goal of the actor

2.1.2 Social Structure

Empirical studies on communication channels among members of the cyber criminal communities demonstrate their social structure. Hackers that cause substantial damages are tightly packed, thus, are efficient in obtaining tools and resources acquired to initiate an attack. Members can also easily improve their skills through peer-to-peer reviews. Holt et al. [29] identified network structures among hackers that facilitate information sharing among members. With that being said, the sociograph shown in Figure 2.2 supports two important findings presented by Holt et al. [29]:

- Highly skilled actors are more popular; they are most likely to know one another, or at least have mutual acquaintances
- Low-skilled hackers outnumber high skilled members and have fewer connections in the network

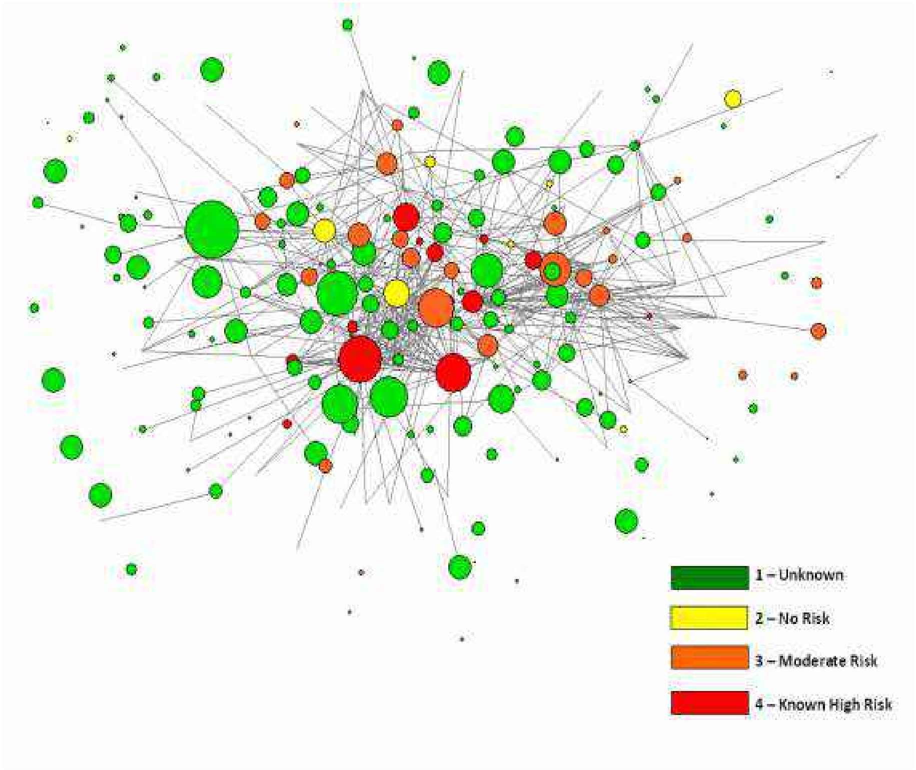


Figure 2.2: Sociograph for connectivity and centrality of the hackers based on skills [29]

The communication media among members are standardized and follow a common practice. Europol has listed two types of online communications experienced by a cyber criminal. When information is exchanged, both communications use Pretty Good Privacy (PGP) encryption methods to cipher the messages and avoid their identities getting leaked.

Criminal-to-criminal communications

Members involved in the creation and distribution of malicious software use different methods to exchange information. According to (Holt et al. [28]), communication practices differ from one community to another based on their local preferences. Russian members use Internet Relay Chats (IRC) or forums to communicate whereas Turkish peers use instant messaging methods and email.

Criminal-to-victim communications

These communications initiate the distribution of malware across several devices. The most common of them being spam email with an infected file attached to it. Social engineering remains a popular method as well, in which a victim is manipulated to install a malicious file or software.

2.1.3 Method of Interaction

The actors in our model might use different modes of communication. Communication channels also differ from one region to another. The main hub of conversation takes place in the dark net. The dark net is a subset of the deep web, a non-indexed segment of the web that cannot be accessed with commercial search engines. The deep web is not only an internet hub that obscures illegal activities. It can also be beneficial for businesses to perform extensive research on their consumer base due to its enormity Obreja et al. [46].

Websites that are similar in structure to online shopping sites, sell illegal goods and services such as narcotics and intellectual property. These websites can go by the name of Dark Net markets/marketplaces, underground markets or cryptomarkets. For the sake of simplicity, the rest of this report will refer to them as cryptomarkets. A popular example of a market place was Silk Road, which received a massive media attention when the administrator of the website, Ross Ulbricht, was arrested. There is evidence that these marketplaces have resilient capabilities ([51, 12]). The business model of Silk Road helped other markets to be created by different administrators such as Silk Road 2.0, Sheep Marketplace, Agora and Hansa to name a few. In Sutcliffe and Vogus [52]'s research, resilience is dependent on two critical conditions:

- Exposure to threats, stress or adversity
- Achievement of positive adaption despite the presence of stress

The following technologies cover the aforementioned dependencies:

- Anonymous internet browsing using the Tor and Onion network
- Cryptocurrencies such as Bitcoins and Monero
- Escrow
- The vendor feedback system as used by commercial e-shopping websites

The first condition is achieved if all activity is performed in the dark net. Users of these marketplaces choose to be active on the platforms because risk is mitigated on several levels [51]:

- There are no physical interactions
- Superior anonymity is guaranteed, reducing risk of getting tracked down by law enforcement intervention
- Financial risk is avoided through the escrow system which are also adopted in eBay and Amazon [1]

However, it is important to mention that the last point might not always be promising. In December 2013, 7 months after the launch of Sheep Marketplace, a vendor who was active on the site discovered a vulnerability and decided to steal 5400 Bitcoins from the ongoing

[1] Escrow: A contractual agreement in which a third-party in a transaction disburses money until the product or service has been shipped

transactions in the site. Marketplaces are suitable for selling the final ransomware product. Making arrangements with other important roles requires a greater level of anonymity and stricter regulations for access. Dedicated communication channels for members within a enclosed organization do not offer access to the general public unless recommended by someone internal.

Based on the mapped model in Table 2.1, we can extract four basic activities in the cybercrime value chain resulting in the creation and distribution of ransomware:

- Discovering zero-day vulnerabilities
- Development of malicious software
- Distribution through exploitation
- Retrieving ransom money

Cybercriminals are naturally successful and confident of their attempts to extort, exploit and steal from their victims. There is no point of interaction with the victim, hence, lack any sympathy for the harm caused. Victims, on the other hand, lack technical knowledge and skill to defend against cybercriminal attacks. Corporate businesses even fail to report an attack for fears of negative publicity. As Cárdenas et al. [11] adds, the reasons for not reporting a cybercriminal attack are:

- Financial market impact
- Reputation
- Damages to the brand of the company
- Legal concerns
- Reporting could increase the potential of getting attacked by other cybercriminals
- Inability to share information
- Fears of job security by the people responsible for securing the businesses systems
- Lack of jurisdiction action

Other victims prefer to comply with the demands of the cybercriminals because it is easier and quicker to get access back to their computers [23].

2.1.4 Business Models

The profit margin is a cost-benefit analysis of an economy. Profit margin analysis on cybercriminal activities has been done before but no study has focused on the economy of ransomware-as-a-service. The business of cybercrime offers monetary benefits for very little risk or costs. The gross margin is also high in countries with high unemployment rates and lack legal action (Kshetri [36]). In this case, cybercrime becomes a free-lancing profession with a very rewarding income.

Analysis of the monetary benefits of cybercrime over its costs have been done in contrast with other traditional organized offences. Although the costs incurred in cybercrime are far less exorbitant since there is little to no physical interaction and thus any physical exposure is eliminated. Other cybercrimes such as trafficking credit cards require individuals called *Drops* to transfer and receive fraudulent cards.

The mathematical model of traditional organized criminal offences can be reused in cybercriminal offences. In criminology, the choice Equation 2.1 was presented by Probasco and Davis [48]. The equation itself is generic and is used by economists to quantify how cybercriminals weigh the costs and benefits [36]. The development and distribution of ransomware-as-a-service may contain additional incurred costs and possibly more factors that augments revenue. These costs and factors is the expected outcome of this research.

$$M_b + P_b > O_{cm} + O_{cp} P_a P_c \tag{2.1}$$

- M_b Monetary benefit of committing a crime.
- P_b Psychic benefit of committing a crime.
- O_{cm} Monetary opportunity cost of committing a crime.
- O_{cp} Psychic opportunity cost of committing a crime such as feeling of guilt.
- P_a Probability of apprehension for a specific time.
- P_c Probability of conviction for a specific crime.

Globalization and technology make it difficult to define and measure cybercrimes. The internet has provided the means for cybercriminals to massive productivity gains without the fear of getting caught. The costs differ from one type to cybercrime to another. Credit card fraud requires a *drop* to record a list of stores that have cashiers that do not pay attention to the legibility of the card. Scamming with illicit and fraudulent bank emails require hosting services and botnets.

One method of decomposing the costs of a cybercrime is to look at the literature used t measure the costs from a victim's angle. Anderson et al. [4] decomposed the costs of a cybercrime on the victim. A framework was devised to visualize the different costs categories incurred on the victim in Figure 2.3.

The framework uses a straightforward approach to determine the costs, which makes it possible to alter and switch the roles from victim to criminal. Since the goal of this research is to determine a cost-benefit analysis of the underground economy of cybercrime, using the same concepts presented in this framework can help decompose the actual costs of incurred.

Criminal Revenue

Criminal revenue includes the money paid by the victim to the cybercriminal. For example, the ransom money received by victims to regain access to their device is in fact a from of revenue. The criminal revenue in the framework is considered as part of the

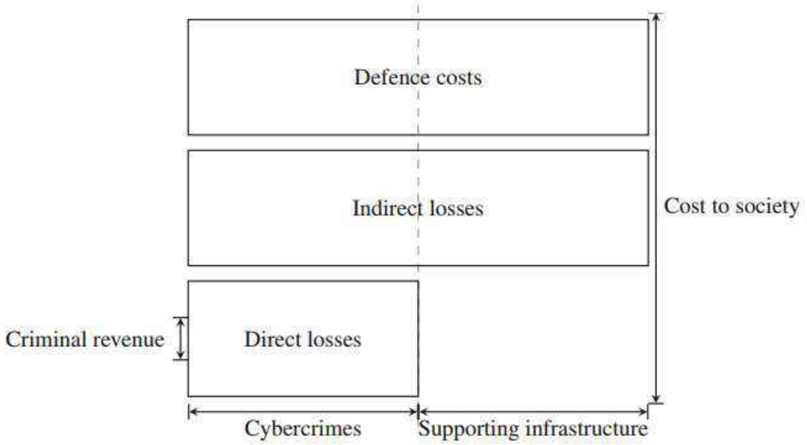


Figure 2.3: Framework for cybercrime cost analysis [4]

direct loss induced on the victim. In the case with cybercriminals, however, this should be distinguished as a source of income.

Direct Losses

According to Anderson et al. [4], direct losses include the money withdrawn from the victim. If the direct losses sustained by the cybercriminal is measured, then any service or product that requires money from the cybercriminal is included in the direct loss.

Indirect Losses

Indirect losses represent adversities or decisions taken to combat a specific threat but ended up failing instead. Examples of indirect losses to a victim is lack of effort to patch the computer-systems with anti-malware programs. In the case of cybercriminals, indirect losses can be the cybercriminal’s mistake of revealing an item that could be used by law enforcement to track the identity.

Defence Costs

Defence costs are the security measures taken to avoid a cybersecurity attack. An example is the purchase of anti-virus programs, spam filters etc. A cybercriminal equivalent would be security precautions taken to avoid being caught by law enforcement agencies.

2.1.5 Cybercrime in Developing countries

Cybercriminals share a common incentive, which is to profit as much as possible from illegal activities. Organized cybercriminal gangs have implemented well-devised criminal methods to increase financial gains while obscuring their tracks from law enforcement. Geographic locations can offer leverage based on the country's current financial circumstances and law enforcement potential [37].

High unemployment rates have a direct impact on the choice of individuals to take part in cybercrime. A position in an organized cybercriminal group can offer a rewarding income, with no imposed taxes and no strict work ethical regulations to adhere to. In addition, countries in which encourage students at an early age to take part in STEM courses but do not have enough vacant positions to hire them have an influx of cybercriminal gangs. Two known countries today with such circumstances are Russia and China [37].

Developing countries do not have the adequate resources to fight cybercrimes. Specially when cybercriminals have gained extensive knowledge in hacking services whereas law enforcement can barely strive to arrest traditional criminal gangs. Added to that, officials in law enforcement agencies may be subject to bribes and can favor cybercriminal activity over the law.

2.2 Cryptomarket Research

> *...market-based indicators derived from price information in vulnerability markets have been proposed as alternatives to threat level indicators for their potential of being forward-looking..*
>
> – R. Böhme, *Security metrics and security investment models* [10]

Dark net marketplaces are coined cryptomarkets for their strong dependence on cryptocurrencies as the medium for transactions. Studying cryptomarkets can offer insight on the economy cybercrime. In this section, a detailed description on the history, infrastructure and research findings is explained.

2.2.1 History of Cryptomarkets

Silk Road was the first dark net marketplace that used cryptocurrency as a mode for payment. Before it, other dark net markets were active, but used other methods of payment. The format of the marketplace bears similarities with e-commerce website on the clearnet such as, ebay and Amazon. The homepage, as shown in Figure 2.5, has a list of categories in which a registered member can buy from with Bitcoin money.

Cryptomarkets have highly emerged in the past decade mainly due to the media's coverage of the Silk Road shut down by law enforcement officials and the consequent arrest of its founder Robert Ulrich. The business model of Silk Road was successful and helped other similar cryptomarkets to follow its footsteps. The marketplace administrators made a living off the vendor fees imposed on members wishing to attain vendor status and commission fees imposed as a percentage take from every transaction. The turnover from these cryptomarkets have proven to be high for many of the administrators. [14]'s approximates a 1.2 million USD turnover made since it got founded.

Patterns of resilient behaviour towards external shocks such as arrests or marketplace owner theft have been proved by other research studies [51, 12]. Right after Silk Road was shut down, *Silk Road 2.0* was founded by a different group of administrators. This was also shut down in an investigation coined Operation Onymous. A while later *Silk Road 3.0* was hosted on the dark net. Figure 2.4 shows a summary of the major events.

In some cases, it wasn't the law enforcement that ended the lifetime of a dark net marketplace. The money stored in escrow was sometimes stolen from the administrators that have access to them. These were coined *exit scams*, and have occurred with several of the notable dark net marketplaces. The largest being Sheep Marketplace, when one of the vendors detected a vulnerability in the marketplace and decided to exploit it, stealing all money in reserve worth 12 million US Dollars.

Despite exit scams creating the sense of *Fear, Uncertainty and Doubt* among the dark net community, members of the dark net, or dark netters still persist to use dark net marketplaces. The dark netters are confident with purchasing items on cryptomarkets for the following reasons:

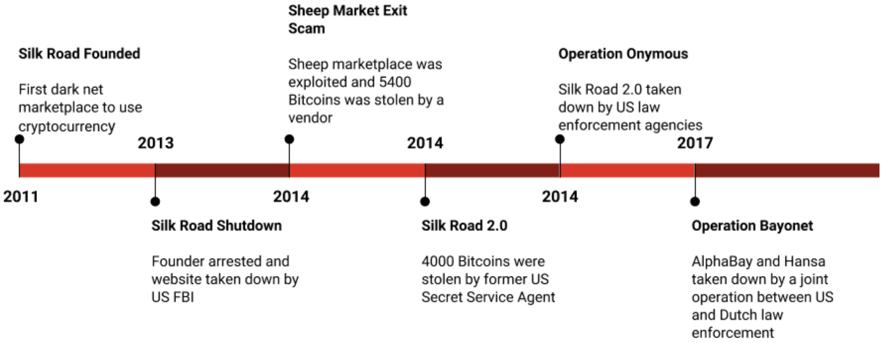

Silk Road Founded
First dark net marketplace to use cryptocurrency
2011
2013
Silk Road Shutdown
Founder arrested and website taken down by US FBI
Sheep Market Exit Scam
Sheep marketplace was exploited and 5400 Bitcoins was stolen by a vendor
2014
2014
Silk Road 2.0
4000 Bitcoins were stolen by former US Secret Service Agent
Operation Onymous
Silk Road 2.0 taken down by US law enforcement agencies
2014
2017
Operation Bayonet
AlphaBay and Hansa taken down by a joint operation between US and Dutch law enforcement

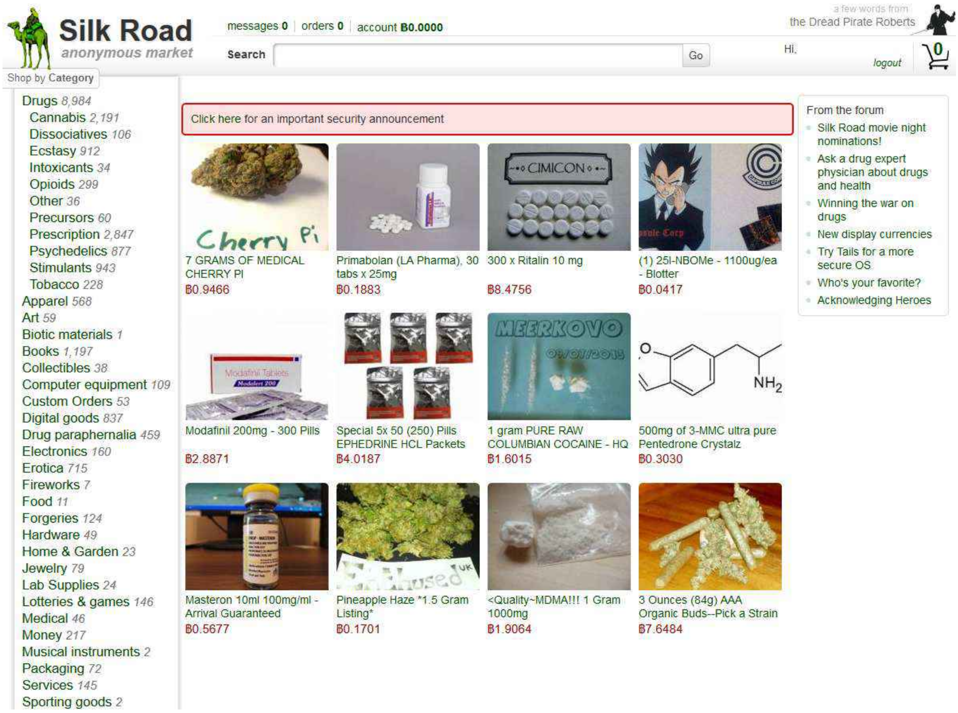
Figure 2.4: Timeline of the major events in cryptomarket history

- Risk is mitigated by other experienced members
- No physical interaction needed to exchange illegal products or services
- A user's identity is concealed
- The use of escrow helps authorize vendors, therefore, maintaining trust among members

2.2.2 Cryptomarket Infrastructure

The start page of a typical marketplace looks somewhat similar to that in Figure 2.5. The infrastructure of marketplaces may differ from one another, but are based on 4 predefined categories. These types of marketplaces are not only limited in the dark net, but can also be observed on the clearnet.

- **Centralized Markets:** Buyers and vendors of a marketplace store their cryptocurrency money in a single wallet owned by the marketplace admins. The users of a centralized market have a high degree of trust towards the administrators, but several marketplaces underwent major scams in which administrators stole money worth millions of dollars. An example of a centralized market is the New York Stock Exchange.
- **Multi-Signature Markets:** Buyers and vendors also store their money in a single wallet, but this wallet is monitored and controlled by at least three different parties. Money cannot be leased from the wallet unless two of the parties approve. In most



Silk Road
anonymous market

messages 0 | orders 0 | account ฿0.0000

Search [ ] Go

a few words from
the Dread Pirate Roberts

Hi,
logout

0

Shop by Category

- Drugs 8,984
  - Cannabis 2,191
  - Dissociatives 106
  - Ecstasy 912
  - Intoxicants 34
  - Opioids 299
  - Other 36
  - Precursors 60
  - Prescription 2,847
  - Psychedelics 877
  - Stimulants 943
  - Tobacco 228
- Apparel 568
- Art 59
- Biotic materials 1
- Books 1,197
- Collectibles 38
- Computer equipment 109
- Custom Orders 53
- Digital goods 837
- Drug paraphernalia 459
- Electronics 160
- Erotica 715
- Fireworks 7
- Food 11
- Forgeries 124
- Hardware 49
- Home & Garden 23
- Jewelry 79
- Lab Supplies 24
- Lotteries & games 146
- Medical 46
- Money 217
- Musical instruments 2
- Packaging 72
- Services 145
- Sporting goods 2

Click here for an important security announcement

7 GRAMS OF MEDICAL CHERRY PI
฿0.9466

Primabolan (LA Pharma), 30 tabs x 25mg
฿0.1883

300 x Ritalin 10 mg
฿8.4756

(1) 25I-NBOMe - 1100ug/ea - Blotter
฿0.0417

Modafinil 200mg - 300 Pills
฿2.8871

Special 5x 50 (250) Pills EPHEDRINE HCL Packets
฿4.0187

1 gram PURE RAW COLUMBIAN COCAINE - HQ
฿1.6015

500mg of 3-MMC ultra pure Pentedrone Crystalz
฿0.3030

Masteron 10ml 100mg/ml - Arrival Guaranteed
฿0.5677

Pineapple Haze *1.5 Gram Listing*
฿0.1701

<Quality~MDMA!!! 1 Gram 1000mg
฿1.9064

3 Ounces (84g) AAA Organic Buds--Pick a Strain
฿7.6484

From the forum

- Silk Road movie night nominations!
- Ask a drug expert physician about drugs and health
- Winning the war on drugs
- New display currencies
- Try Tails for a more secure OS
- Who's your favorite?
- Acknowledging Heroes

Figure 2.5: The home page of Silk Road, the first cryptomarket on the dark net

occasions, its usually the buyer, vendor and marketplace administrator who control the wallet.

- **Decentralized Markets:** As of writing this report, no marketplace has implemented this infrastructure on the dark net. Decentralized markets do not involve centrally controlled wallets, but offers *locality of control* principle [9].
- **Vendor Markets:** Many vendors prefer to sell their products and services in a privately owned website. Depending on the capabilities of the team of vendors and popularity, vendor markets can be a cheaper and more secure option.

2.2.3 Forums

Members of the dark net marketplaces often face with a specific level of uncertainty. When dealing with users that do not reveal their identity, trust becomes a serious issue. The quality of the goods and services marketed on the website can also be questionable. Forums for marketplaces were eventually created to tackle uncertainties of the cryptomarkets [58]. Previous cryptomarket research have highlighted the importance of including forums to the study because of "*how the vivid interaction leads to a closer community bond that heightens the level of trust*" [6].

If we look back to Figure 2.5, on the far right side of the page are a set of links that direct the user to the forum page. Every cryptomarket on the dark net is accompanied with a forum of its own. These forums act as a discussion hub in which a wide variety of issues are addressed. Examples of topics mentioned are reviews of vendors on the cryptomarket. Such topics provide affirmation to users who are interested in a particular item but doubt the quality of the product or service, or is uncertain whether the vendor is a potential scammer and can rip the buyer off.

The infrastructure of forums is simple and bears similarities to the forums on the surface web. However, forums do have strict regulations on what topics can be posted and what opinions and ideas are shared. These are regulated by moderators; assigned members that monitor the activity on the forum and ban members that trespass forum rules.

Generally, forums tied with marketplaces do not allow vendors to market their goods or services on the forum. These are eventually removed by the moderator. If the member has posted several banned posts, the user is eventually barred from the forum. The administrator of the marketplace has the responsibility to assign which member is eligible for a moderator position. A potential moderator must have an extensive experience in the marketplace. The overall hierarchy of the forum is illustrated in Figure 2.6, in which the administrators have the greater control of forum content and userbase, whereas registered members have no control at all.

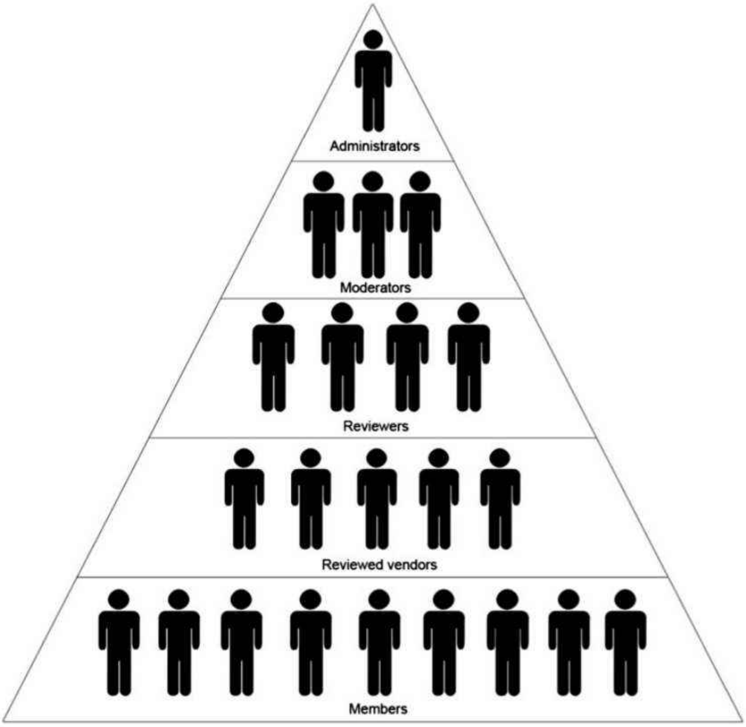


Figure 2.6: Management Hierarchy of a carding forum [58]

2.3 Ransomware

> *...we are unaware of any research which focuses on the strategic economic aspects of the interactions between cybercriminals that distribute ransomware...*
>
> – Laszka et al., *On the Economics of Ransomware* [38]

Ransomware has been in the news recently due to its sudden global outbreak which infected hundreds if maybe thousands of enterprises. Very little research has been found regarding the economy of ransomware. As a matter of fact, new research papers are in the process of getting published, but are not accessible at the time of writing this report. An example would be an study traces the transactions related to the development, distribution and ransom payment of ransomware [30].

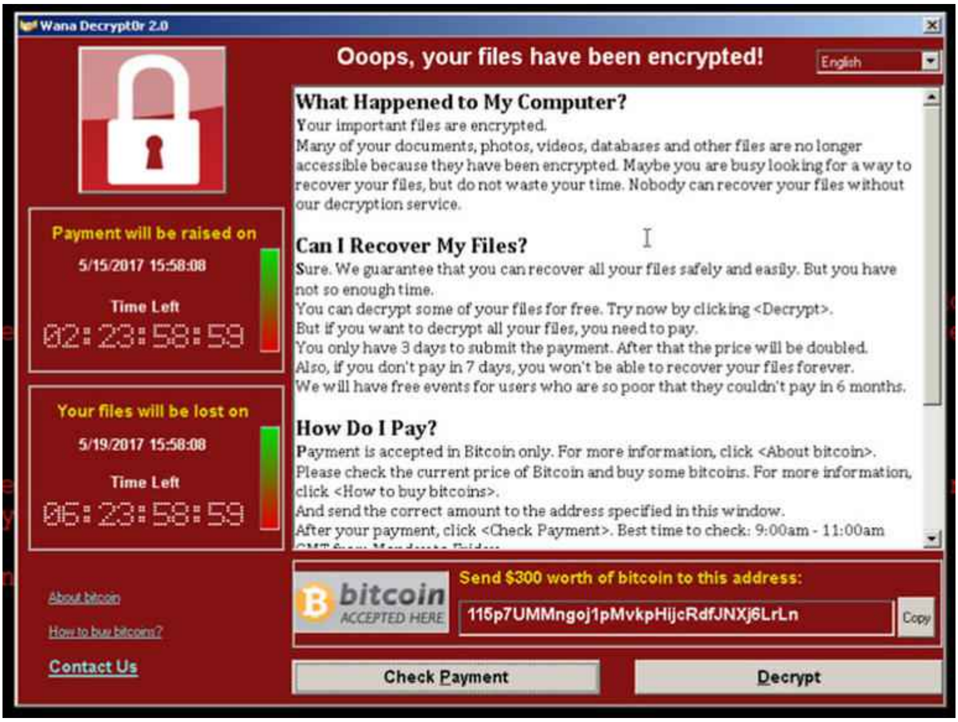
It was, hence, very challenging to deliver a concise literature review on the economy of ransomware. For the rest of this section, the basics of ransomware is covered. With very little emphasis on how ransomware works.

2.3.1 Definition of ransomware

Symantec best describes ransomware as an *extortion racket*; a malicious software that prevents the victim's access to a computer's functionality unless a sum of money is paid [47]. Numerous reports document the increasing widespread of ransomware on an international scale [47], [8]. The most popular type of ransomware is the encryption ransomware which locks the screen and encrypts all files in the victim's computers. The lock screen usually includes a message indicating that all files have been encrypted and the only way to retrieve them back is by paying the ransom. A timer ticking down is also displayed to threaten the victim with the deletion of files if the victim fails to pay before a specific deadline. In most cases, payment of ransom is done through Bitcoins [2]. Figure 2.7 shows the lock screen of the infamous WannaCry ransomware that hit businesses and governmental institutions on a global scale in May 2017 (Ehrenfeld [21]).

Ransomware has proven itself to be a successful threat in cybercrime, ultimately leading to the growth of the ransomware-as-a-service industry on the dark net. Ransomware-as-a-service, or RaaS in short, is a particular type of Software-as-a-Service (SaaS), but offers ransomware instead of software. RaaS can be sold not only by cybercriminals with a qualified skill for coding and hacking, but by criminals with no knowledge of coding (Tuttle [53]).

[2] Bitcoin: A decentralized digital currency



Ooops, your files have been encrypted!

Payment will be raised on
5/15/2017 15:58:08
Time Left
02:23:58:59

Your files will be lost on
5/19/2017 15:58:08
Time Left
06:23:58:59

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Figure 2.7: Message revealing that a computer has been infected by the WannaCry ransomware

2.3.2 Ransomware characterization

Ransomware may apply similar cryptosystems such as RSA and AES, but varients differ in the way they encrypt files on a disk. In 2012, a number of 16 different ransomware variants were identified (O'Gorman and McDonald [47]). By 2014, there were 99 unique variants after a huge increase of ransomware families between 2012 and 2015 (Kharraz et al. [32]). Ransomwares are categorized into different families. This categorization is set based on the factors listed in Table 2.2.

There other minor characteristics that may be included in the ransomware package. These characteristics do not offer a wide range of options such as the aformentioned ones, but they are either included or not. The following are to name a few:

- Deletion of files
- Customization
- Theft of intellectual property

Factor	Description
Encryption Mechanism	According to Kharraz et al. [32], ransomware samples can use either customized or standard cryptosystems. Standard cryptosystems are provided by the underlying operating systems platform e.g. Windows. The reason why cybercriminals will prefer customized cryptosystems is to reduce both the risks of getting tracked down or the chance of retrieving the encrypted files
Method of Payment	From a cybercriminal perspective, the payment made by the victim should not be traced back to the recipient and that the it can be easily to exchanged to the local currency [32]. Cryptocurrencies today have proven to secure both considerations and thus, has been used as the method of payment in most cases. However, methods such as prepaid online payment systems or cards are also comment in modern day ransomwares.
Price listing	The amount of ransom set by the cybercriminals can be a fixed price, or an amount that fluctuates based on a number of factors. Hernandez-Castro et al. [27] claims that the price is tailored based on the *victim's willingness* to pay, size and quantity of files encrypted, or use machine learning techniques to categorize victims into either home or corporate users. Price is also tailored to a country's ability to pay.
Vulnerability Exploited	Ransomware kits exploit specific vulnerabilities. According to Lee and Lee [39], the most common vulnerabilities stem from Adobe Flash, Internet Explorer and Microsoft Silverlight. These vulnerabilities have a price, and cybercrimials usually go for the cheaper for greater monetary rewards.

Table 2.2: Characterization factors of ransomware variants

2.3.3 Ransomware timeline

The first ransomware dates back to 1989. At that time, it was not a malware attached to an email that was sent out to a random set of users. but instead a floppy disk infected by the malware was sent out in the actual mail. Once of a victim inserted the floppy disk to their own computer, all the files are locked and the screen is replaced with a message calling for a ransom to be paid. Back then, the method of encryption used symmetric cryptography which was easily reversible. Advanced encryption methods in the 90s were not easily accessible due to strict regulations placed by the government. For a cryptovirus to be implemented, it had to be made by a crypto expert. Post-1998, and OpenSSL is distributed across the network. Cryptographic libraries can be easily integrated in the malware made by the criminals. Most modern day ransomware use Advanced Encryption Standard (AES).

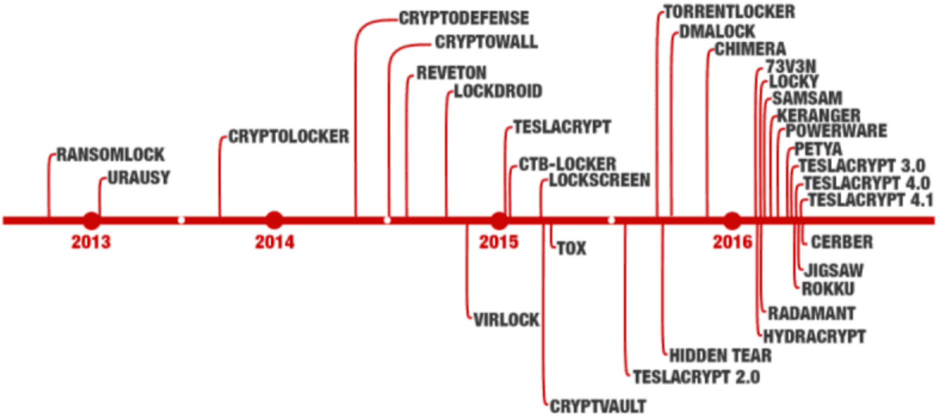


Figure 2.8: Ransomware tubemap presented by [50]

2.3.4 Ransomware Economy

Economic incentives from developing and distributing ransomware are high, simply because the revenue is high, whereas the costs of resources and probability of apprehension are low. From the perspective of a cybercriminal, optimizing financial gains have a very high priority. Spreading ransomware may be profitable, but the victim does not necessarily pay the ransom. The victim could also not necessarily be an individual or a small business, but could be a large enterprise that is willing to pay, but the ransom was placed at a low bet. With that being said, micro-managing the spread of ransomware with respect to the victim's ability to pay is very effective in increasing financial gains.

Researchers have previously deduced economic models on the profitability of ransomware. Like a threat model, an economic model can be asset-centric, software-centric or attacker-centric. Most papers visited during the literature review were either asset or software centric in which the probable losses of a victim of ransomware or costs of private protection were used as exogenous variables to the model. Since this research questions are more concerned with cost-benefit analysis of selling ransomware on the dark net, mathematical models based on software or assets of the individual are not relevant.

An economic model that was centered around the attacker was presented in [27]. The economics of ransomware was based on the profits attained by cybercriminals when spreading ransomware. One important factor used to reconstruct the presented model was the victim's willingness to pay the ransom. The profit of a cybercriminal can be equated in Equation 2.2.

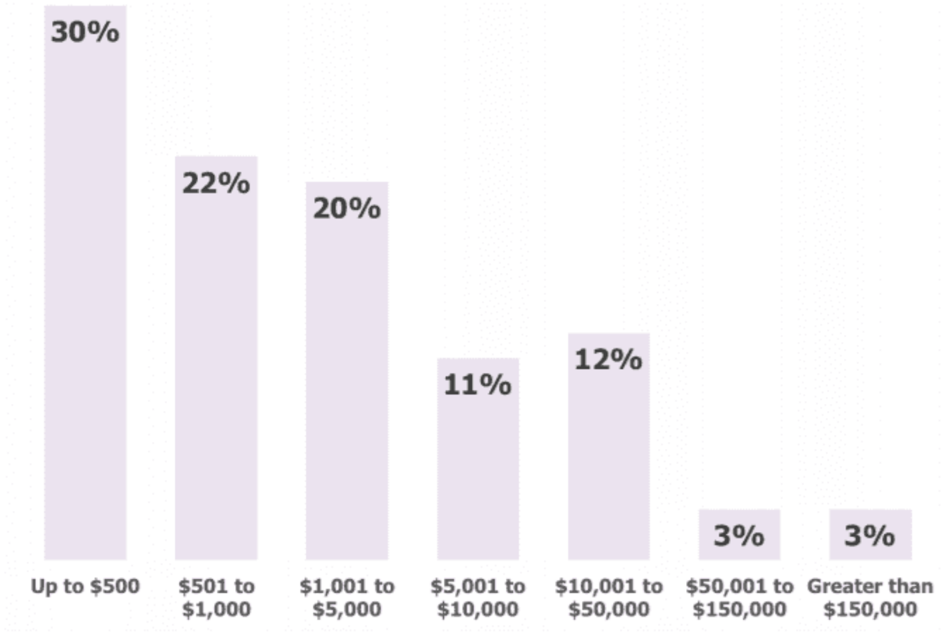
$$\Pi = \Sigma_{i=1}^{N}(p_i - c)1_i - F \tag{2.2}$$

- N is the number of attacked victims.
- p_i is the ransom amount asked by victim i.
- c is the cost of liquidizing the ransom revenue.
- 1_i is an indicator variable that takes value 1 if $p_i \leq v_i$ and 0 otherwise. Where v_i represents the person i's willingness to pay
- F is the fixed cost operating the malware.

The fixed cost F for operating the malware and the cost for liquidizing the revenue c, although not mentioned in the literature, can be equated to the cybercrime costs mentioned in Section 2.1.4.

One important issue worth mentioning is the value of the ransom amount p_i. The ransom amount differs from one variant to another. Figure 2.9 shows the variety of amounts demanded from the victims. The amount for a single ransowmare varient can either be a fixed price for all victims, or fluctuating based on a set of factors. This fluctuation of ransom amount is referred to by [27] as *price discrimination*.

Price discrimination is when the ransom amount of one ransomware variant differs from one victim to another. Perpetrators precisely calculate and code an algorithm to set an amount based on the victim's willingness to pay v_i. This mainly depends on the victim's well-being. For instance, if the victim is from a developing country, the amount is lower than that in a developed country. Another method would be to set a price based on the type of file downloaded. If the victim chose to download a malicious file resembling an expensive software, the ransom amount will be set to high.



Source: Osterman Research, Inc.

Figure 2.9: Amounts demanded by ransomware perpetrators [33]

2.4 Applied Methodology in Dark Net Studies

Research on cryptomarkets and cybercrime either implemented qualitative or quantitative methods. The study on Silk Road markets written by Bakken [6] used netnography to understand drug markets and the social structure of marketplaces. On the other hand, Christin [14] used crawling methods to gather large amounts of data to be analyzed through data visualization.

2.4.1 Netnography

In short, netnography is the ethnography of the online communities on the internet. The expected outcome of a netnographic study is an understanding of how members of the community behave and communicate with each other. The researcher immerses his/herself in the community and attempts to interact and experience the environment. Empirical analysis are based on reflexive field notes recorded by the researcher throughout the experience.

Most studies that implemented the netnographic methodology, were examining social media communities on the surface web. Upon searching for netnographic studies on the dark net, only one research paper was listed. The study was concernced with the social and hierarchial structure of the Silk Road Market [6]. No cost-benefit analysis was made on the observations, but interprets the social structure of the users and administrators of the Silk Road marketplace and forum as a rhizomatic structure.

The study presented by Bakken [6] only focused on drug trafficking in the Silk Road market and analyzed the findings from a philosophical angle. Although this research has different goals, the methodology satisfies one of the requirements listed in the research question.

2.4.2 Crawling Mechanisms

Crawling is an automated method of iterative parsing through webpages while indexing and storing them accordingly. Crawling hidden services on the dark net is not new. Several of the papers included in the research review used crawling mechanisms to retrieve data and apply their empirical analysis. What differentiates most crawling mechanisms is the implemented algorithm. A recent dissertation claims that the accuracy of a crawl can be optimized by combining different algorithms [25]. Other studies have used commercial software to assist them with retrieving data from the dark net. For this section, we look into the mechanism used, and not the algorithm.

Crawling a marketplace for an uninterrupted period of time minimizes the likelihood of missing out a vendor action such as changing the price of an item. Prior to crawling any hidden service, there are specific requirements that need to be addressed. First and foremost, the issue of anonymity and security. Crawling for long periods of time can signal a red flag as a DDoS attack to the marketplace administrators. It is best advised to pause the crawling software/algorithm for a period of 3 days to avoid being caught by the administrators [20]. To gain access to the items sold in a marketplace, one must create an account and login the marketplace.

The methodology presented by the literature differs from one case to another. Some have crawled the dark net with the assist of a software [14], or have written their own scraping code, or have used other open source scraping code in the project. For the rest of this section, a brief explanation of the methods used will be presented along with the choice of crawling mechanism for this research.

HTTrack

HTTrack is a website mirroring software and an offline browser. It copies the infrastructure of the website, thus, the downloaded content can be browsed offline. The software itself is open source and free to download and use. Crawling with HTTrack can be time and space consuming considering that it also downloads the images and the advertisements. In [20], HTTrack was adjusted to crawl text only and omit any images for time efficiency. In [14], HTTrack was not automated to crawl periodically, but crawled Silk Road once No additional coding or complicated configuration needs to be setup before running a crawl on HTTrack. This makes it very simple to use and little time is needed to go through the documentation and understand its functionality.

Custom Crawlers

Research similar to Demant et al. [18] and Ceci et al. [12] have developed custom crawlers to fit their research goals. Several open source crawling algorithms on Github and other source code sharing platforms can be used to extract information specifically from the dark net. One popular dark net scraper is Fresh Onions TOR Hidden Service Crawler which crawls the dark net to find new hidden services and URLs [19]. A Tor website uses this algorithm to retrieve as many hidden links as possible and scans its availability. It is not practical to use this algorithm to crawl content from a specific Tor page, but the hidden service hosted on the Tor network is useful to search for the availability of hidden services. Lastly, it is important to mention that scripts written in python on a virtual OS running Tor comes with its own risks.

Data Dumps

Some research use open source data provided by other researchers. In dark net studies, that would be Gwern Branwen [26]. Gwern Branson, a freelance researcher has provided crawled data of 89 different marketplaces between 2011 and 2015. The downloaded data totalled approximately 60 Gigabytes in size and offered HTML pages. This data sounds promising for this research, however, it has some faults. Most marketplaces offer DDoS protection through Captchas. The captchas were sometimes asked randomly during the crawls and would block entry when it failed to solve. Therefore there are instances in which a blocked page was crawled instead of true content. Added to that, Gwern crawled the websites without images to save time and space. Images could add to the empirical analysis.

In conclusion, crawling can be a useful method for triangulation of cryptomarket records with the netnographic observations. Crawling data can also be used as a backup in cases of a sudden *external shock* in which the data cannot be retrieved from its source again. Creating a custom crawler can be time consuming, and so it is best if HTTrack was installed and used for this research. Added to that, the data dumps opens the door to the past of dark net marketplaces.

3

NETNOGRAPHIC STUDY

Netnography is a qualitative research that involves the researchers visual perception and reflections of a community of users active on the internet. According to Kozinets [34, p 243], the five common practices in netnographic research are the following:

- Netnography involves participant-observation
- Netnography seeks to describe and theorize the human element of online human and technological interaction, social interaction and experience
- Netnography focuses primarily on data collected through the internet
- Netnography adheres to a strict and widely accepted standards of ethical online research
- Netnography always includes human intelligence and insight as a major but not always exclusive, part of data and analysis and interpretation

In this Chapter, a brief explanation of the netnographic framework used in this study with focus on the five common practices. In short, a plan prior to the research is listed along with the important guidelines that need to be adhered to during the study.

3.1 Framework

The outcome of planning a process for the netnographic study was a concise framework that can be applicable to the dark net. The factors that attributed to the framework include the ethical considerations, type of data collected, interaction strategy and representation of findings. The framework was created with the help of Kozinets' proposal of what makes a good netnographic study [34]. It was suitable to use this framework because no other source provided a more detailed plan of how a netnographic study should be devised.

Kozinets' provides a defined set of phases for performing a netnographic study. Some process levels involve immersion within the community and direct interaction among its users. The 12 phases are adequate enough to use in all netnographic study, but considering the time constraint and ethical complications, it will be tough to stick to the proposed plan. What we hope to achieve with these steps is to merely have a basic framework to apply netnography for novice researchers. These stages are listed as follows:

1. Introspection phase where researcher must give thought to the research questions and the expected outcome from the research.

2. Investigation phase where researcher must refine netnographic study based on extensive research

3. Informational phase where ethical considerations must be listed

4. Initial interview phase, users registered in the sites/forums are interviewed to fulfill research on interaction and sociality

5. Inspection of sites to refine application of study on a set of sites based on evaluation

6. Interaction strategy that outlines the extent of the researcher's participation within the selected sites/forums

7. Immersion in the site for several days on a frequent basis

8. Indexing data collection strategy to highlight meaningful aspects of the community

9. Interpretation of collected data for a deeper understanding

10. Iterating several times through the literature, previous findings, research questions etc.

11. Penultimate phase where netnography is instantiated using one of these representations: symbolic, digital, auto or humanist

12. Integration research answers with the research questions

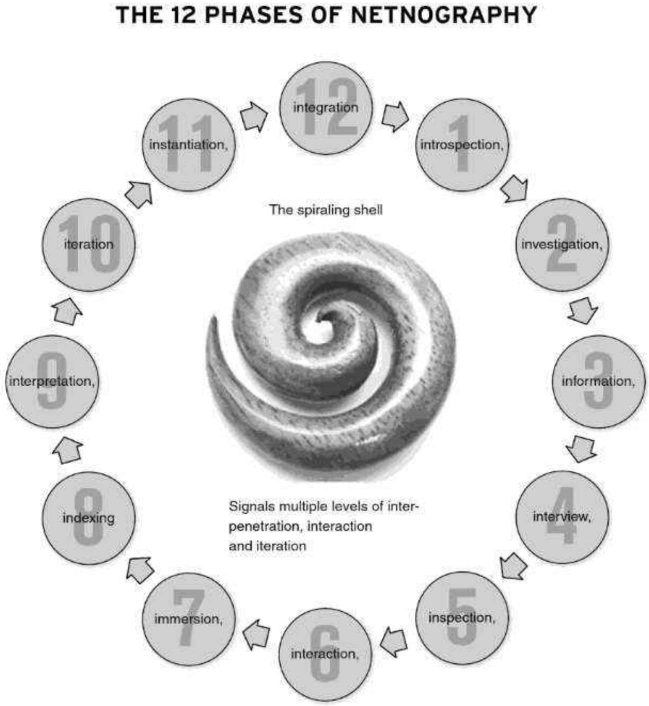


Figure 3.1: The 12-step process of netnography [34]

Time is a vital factor in the aforementioned phases, and unfortunately, there is insufficient amount of time to achieve a proper netnographic study. Many more limitations are expected to decline the pace and quality of the research, therefore, it is important to refer to the approach and outcomes of similar studies. [6] put through a netnographic stud on the notorious Silk Road marketplace before it was brought down by authorities.

3.2 Process

This section explains in detail the phases in the framework and the plan for this research. The last phase has been omitted since its self-explanatory.

3.2.1 Phase 1 and 2: Introspection and Investigation

Introspection is a reflective process in which the researcher defines his/her own understandings prior to performing the research, personal judgments and previous experiences of the study. The purpose of this process is to capture the personality of the researcher and reduce researcher bias as much as possible. Kozinets proposes a three-question exercise in which the researcher is instructed to answer from his/her own personal narrative.

Who Are You? The answer to this question should refer to my personal intellectual curiosity and what unique addition will I present in this research. My intellectual curiosity stems from the secretive attribute of the dark net. Not much is known and my impressions of it is greatly influenced by what is presented by mainstream media.

What Do You Want? A better understanding of dark net content. I would also want to gain awareness of the various activities taking place, the immense number of users partaking in such illegal activities and their social cultures.

Personal Statements The audience for this research are security experts, researchers and law enforcement agencies. The data I am looking for should be useful to accumulate a clear perception of the business model used by participants in the making of ransomware. Collection of data will be done by surfing the different pages of the online markets and searching for relevant topics.

3.2.2 Phase 3: Ethical Considerations

The territory of the internet is vast and involves a wide variety of socio-cultural backgrounds. Research ethics matter and every study has its own principles that researchers must adhere to. Performing a netnographic study on a specific aspect of the internet has its own ethical implications. Kozinets' connects ethics of netnography to that of ethnography despite its differences. However, Kozinets' acknowledges that every netnographic study has its own unique environment and hence, may include a set of complex ethical questions.

In contrast, the dark web offers a variety of ethical complications that vary greatly from that of the surface web. A simple example that supports this claim is that most of the activities that are conducted in the dark web are considered illegal on a global scale. Criminal activities include drug and weapon trafficking to name a few. Immersing oneself for the cause of research can be risky at this stage. Referring to ethical guidelines of dark web research can help place ground rules before beginning the study. The provides a set of guidelines. These guidelines can be categorized in the following key ethical issues:

- Public or private?
- Informed Consent
- Personal data, confidentially and anonymity
- Regard for third parties

The circumstances in regards to the aforementioned issues vary greatly in the dark web. An increasing awareness to the activities supported through the anonymity feature of the dark web has encouraged more researchers to look into the ethical guidelines that pertain to researcher involvement in the dark web. On the other hand, there are difficulties in determining the guidelines as these studies are carried out from different countries and cannot be tied to a specific national jurisdiction [42].

For this research, the ethical guidelines are determined from the Internet Research Ethics presented by the Norwegian National Committees for Research Ethics [24] and the ethical questions presented by Martin and Christin [43]. Both offer examples to what may constitute an ethical complication during a research on the internet.

Research on the dark web comes with a number of ethical questions that need to be addressed, these include:

- What appropriate permissions need to be gained?
- Whose informed consent is needed for the netnographic study of the dark net?
- How involved should we be within the community?
- To what extent should we participate in activities within the community?

The services sold in the markets are publicly posted for all to see. However, the personal identity of the seller is strictly confidential and all sellers go about with their activity using a random pseudonyms. The seller is a suspected perpetrator of a possible crime that may drastically affect organizations huge sums of money and even worst, put people's live at risk if they target health care systems. Asking for a user's permission to be a participant of the research becomes a serious task that needs precaution.

To avoid all possible legal risks that could be imposed, it would be best to avoid any contact with the perpetrators. Data relevant for this research can be collected without any direct interaction. This is stressed by Martin and Christin [43] for two main reasons. Firstly, the research after publication will not be pertinent to any proof for prosecution against any individual. Despite the fact that the collected information can be useful to capture the *bad guys*, it is best advised not to mingle in such affairs. Secondly, there will be no need to ask for permissions because there will be no contact with the participant.

The pseudonyms that these users go by are either altered or not displayed in this report if no permissions will be asked. No data linked to the user's identity or personal background are recorded or used throughout this research.

Ethics of the researcher also needs to be addressed. When the focus of a research is the dark net, the researcher is placing him/herself in the frontier of substantial legal consequences. Restrictions to researcher involvement in the online community must be listed beforehand. As previously mentioned, there is little to no contact with those involved in the making and selling of ransomware. However, in some occasions, the researcher has the opportunity to ask questions in forums and chats in the dark net. In this case, the researcher must not expose the identity of oneself or give out any personal information.

However, other users of the chat or forums must be informed the purpose of the question. The researcher should then publicly announce that there is an ongoing research study, but no more than that. The name of the institution, participants and purpose of research should not be disclosed.

Other general ethical guidelines that are advised to the general public who wish to wander in the realms of the dark net are also applied here. An example would be to avoid or revoke any financial purchases to products and services sold through the dark net. Other instructions can be easily found in common forums that are made for novice users of the dark net with regards to anonymity. Examples range from installing a virtual machine before browsing or using TOR to subscribing to a VPN service.

3.2.3 Phase 4: Interview

The importance of conducting interviews is to study the social interaction experience in an online community in its normal setting. The interview format is flexible and does not conform to a specific structure. However, it is important to address any pre-requirements and eventually design a structure.

Online interviews can take the format of a real-time video conference, instant messaging chats, or even in-person meet-ups. Although the first and the latter are impossible to implement considering that all members of the dark net maintain anonymity, chatting with dark net members on Internet Relay Chats can be the only possible option for an interview. However, the since the identity of the interviewee is concealed, it is impossible to know authorize the role or responsibility claimed by the interviewee. Added to that, dark net members are apathetic to any research made or done about them. In the preliminary study, an attempt to submit private messages to vendors on the dark net was not successful. All vendors failed to respond to any of the messages. The messages included the intent behind asking these questions and were clear enough that the inquiry was for research purposes.

Interviewing dark net members may not be achieved if the research has no experience with dealing in any of the dark net social circles. Fortunately, other researchers and investigative journalists have already provided the public with interviews with different dark net members. Using this as an asset for the netnographic researcher does not only provide information on the strategic roles of dark net members, but it also avoids conflict with ethical implications. Data from interviews can be easily attained with a simple search.

3.2.4 Phase 5: Site Inspection and Evaluation

Inspection and evaluation of sites helps refine the application of netnography to a predefined set of hidden services or .onion websites. The process of distinguishing the useful websites and irrelevant ones was done with the help of selection guidelines specified by Kozinets [34, p.168]. These are listed as follows:

- *Relevant*: The content of the website is related to the research study
- *Active*: The website is constantly updated and is accessible
- *Interactive*: Users regularly post on the website
- *Substantial*: The website has a large userbase

- *Heterogeneity*: The website has a diverse community of participants with a common interest
- *Rich in data*: The website shows richness in data of all sorts of text and media
- *Experiential*: The website offers an experience to the netnographer

A decision matrix was set to compare the different hidden services from each other, and select the websites that satisfy a given threshold. These weight scales for every factor used to rank websites are listed in Table 3.1. The actual table of comparisons is listed in Section 4.2.2.

Table 3.1: Decision Matrix Weighting Scale

Factor	Weight	Description
Relevant	1	Content of the website is irrelevant to the research study
	5	Some content in the website is relevant to the research study
	10	All content in the website is relevant to the research study
Active	1	The website has an uptime status that is less than 50%
	5	The website has an uptime status more than 50% but is slow
	10	The website has an uptime status more than 90%
Interactive	1	There is no user activity in the website
	5	There is some user activity in the website
	10	There is rich user activity in the website
Substantial	1	The website has no registered members
	5	The website has a few registered members
	10	The website has a substantial number of members
Heterogeneity	1	The website only represents one community of common interest
	5	The website represents a few diverse communities
	10	The website has a wide variety of diverse communities
Rich in data	1	The website is not rich in data of all sorts of text and media
	5	The website has some rich data of all sorts of text and media
	10	The website is very rich in data of all sorts of text and media
Experiential	1	The website does not offer an experience to the netnographer
	5	The website offers some experience to the netnographer
	10	The website offers a personal experience to the netnographer

3.2.5 Phase 6: Interaction Strategy

Defining an interaction strategy is the most challenging phase in the framework. The ethical implications, as much as anything, has restricted any proper interaction strategy recommended by Kozinets'. In one example, Kozinets suggests the idea of *NiRWebs*, short for Netnographic Interactive Research Websites. These websites creates an online environs for the users to participate and thus become key informants for the research. An example of an NiRWeb are online forums. They are discussion hubs in which users post questions related to a number of topics within the online community and receive answers from well-informed members. NiRWebs are effortless to make but conflict with the researcher's ethical position. Creating an NiRWeb in the dark net is an act of support for the illegal activities of cybercrime.

However, one option remains feasible and does not interfere with the ethical issues mentioned earlier. The dark net does provide already implement online forums, making it easy for the researcher to simply observe the posts and the answers provided by the forum moderators. It also offers the opportunity for the researcher to post questions that can clear out possible misapprehensions of the dark net community and receive answers from experienced dark net members.

3.2.6 Phase 7: Immersion in the Tor Network

Immersion involves recording of field notes and taking screenshots to support researcher analysis. As far as researcher involvement is concerned, the connection to the Tor Network must be secure and researcher's identity kept anonymous. Accessing the Tor network alone does not guarantee a concealed identity. Extra precautions must be considered when surfing the different .onion websites in the Tor network. A *DoNot* documentation is a relevant source for those who are new to the dark net [56]. An environment setup was created to protect the identity of the researcher and the institution from any harm. The following is a detailed description of the steps taken.

System Settings

It is best advised to access the dark net on a device that does not contain any personal information. For instance, device username, stored files that contain trackable data etc. Therefore, it is recommended that a Virtual Machine (VM) is installed on the device or a USB configured to browse the Tor network.

There are three operating systems that focus on anonymity, privacy and security: *Whonix*, *Tails* and *Qubes OS*. From these three, Whonix was chosen to be the running operating system on an Oracle VM VirtualBox. The *Whonix* wiki offers a concise comparison between the different types of OS with respect to network security, web fingerprint, usability and attacks protection [55]. All are Linux-based, but, only Whonix can run on a VM without additional configurations. Tails is recommended to be used on a Live USB or CD [1], whereas Qubes OS does not work in a VM, but needs to be booted on a separate device. Other commercial operating systems are often frowned upon. Windows, uses key loggers that keep track of the user's keyboard strokes. Cybercriminals can easily acquire secret data such as passwords from these logs. Mac OSX are often unstable as virtual machines.

[1] *Live USB or CD* have a distribution of any operating system that can boot and run when plugged in a device

Tor Browser

The Tor browser is used to access .onion websites on the Tor network. The browser is a modified version of Firefox and can be installed on MacOS, Linux and Windows. However The connection between user's device and the destination is kept *anonymous* but not *pseudonymous*. The *DoNot* documentation defines both these terms and stresses out the differences between the two in Definitions 3.2.6 and 3.2.6.

Definition 3.2.1. Anonymous A connection to a destination server, where the destination server has no means to find out the origin (IP address / location) of that connection nor to associate an identifier (e.g. a cookie) to it.

Definition 3.2.2. Pseudonynous A connection to a destination server, where the destination server has no means to find out the origin (IP address / location) of a connection, but can associate it with an identifier.

To guarantee an *anonymous* and *pseudonymous* connection the following must be configured on a Tor browser:

- Use *Bridges* [2] on Tor to avoid being identified by the Internet Service Provider (ISP).
- Do not use clearnet and Tor at the same time to avoid being spotted by services such as Google Analytics running on the background of a non-anonymous server.
- Do not post sensitive information and or photographs with metadata that includes location of where the picture was taken.
- Maximize the screen size of the virtual machine as some CSS's can retrieve device type from screen width and height.
- Enable the *Forbid Scripts Globally*. Tor can be compromised with a malicious Javascript that can de-anonymize hidden services.

Virtual Private Network (VPN)

A VPN offers a secure connection that is encrypted and are provided through private tunnels that cannot be open for surveillance. VPN does not necessarily anonymous, but it does reinforce privacy and security. Selecting a VPN service was based on DeepDotWeb's comparison chart of the different VPN services [16]. IPVanish was ranked as the best for its anonymous configurations and its support for P2P BitTorrent traffic. However, many seem to argue that IPVanish as a company that headquarters in the USA, must hand in logged data to the NSA and FBI. In the end, there was no other suitable VPN for our needs, and therefore configured the VPN to an IP address in the US.

[2] Tor Bridge relays are non-public alternative entry points

PGP Encrypted Messages

When communicating with members in the dark net, it is best advised to encrypt the content of the messages with PGP (Pretty Good Privacy) before sending it. The encryption program was developed by Phil Zimmerman in 1991 and since then, has been considered the one of the toughest encryption programs. Law enforcement agencies have expressed how difficult it is to decrypt messages that could be useful for prosecution.

Many of the members in the dark net have made it clear that they will not respond to messages if they are not encrypted. Therefore, a public and private hash key was generated to encrypt and decrypt messages in private chat.

3.2.7 Phase 8: Indexing Data Collection

There are three forms of data in a netnographic study:

- Previously recorded and *archival data*. These are data collected from other researchers that are relevant for the interpretation of current social interactions in the online community.
- The researcher's own impression of the social interaction in the online community is labeled as *elicited* or *co-created* data. This includes the researcher experience of surfing the webpages.
- Data created by the researcher is labeled as *produced* data. Reflexive notes are the personal reflections of the researcher upon observing the interactions among community members.

In Chapter 4, the data collection phase is addressed in more detail.

3.2.8 Phase 9: Data Interpretation

Kozinets [34] describes two different ways to interpret the data collected from netnographic study:

- *Analysis* which is breaking phenomenon down into its component parts.
- *Hermeneutics* which is rendering the human aspects of the observations as a whole.

The aim of the data interpretation is to search for feasible answers for the research questions. In reference to *RQ1.2*, the analysis should include a cost-benefit analysis of the sale of Ransomware-as-a-service. The components needed to perform this analysis is the costs inferred on the creation of ransomware and the revenue received.

On the other hand, understanding the nature of activities and incentives in the dark net is best analyzed using Kozinets' proposed hermeneutics. The process involves data contextualization of the forum posts and interview data and using textual analysis tools such as a word cloud generator to decode a given text. The analysis and hermenutics the collected data is presented in Chapter 5.

3.2.9 Phase 10: Iteration

Iteration process involves the reexamination of the concepts and theory mentioned in the literature review, the findings and research questions to avoid getting too absorbed in irrelevant content in the online communities. There was no particular structure for how often this iteration occurred. This phase has a significant impact if the timeline of the netnographic study was longer.

3.2.10 Phase 11: Netnographic Representation

Kozinets [34, p. 244] points out four types of netnography for representation. The types add more to the study and then simply being an observational netnography. Each type represents a research direction. Pre-defining the type of netnographic representation based on the research questions is essential for the design decisions of the results and research observations. The four types are listed in Table 3.2.

Type	Description
Digital	Deployment of digital tools to analyze and visualize the data
Symbolic	The purpose of the netnography is to seek an understanding of how cultures and communities are emerging through on online websites
Auto	Auto-netnography is retrieved from auto-ethnography in which the the study is made on the researcher's own people
Humanist	Hermeneutics is the main methodology behind this representation. Observing the data from

Table 3.2: The four types of netnographic representation

From the four types, the best suited two are *digital* and *symbolic*. The reason behind it is best explained with the help of the diagram in Figure 3.2. The research approach mentioned uses a triangulation of data sources, both crawled data and netnographic observations. This is comparable to the complementary analytic field focus as represented in the diagram.

The crawled data is attained from the deployment of digital tools, consequently, will be represented with the help of visualization tools. The netnographic observations present how the dark net members communicate and interact through forums and other hidden services. Finally, the research is not limited to the researcher's interaction with the community, but also encompasses all members of the online community and is thus global and not local.

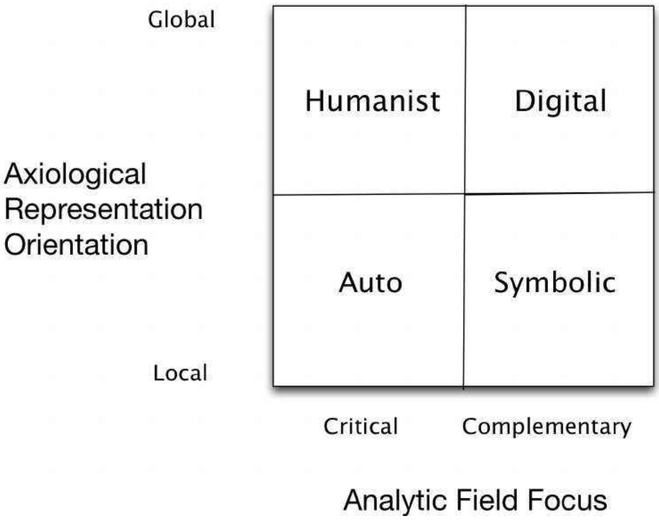


Figure 3.2: The four types of netnographic processes

4

DATA COLLECTION

In theory, there are three types of netnographic data; the **collected**, **co-created**, and **produced** [34]. They conform to two key categories which are **archival** and **communicative**. The collected data is information stored or archived by other researchers or scientists. The co-created data is generated when the research is practiced in the online social environment through communication and elicitation with individuals. The produced data is the output of the researcher's reflections, analysis and interpretation of the co-created data. The form of this data is presented by reflexive field notes solely written by the researcher conducting the netnographic study. This Chapter will focus on every form of data, describing how and where was the data collected from.

4.1 Archival Data

Archival data includes data collected by previous research studies and are relevant to the scope of this research. The data can be useful to compare trends and statistics over time. Researcher immersion in this study was limited to two months scouring the dark net marketplaces. Having data collected for several years can give a better researcher perspective and input on the dark net ecosystem with respect to unpredictable events, also known as *external economic shocks*.

Common examples of external shocks include the take down of Silk Road in Operation Onymous and the exit scam of Sheep Marketplace in which a vendor exploited a vulnerability and stole approximately $ 6 million worth of Bitcoins. These incidents show indications of a ripple effect across other cryptomarkets and online communities active on the forums. Figure 4.1 shows previous research on the sales volume of cryptomarkets across 7 different cryptomarkets. The consequences of Silk Road's takedown and Sheep's exit scam among other external shocks can be easily noticed on first glance.

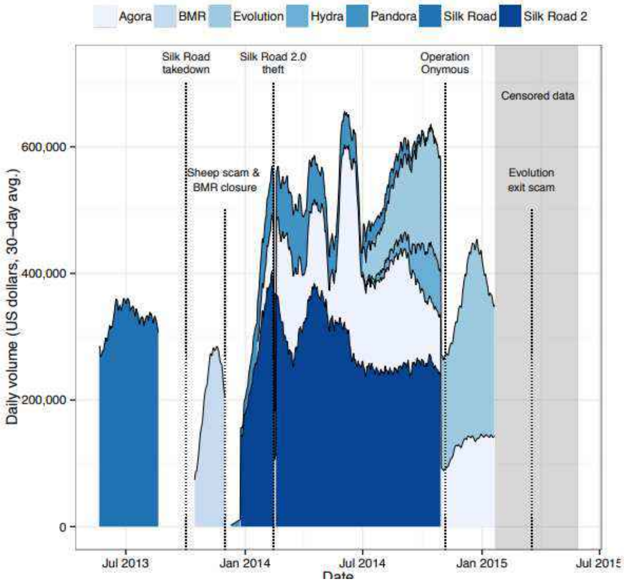


Figure 4.1: The sales volume of 7 cryptomarkets between July 2013 and July 2015 [51]

Defining the type of historical data depends on the research questions addressed in Chapter 1. To assess the economic impacts of ransomware-as-a-service, the revenue volume needs to be measured first. Information relating to the costs of developing ransomware and price listings of digital good items on cryptomarkets for previous years can be easily retrieved from internet repositories.

Gwern Branwen, a freelance researcher has uploaded the largest data set of cryptomarket activity [26]. This particular repository includes approximately 55 GB worth of data scrapped from over 89 different cryptomarkets and 37 forums between the years 2011 and 2015.

Years 2016 and 2017 were retrieved from another data dump provided by Michael McKenna and Sigi Goode [44]. It does not cover a wide variety of cryptomarkets and only focuses on AlphaBay's item listings and buyer feedbacks in early 2017.

The last dataset retrieved was uploaded by Sarah Jay Lewis, and it includes item listings and buyer feedback for 2 marketplaces on October and December 2016 [40]. These marketplaces are Hansa and Valhalla and while Valhalla is still active at the time of writing of this report, Hansa was taken down along with AlphaBay in Operation Bayonet in the summer of 2017.

Gwern's data set of 89 marketplaces and 37 forums also includes a substantial number of deactivated marketplaces such as AlphaBay and Hansa. Searching for cryptomarket data dumps was concluded after finding valid and useful datasets. Other datasets were either focused on insignificant items such as drugs and narcotics or their validity was questionable.

Historical data was not limited to previous data dumps of cryptomarkets, but also included researcher participation of previous studies. Unfortunately, most studies conducted on the dark net were not concerned with the ransomware-as-a-service but the ecosystem of cryptomarkets that were mainly focused on drug trafficking and other inconsiderable items. Added to that, a common limitation addressed by most researchers is their involvement in the closed social circles of the dark net. High ranked forums and marketplaces acquire references from members or a payment of a large sum of cryptcurrency. In this case, information concerning skilled dark net members was retrieved from individuals that had strong connections and that was not difficult to find. A team of experts on the dark net have published a news website that mainly concerns dark net activity. That website, called *DeepDotWeb*, includes articles, interviews with dark net members and statistics of cryptomarkets and forums. It also hosts a Q&A forum that is open for the general public. The interviewed dark net members are cryptomarket administrators, vendors, former dark net carders, or developers to name a few. Their most popular interview which gained attention from journalists was with the developers behind the RaaS *Tox*.

DeepDotWeb: What is Tox?

Tox Developers: We developed a virus which, once opened in a Windows OS, encrypts all the files. Once this process is completed, it displays a message asking to pay a ransom to a bitcoin address to unlock the files.

DeepDotWeb: How do I make money with Tox?

Tox Developers: You can subscribe (no mail or other shit needed) and create your virus. You will have to decide the ransom to unlock the files. Once you have downloaded your virus, you have to infect people (yes, you can spam the same virus to more people). How? That's your part. The most common practice to spam it as a mail attachment. If you decide to follow this method be sure to zip the file to prevent antivirus and antispam detection. The most important part: the bitcoin paid by the victim will be credited to your account. We will just keep a 30% fee of the income, so if you specify a 100$ ransom, you will get 70$ and we'll get 30$, isn't this fair?

DeepDotWeb: Are you serious?

Tox Developers: Yes, why not? This is the best way for us to infect a lot of people and make a lot of money.

DeepDotWeb: Am I safe?

Tox Developers: Sure, as long as you use tor and don't use personally identifiable information: we don't need to know you, and you don't need to know us. The only thing we'll ask you is the bitcoin address to withdraw your part.

DeepDotWeb: Are you going to steal my profit?

Tox Developers: Nope, why should we? The best way for us to make money is having you helping us.

DeepDotWeb: Then why aren't you spreading the virus yourself?

Tox Developers: We are! But with you, we're going to have a bigger income.

DeepDotWeb: Why is the file a .scr?

Tox Developers: Because in this way people will not suspect anything (who knows what is a .scr?). If you wish, you can change it to .exe it'll work the same.

DeepDotWeb: How does the virus look?

Tox Developers: Sexy. The virus has a .src extension (same as .exe files) and it has the icon of a word document, so the victim wont be suspecting anything.

DeepDotWeb: Will you actually decrypt the files once the ransom is paid?

Tox Developers: Yes, we will. We want people to trust us, so that more people will pay the ransom.

DeepDotWeb: How do I withdraw the money?

Tox Developers: In the virus section you can monitor the status of all your viruses. When you have bitcoins to withdraw, just enter your address and press the Withdraw button

4.2 Communicated Data

Communicative data is information retrieved from researcher participation in the dark net. Before all, a set of websites need to be predefined for research immersion. Searching for websites was the first step, then refining the list of websites to a limited set of Kozinets provided a set of guidelines to refine the list of websites based on a number of factors. Once listed, accessing these websites had to be taken with extra precaution for security and privacy reasons.

There are three different communication platforms that are the center of focus in this research:

- **Marketplaces:** Websites made for dark net members to exchange illegal goods and services with cryptocurrency
- **Forums:** Discussion hub for dark net members. Users exchange reviews on vendors, tips to survive the dark net and experience sharing.
- **IRC Chats:** (Internet Relay Chat) messaging system used between individuals and teams to instantly communicate with each other. Users create channels and add or remove other users to that channel.

4.2.1 Site Search

The sites were gathered from different sources available on the dark net. These include, Reddit, Deep Dot Web and DNStats. Prior to 22nd of March 2018, Reddit offered several subreddits that offered posts concerning dark net marketplaces and activity. These subreddits also offered advice for people are new to the dark web. The advice would cover important matters such as how to access the dark web, installation procedures, security requirements to avoid getting caught etc. By the end of March 2018, Reddit began banning all dark net marketplaces in an attempt to crackdown on illegal activity or any activity that supports illegal activity. However, Reddit was not a major field site for this research, and was only acquired to retrieve the onion links of the most popular dark net marketplaces.

Another useful website was DeepDotWeb. It offered an extensive list of all the cryptomarkets with their onion URLs, user rating and a short description. If a cryptomarket was taken down, it will listed as a *Dead Market*. Some cryptomarkets were taken down by law enforcement agencies, but others were from other hackers, exit scams or an unknown reason.

4.2.2 Site Selection

Dark net websites that have URLs ending with *.onion* were refined based on a selection criteria prior to the netnographic study. This puts more focus on the research goals by defining boundaries for the search field.

Based on the factors mentioned in Phase 5: Site Inspection and Evaluation in Chapter 3, a decision matrix was set with the weighted rankings to select the top 3 cryptomarkets and top 3 forums. The list of cryptomarkets and forums was retrieved from DeepDotWeb list of top dark net websites. The decision matrix for marketplaces and forums are listed in Tables 4.1 and 4.2 respectively.

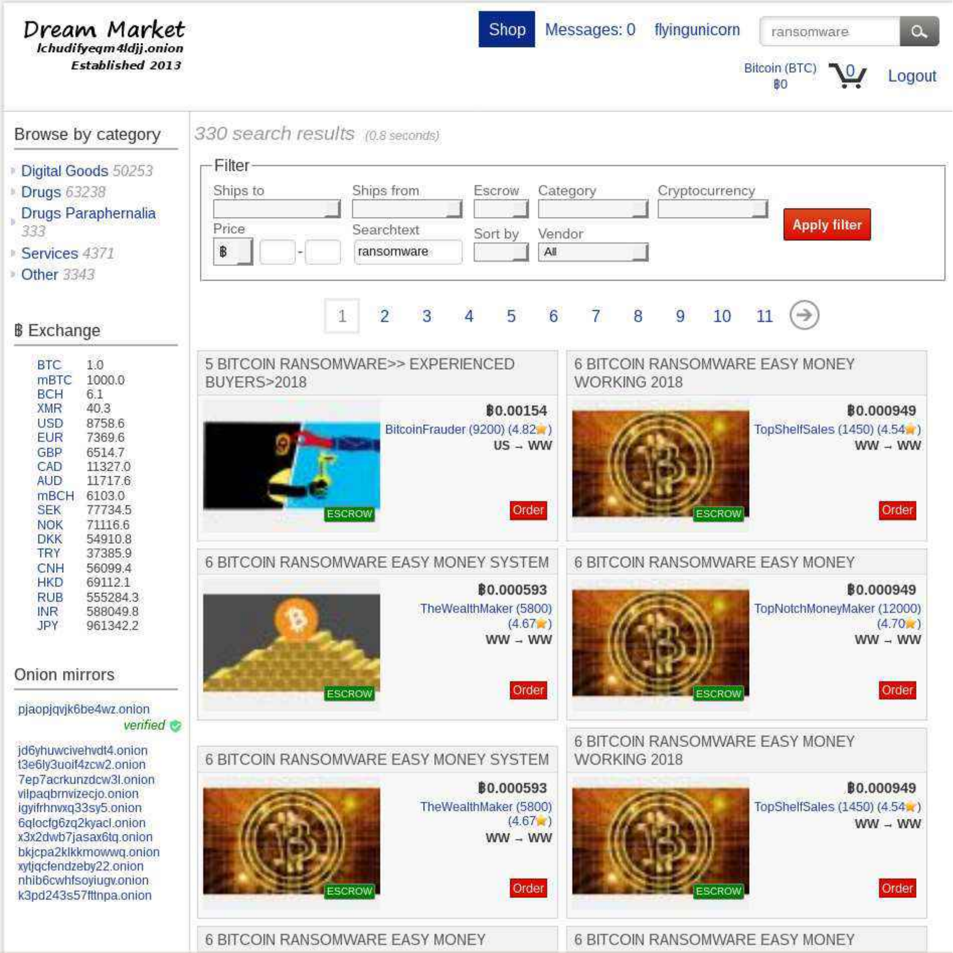
Site/Factors	Relevant	Active	Interactive	Substantial	Heterogeneity	Rich in Data	Experiential	Average
Dream	10	10	10	10	10	10	5	9.29
Wall Street	10	10	10	10	10	10	5	9.29
Berlusconi	5	5	5	5	10	10	5	6.43
Point Tochka	1	10	10	10	5	5	1	6.00
Olympus	5	5	5	5	5	5	5	5.00
Rapture	5	5	1	5	1	1	5	3.29
Cannazon	1	5	5	5	1	5	5	3.86

Table 4.1: Selection of the top 3 cryptomarkets

Site/Factors	Relevant	Active	Interactive	Substantial	Heterogeneity	Rich in Data	Experiential	Average
OnionLand	10	10	10	10	10	10	10	10.00
Hidden Answers	10	10	10	10	10	10	10	10.00
The HUB	5	10	10	10	10	10	5	8.57
DNM Avengers	1	10	5	10	5	5	5	5.86
IntelExchange	5	5	5	5	5	5	5	5.00
Dread	1	10	5	5	1	1	5	4.00

Table 4.2: Selection of the top 3 forums

Dream Market



Dream Market
lchudifyeqm4ldjj.onion
Established 2013

Browse by category

- Digital Goods 50253
- Drugs 63238
- Drugs Paraphernalia 333
- Services 4371
- Other 3343

฿ Exchange

BTC	1.0
mBTC	1000.0
BCH	6.1
XMR	40.3
USD	8758.6
EUR	7369.6
GBP	6514.7
CAD	11327.0
AUD	11717.6
mBCH	6103.0
SEK	77734.5
NOK	71116.6
DKK	54910.8
TRY	37385.9
CNH	56099.4
HKD	69112.1
RUB	555284.3
INR	588049.8
JPY	961342.2

Onion mirrors

pjaopjqvjk6be4wz.onion
verified

jd6yhuwcivehvdt4.onion
t3e6ly3uoif4zcw2.onion
7ep7acrkunzdcw3l.onion
vilpaqbrnvizecjo.onion
igyifrhnvxq33sy5.onion
6qlocfg6zq2kyacl.onion
x3x2dwb7jasax6tq.onion
bkjcpa2klkkmowwq.onion
xytjqcfendzeby22.onion
nhib6cwhfsoyiugv.onion
k3pd243s57fttnpa.onion

330 search results (0.8 seconds)

Filter
Ships to:
Ships from:
Escrow:
Category:
Cryptocurrency:
Price: ฿ -
Searchtext: ransomware
Sort by:
Vendor: All

5 BITCOIN RANSOMWARE>> EXPERIENCED BUYERS>2018
฿0.00154
BitcoinFrauder (9200) (4.82★)
US → WW
ESCROW
Order

6 BITCOIN RANSOMWARE EASY MONEY WORKING 2018
฿0.000949
TopShelfSales (1450) (4.54★)
WW → WW
ESCROW
Order

6 BITCOIN RANSOMWARE EASY MONEY SYSTEM
฿0.000593
TheWealthMaker (5800) (4.67★)
WW → WW
ESCROW
Order

6 BITCOIN RANSOMWARE EASY MONEY
฿0.000949
TopNotchMoneyMaker (12000) (4.70★)
WW → WW
ESCROW
Order

6 BITCOIN RANSOMWARE EASY MONEY SYSTEM
฿0.000593
TheWealthMaker (5800) (4.67★)
WW → WW
ESCROW
Order

6 BITCOIN RANSOMWARE EASY MONEY WORKING 2018
฿0.000949
TopShelfSales (1450) (4.54★)
WW → WW
ESCROW
Order

6 BITCOIN RANSOMWARE EASY MONEY

6 BITCOIN RANSOMWARE EASY MONEY

Figure 4.2: Screenshot of a search on ransomware on *Dream Market*

Dream Market began in late 2013. Reviews on DeepDotWeb show general approval and support of the website. Its average rating exceeds 4 out of 5 stars. It has been under DDoS attacks, but administrators were successful to regain access of their market with the help of mirror links. Dream market received a great number of new users when AlphaBay and Hansa was taken down. The products sold on this cryptomarket varies from illegal drugs to digital goods such as carding services. RaaS items are not substantial, but many exploit kits used to make ransomware is sold. Figure 4.2 shows a screenshot of a RaaS search on the marketplace.

At the start of this research, Dream Market was properly functioning and was preferred more than other marketplaces because it was not slow and offered similar content. It also integrated a new feature that encourages more vendors to register profiles. For every vendor profile, the vendor's AlphaBay ranking was listed. This ultimately provided the vendors the chance to maintain the high reputation they have gained even after a marketplace was shutdown. Buyers, on the other hand, would base their vendor trust not only on the Dream market rating but also the previous rating on AlphaBay. It is unclear how this was managed, whether the administrators were in contact with the AlphaBay moderators or not has not been confirmed by any authentic resource.

Dream Market's popularity rose when AlphaBay was shutdown in Operation Bayonet. Figure 4.3 shows the ratio of registered users across time (van Wegberg et al. [54]). A spiked increase in the number of registered users begins mid-July, when Operation Bayonet was successful.

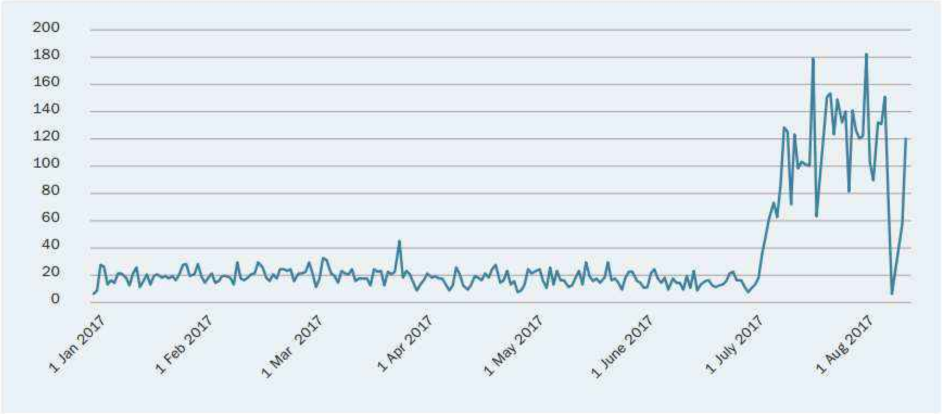
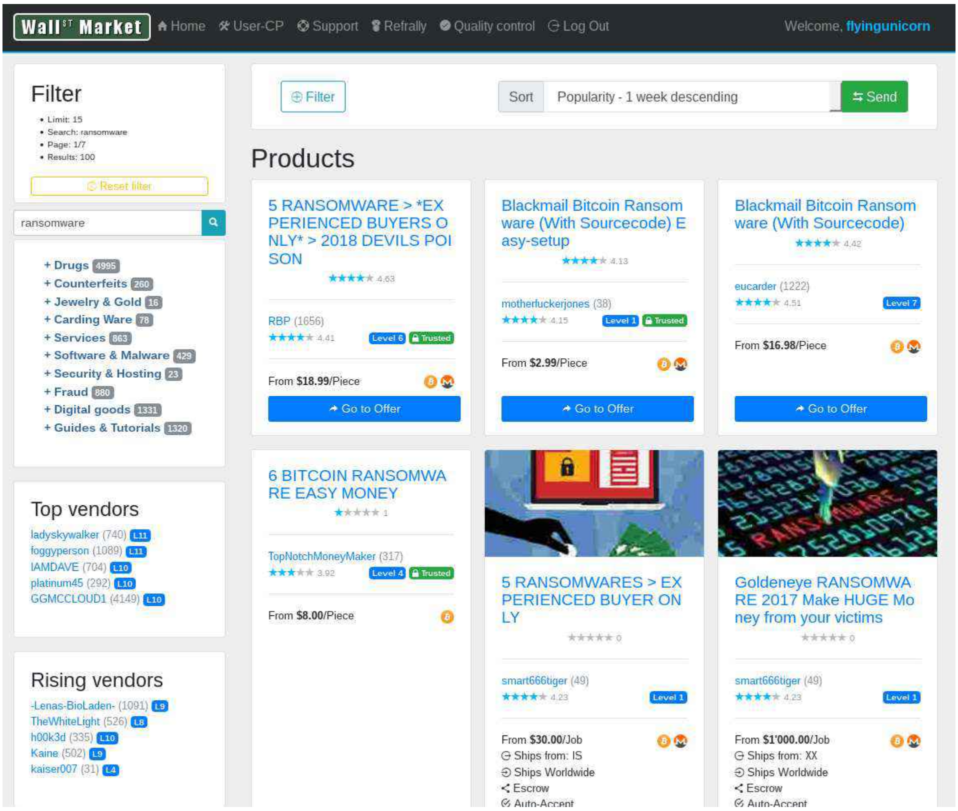


Figure 4.3: The sharp increase of registered users on Dream Market after AlphaBay has been shutdown [54]

Wall Street Market

Another popular marketplace is Wall Street Market. It has a reputation similar to that of Dream, but on many users have complained that it sometimes has a slow loading time. It ranks high in anonymity and security because it offers Multisignature transactions, and PGP encrypted login. It has multi-lingual support and is available in English and German. Aside from Bitcoin, it also accepts Monero, but some vendors may choose to define the purchase to a particular cryptocurrency.



Welcome, flyingunicorn

Filter

- Limit: 15
- Search: ransomware
- Page: 1/7
- Results: 100

ransomware

- + Drugs 4995
- + Counterfeits 260
- + Jewelry & Gold 16
- + Carding Ware 78
- + Services 863
- + Software & Malware 429
- + Security & Hosting 23
- + Fraud 880
- + Digital goods 1331
- + Guides & Tutorials 1320

Top vendors

ladyskywalker (740) L11
foggyperson (1089) L11
IAMDAVE (704) L10
platinum45 (292) L10
GGMCCLOUD1 (4149) L10

Rising vendors

-Lenas-BioLaden- (1091) L9
TheWhiteLight (526) L8
h00k3d (335) L10
Kaine (502) L9
kaiser007 (31) L4

Sort: Popularity - 1 week descending

Products

5 RANSOMWARE > *EXPERIENCED BUYERS ONLY* > 2018 DEVILS POISON
★★★★★ 4.63
RBP (1656) ★★★★★ 4.41 Level 6 Trusted
From **$18.99**/Piece

Blackmail Bitcoin Ransomware (With Sourcecode) Easy-setup
★★★★★ 4.13
motherfuckerjones (38) ★★★★★ 4.15 Level 1 Trusted
From **$2.99**/Piece

Blackmail Bitcoin Ransomware (With Sourcecode)
★★★★★ 4.42
eucarder (1222) ★★★★★ 4.51 Level 7
From **$16.98**/Piece

6 BITCOIN RANSOMWARE EASY MONEY
★★★★★ 1
TopNotchMoneyMaker (317) ★★★★★ 3.92 Level 4 Trusted
From **$8.00**/Piece

5 RANSOMWARES > EXPERIENCED BUYER ONLY
★★★★★ 0
smart666tiger (49) ★★★★★ 4.23 Level 1
From **$30.00**/Job
Ships from: IS
Ships Worldwide
Escrow
Auto-Accept

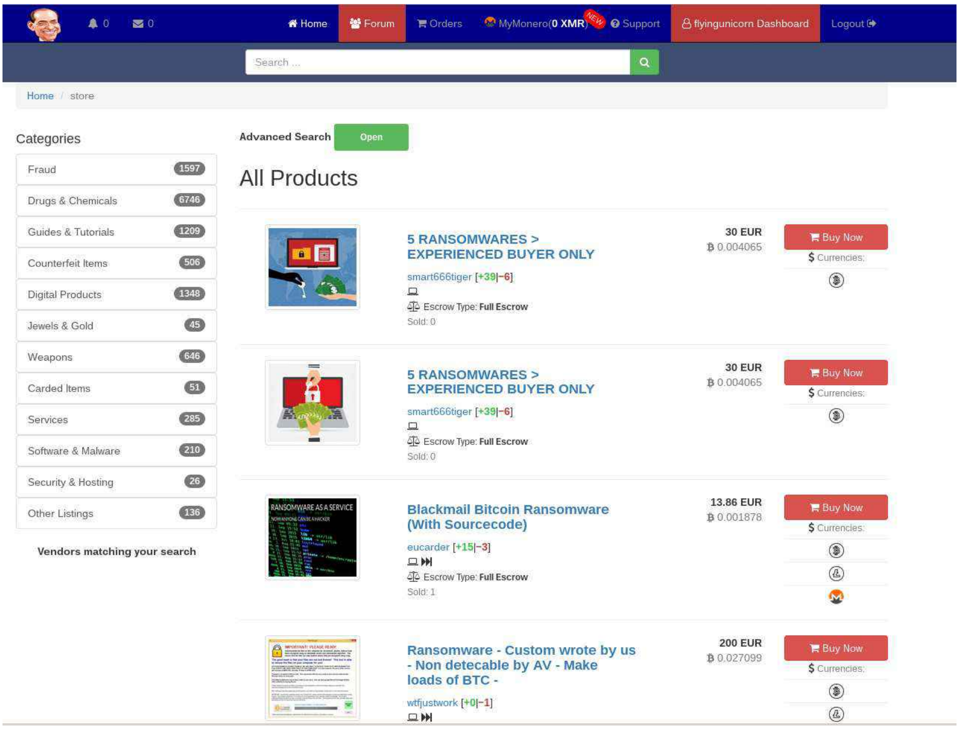
Goldeneye RANSOMWARE 2017 Make HUGE Money from your victims
★★★★★ 0
smart666tiger (49) ★★★★★ 4.23 Level 1
From **$1'000.00**/Job
Ships from: XX
Ships Worldwide
Escrow
Auto-Accept

Figure 4.4: Screenshot of a search on ransomware on *Wall Street Market*

The variety of goods sold on Wall Street Market range from drugs and hash to carding services. Services related to cyber threats and trading of intellectual trading are offered on Wall Street. Most of the bots and malware services are RaaS, and some of the security software are paid tutorials on how to become a hacker or how to develop exploitative code for beginners.

Berlusconi Market

Berlusconi is a small marketplace that is growing quickly with an expanding userbase. Drug and narcotics dominates in the list of categories with the number of items. It also promises users with security against scams with the help of escrow services. However, being a small market does have its troubles. Some users complain that support by the administrators is slow and, in some cases, fail to reply to their complaints. These users have openly expressed their frustration in the comments on DeepDotWeb. Figure 4.5 shows a search on the RaaS items on the marketplace. Prices are listed in Euros but purchases of items can be done with the help of Bitcoin and Monero.



Categories

Fraud	1597
Drugs & Chemicals	6746
Guides & Tutorials	1209
Counterfeit Items	506
Digital Products	1348
Jewels & Gold	45
Weapons	646
Carded Items	51
Services	285
Software & Malware	210
Security & Hosting	26
Other Listings	136

Vendors matching your search

All Products

5 RANSOMWARES > EXPERIENCED BUYER ONLY
smart666tiger [+39|−6]
Escrow Type: Full Escrow
Sold: 0
30 EUR
฿ 0.004065
$ Currencies:

5 RANSOMWARES > EXPERIENCED BUYER ONLY
smart666tiger [+39|−6]
Escrow Type: Full Escrow
Sold: 0
30 EUR
฿ 0.004065
$ Currencies:

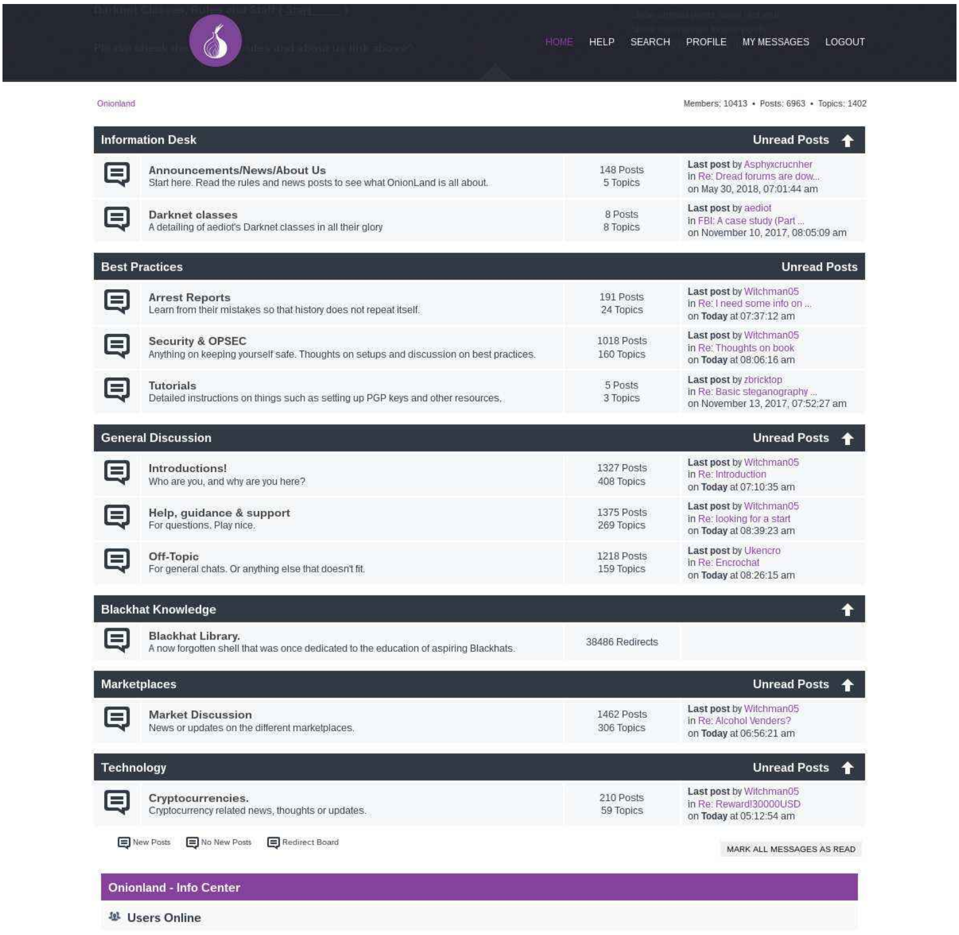
Blackmail Bitcoin Ransomware (With Sourcecode)
eucarder [+15|−3]
Escrow Type: Full Escrow
Sold: 1
13.86 EUR
฿ 0.001878
$ Currencies:

Ransomware - Custom wrote by us - Non detecable by AV - Make loads of BTC -
wtfjustwork [+0|−1]
200 EUR
฿ 0.027099
$ Currencies:

Figure 4.5: Screenshot of a search on ransomware on *Berlusconi Market*

OnionLand Forum

OnionLand is one of the prominent forums that are currently active and rich in content. The moderators of the forum claim to have an experience in dark net activities and are very responsive to questions posted on the forum. The highest ranked moderator on the forum has created a set of classes or tutorials for new dark net members or members who are trying to improve their survival strategy in the fierce competition against other vendors. What makes this forum unique and useful for this research the interactive environment and the relevance of the posted tutorials.



Members: 10413 • Posts: 6963 • Topics: 1402

Information Desk		Unread Posts
Announcements/News/About Us Start here. Read the rules and news posts to see what OnionLand is all about.	148 Posts 5 Topics	**Last post** by Asphyxcrucnher in Re: Dread forums are dow... on May 30, 2018, 07:01:44 am
Darknet classes A detailing of aediot's Darknet classes in all their glory	8 Posts 8 Topics	**Last post** by aediot in FBI: A case study (Part ... on November 10, 2017, 08:05:09 am

Best Practices		Unread Posts
Arrest Reports Learn from their mistakes so that history does not repeat itself.	191 Posts 24 Topics	**Last post** by Witchman05 in Re: I need some info on ... on **Today** at 07:37:12 am
Security & OPSEC Anything on keeping yourself safe. Thoughts on setups and discussion on best practices.	1018 Posts 160 Topics	**Last post** by Witchman05 in Re: Thoughts on book on **Today** at 08:06:16 am
Tutorials Detailed instructions on things such as setting up PGP keys and other resources.	5 Posts 3 Topics	**Last post** by zbricktop in Re: Basic steganography ... on November 13, 2017, 07:52:27 am

General Discussion		Unread Posts
Introductions! Who are you, and why are you here?	1327 Posts 408 Topics	**Last post** by Witchman05 in Re: Introduction on **Today** at 07:10:35 am
Help, guidance & support For questions. Play nice.	1375 Posts 269 Topics	**Last post** by Witchman05 in Re: looking for a start on **Today** at 08:39:23 am
Off-Topic For general chats. Or anything else that doesn't fit.	1218 Posts 159 Topics	**Last post** by Ukencro in Re: Encrochat on **Today** at 08:26:15 am

Blackhat Knowledge		
Blackhat Library. A now forgotten shell that was once dedicated to the education of aspiring Blackhats.	38486 Redirects	

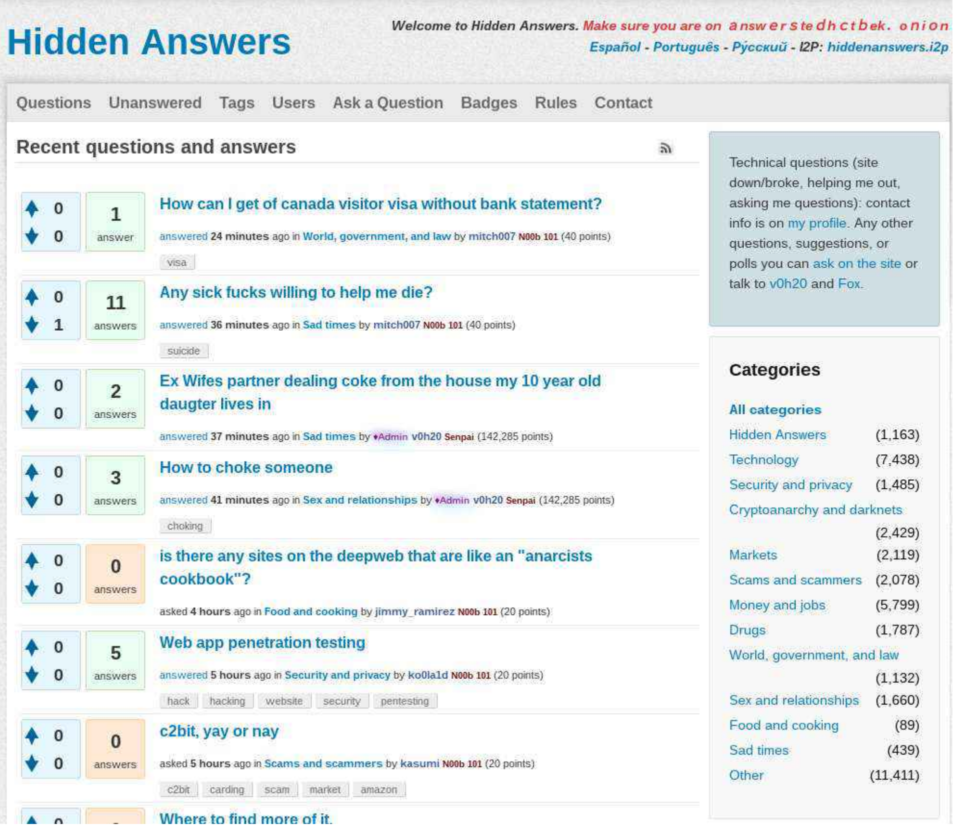
Marketplaces		Unread Posts
Market Discussion News or updates on the different marketplaces.	1462 Posts 306 Topics	**Last post** by Witchman05 in Re: Alcohol Venders? on **Today** at 06:56:21 am

Technology		Unread Posts
Cryptocurrencies. Cryptocurrency related news, thoughts or updates.	210 Posts 59 Topics	**Last post** by Witchman05 in Re: Reward!30000USD on **Today** at 05:12:54 am

Figure 4.6: Screenshot the categories in OnionLand forum

Hidden Answers Forum

The Hidden Wiki is also another public forum created by the same team that offered The Hidden Wiki. The Hidden Wiki is a Wiki of all the list of .onion hidden services and IRC chats. The categories cover a wide range of topics, from security and cryptoanarchy to relationships and food and cooking. It also supports multiple languages including Spanish, Portuguese and Russian. The forum implements badges for users, if the user has been a registered member for a pre-defined amount of time, the user can have his/her badge upgraded. Posts can have tags to represent the topic of discussion. The most popular tag was money with 2,564 posts as shown in Figure 4.8. Ransomware was not one of the most popular topics of discussion in the forum and had a low number of posts as low as 79. Figure 4.7 shows the home page of the forum with the list of categories.



Welcome to Hidden Answers. Make sure you are on answerstedhctbek.onion
Español - Português - Рýсский - I2P: hiddenanswers.i2p

Recent questions and answers

0 0 | 1 answer
How can I get of canada visitor visa without bank statement?
answered 24 minutes ago in World, government, and law by mitch007 N00b 101 (40 points)
visa

0 1 | 11 answers
Any sick fucks willing to help me die?
answered 36 minutes ago in Sad times by mitch007 N00b 101 (40 points)
suicide

0 0 | 2 answers
Ex Wifes partner dealing coke from the house my 10 year old daugter lives in
answered 37 minutes ago in Sad times by ♦Admin v0h20 Senpai (142,285 points)

0 0 | 3 answers
How to choke someone
answered 41 minutes ago in Sex and relationships by ♦Admin v0h20 Senpai (142,285 points)
choking

0 0 | 0 answers
is there any sites on the deepweb that are like an "anarcists cookbook"?
asked 4 hours ago in Food and cooking by jimmy_ramirez N00b 101 (20 points)

0 0 | 5 answers
Web app penetration testing
answered 5 hours ago in Security and privacy by ko0la1d N00b 101 (20 points)
hack hacking website security pentesting

0 0 | 0 answers
c2bit, yay or nay
asked 5 hours ago in Scams and scammers by kasumi N00b 101 (20 points)
c2bit carding scam market amazon

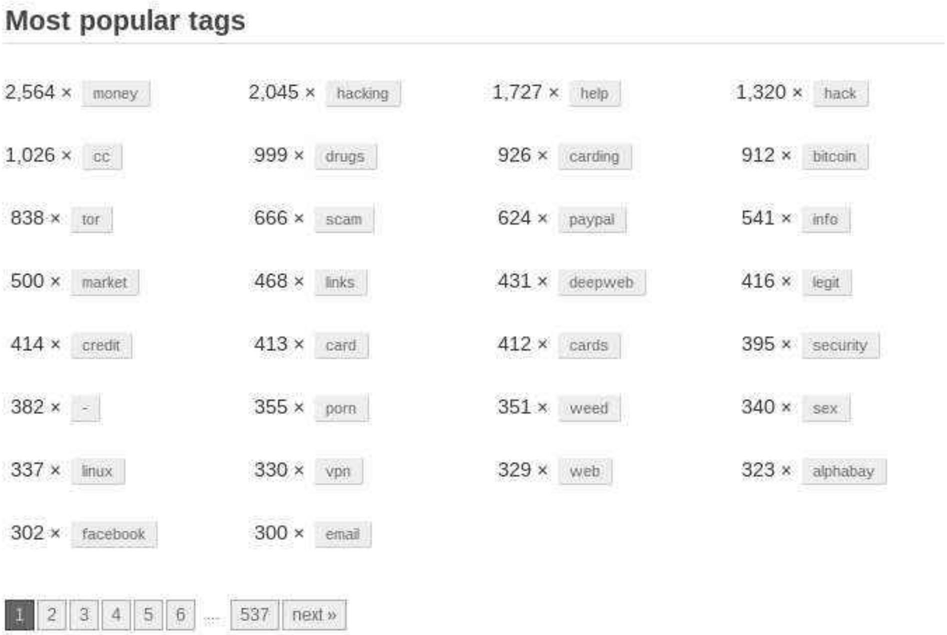
Where to find more of it.

Technical questions (site down/broke, helping me out, asking me questions): contact info is on my profile. Any other questions, suggestions, or polls you can ask on the site or talk to v0h20 and Fox.

Categories

All categories	
Hidden Answers	(1,163)
Technology	(7,438)
Security and privacy	(1,485)
Cryptoanarchy and darknets	(2,429)
Markets	(2,119)
Scams and scammers	(2,078)
Money and jobs	(5,799)
Drugs	(1,787)
World, government, and law	(1,132)
Sex and relationships	(1,660)
Food and cooking	(89)
Sad times	(439)
Other	(11,411)

Figure 4.7: Home page of the Hidden Answers

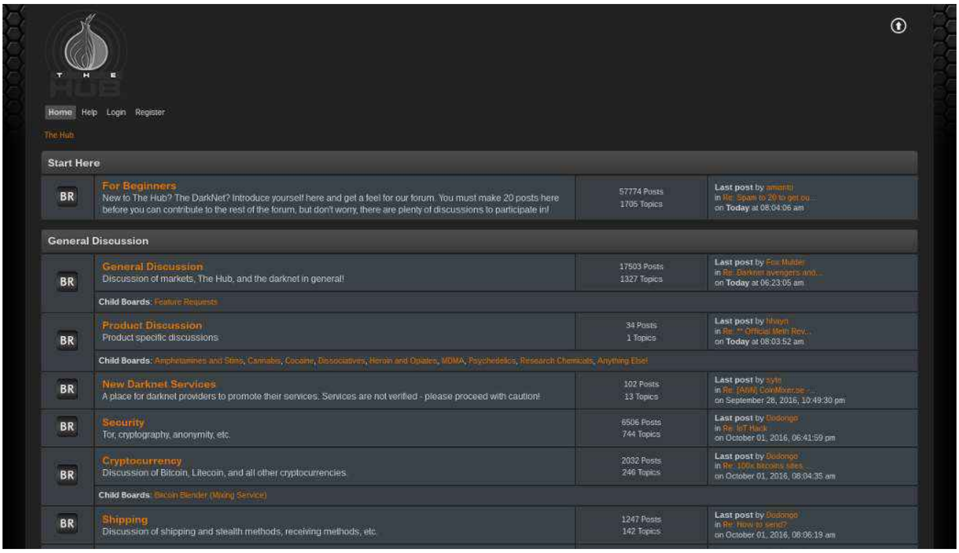


Most popular tags

2,564 × money	2,045 × hacking	1,727 × help	1,320 × hack
1,026 × cc	999 × drugs	926 × carding	912 × bitcoin
838 × tor	666 × scam	624 × paypal	541 × info
500 × market	468 × links	431 × deepweb	416 × legit
414 × credit	413 × card	412 × cards	395 × security
382 × -	355 × porn	351 × weed	340 × sex
337 × linux	330 × vpn	329 × web	323 × alphabay
302 × facebook	300 × email		

Figure 4.8: The top 32 tags of posts on Hidden Answers

The HUB Forum



The Hub

Start Here

BR	**For Beginners** New to The Hub? The DarkNet? Introduce yourself here and get a feel for our forum. You must make 20 posts here before you can contribute to the rest of the forum, but don't worry, there are plenty of discussions to participate in!	57774 Posts 1705 Topics	**Last post** by amantti in Re: Spam to 20 to get ou... on **Today** at 08:04:06 am

General Discussion

BR	**General Discussion** Discussion of markets, The Hub, and the darknet in general! **Child Boards**: Feature Requests	17503 Posts 1327 Topics	**Last post** by Fox Mulder in Re: Darknet avengers and... on **Today** at 06:23:05 am
BR	**Product Discussion** Product specific discussions **Child Boards**: Amphetamines and Stims, Cannabis, Cocaine, Dissociatives, Heroin and Opiates, MDMA, Psychedelics, Research Chemicals, Anything Else!	34 Posts 1 Topics	**Last post** by hhayn in Re: ** Official Meth Rev... on **Today** at 08:03:52 am
BR	**New Darknet Services** A place for darknet providers to promote their services. Services are not verified - please proceed with caution!	102 Posts 13 Topics	**Last post** by syte in Re: [ANN] CoinMixer.se - ... on September 28, 2016, 10:49:30 pm
BR	**Security** Tor, cryptography, anonymity, etc.	6506 Posts 744 Topics	**Last post** by Dodongo in Re: IoT Hack on October 01, 2016, 06:41:59 pm
BR	**Cryptocurrency** Discussion of Bitcoin, Litecoin, and all other cryptocurrencies. **Child Boards**: Bitcoin Blender (Mixing Service)	2032 Posts 246 Topics	**Last post** by Dodongo in Re: 100x bitcoins sites ... on October 01, 2016, 08:04:35 am
BR	**Shipping** Discussion of shipping and stealth methods, receiving methods, etc.	1247 Posts 142 Topics	**Last post** by Dodongo in Re: How to send? on October 01, 2016, 08:06:19 am

Figure 4.9: Home page of The HUB

The HUB is also listed as one of the top three forums on DeepDotWeb. It is one of the oldest forums and has a huge userbase that present a variety of discussions. Even more so, are the *forum contributors*, an additional role in the hierarchy that has the responsibility to answer most of the questions on the forum. One contributor that goes by the name *hackerjon* has expertise on hacking services and closed circles on the dark net.

4.3 Reflexive Notes

Producing reflective data is necessary to satisfy the *symbolic* representation of netnography. Notes were written during the observations of the online communities. There is no particular format these notes should adhere to. They can be written with pen and paper using the language the researcher is more comfortable with. What matters the most is that the notes should encompass the experience of the researcher during the study.

Reflexive notes are used to achieve the following points when presenting the collected data [34]:

- Provide an accurate atmospheric overview of the online social environment
- Extend current understanding by presenting one or more unique events that expand our knowledge and increase our understanding of elements, categories, processes, or practices in the community

When there is too much information useful for the research, colleced data from the HT-Track crawlers made it easy to summarize it. Data collected was listed in a spreadsheet. The attributes for each item listed in the cryptomarkets is mentioned below. Dictionary of objects:

- Product listing
- Listing title
- Listing price
- Vendor name
- Vendor Rating

The data of recorded will be projected onto graphs and diagrams to satisfy the *digital* netnographic representation. An overall analysis will give us better insight on the rate of increase in the sales of ransomware on cryptomarkets and how external shocks affects the sale of ransomware-as-a-service. The data content can also provide a glimpse of the organizational structure. The popularity of a vendor and the variety of items sold can be a good asset for both the digital and symbolic netnographic representation.

4.3.1 Method of Data Capture

The previously mentioned websites contain data of a wide range of products and services sold to members, but products such as cannabis and paypal accounts are irrelevant to include in the netnographic study. Therefore, the keywords needed to search for data had to be defined. Since this research mainly focuses on RaaS, it would be relevant enough to use *Ransom* or *Ransomware* for our search.

The type and expected quantity of data and how it should be analyzed must also be taken into consideration. Kozinets offers two choices for netnographers:

- Manual data capture using pen-and-paper for collecting small limited amounts of data
- Qualitative data analysis software program for large amounts of data to apply a general analysis

The choice for this research was to manually write observations and field notes since this is a discovery process of the irregular and unfamiliar structure of dark net markets. The second approach also disregards visual data such as videos, images and audio elements. These elements were necessary to present when using *humanistic* and *hermeneutic* methods to interpret the findings.

Data was recorded using spreadsheets, field notes and screen captures. Data registered through the spreadsheet was classified based on the service sold, its price in Bitcoins (BTC), marketplace, vendor account name, product description and field notes. Applying these labels to each RaaS could help us to retrieve a general analysis later on with the help of a software program.

The announcement of Dream Market's shutdown during the netnographic research could indicate the no more data can be retrieved from the website. However, data dumps of previously shut down dark net websites can be easily retrieved here (Gwern Branwen [26]).

5

RESULTS AND ANALYSIS

This Chapter presents an overview of the data collected, the findings of the netnographic observations and the deduced cost-benefit framework.

5.1 Overview of Collected Data

The data gathered included notes from interviews conducted by the external sources mentioned in Chapter 4 and observations of dark net activities and item listings. Item listings collected from other sources were also referred to in this research. A total count of 196 different ransomware item listings were collected from a variety of cryptomarkets. This section gives a summary of the amount of data collected from cryptomarkets, forums and interviews.

5.1.1 Cryptomarket Data

Data from dark net marketplaces was either archived or from reflexive notes. The archived data included data dumps of cryptomarket sales and buyer feedbacks, publicly posted by researchers. All of the archive data are from cryptomarkets that are no longer active. In Table 5.1, a list of the marketplaces that were included in the data dumps.

Name	Description	Date
AlphaBay	Popular cryptomarket shutdown in July 2017 by LE in Operation Bayonet [5]	April 2015 - January 2017
Hansa	Cryptomarket also shutdown in Operation Bayonet	December 2016
TheRealDeal	Cryptomarket for digital goods, intentionaly taken down by administrators	June 2015
Agora	Cryptomarket intentionally taken down by administrators	Unknown

Table 5.1: Dead cryptomarkets with the dates of the data retrieved for this research

The reflexive notes included screenshots and observational points of active marketplaces. Ransomwares listed from active marketplaces were also stored in spreadsheets with their price tags and descriptions. Aside from ransomware items, other digital goods had ransomware tags, such as hacking services, were included in the data.

5.1.2 Forum Data

From the three selected forums, the Hidden Answers had the most number of posts concerning RaaS. The Hidden Answers is in fact the oldest forum of the three, and comes in multiple languages including Portugese, Spanish and Russian. The forum is easily accessible and therefore has a huge userbase, covering a wide range of expertise.

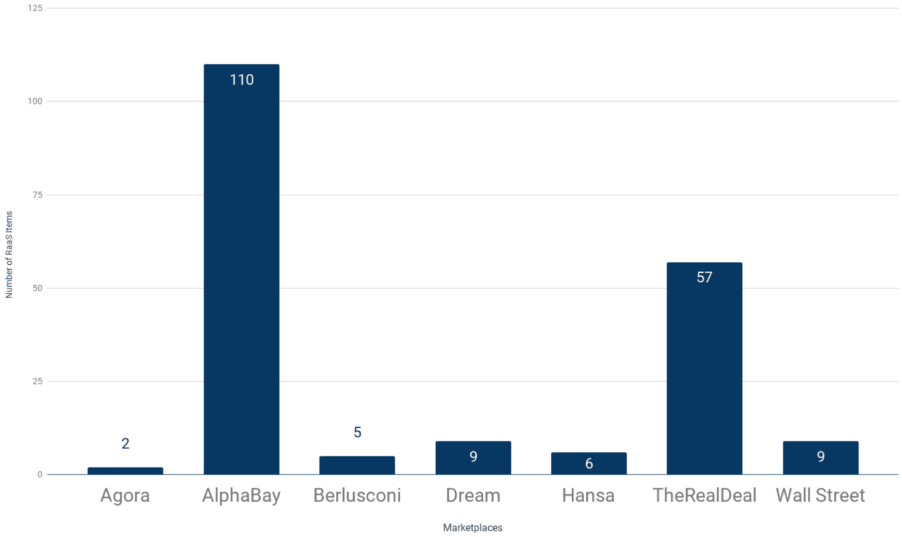


Figure 5.1: Number of ransomware related items for every marketplace

5.1.3 Interviews

Getting hold of chief dark net members is not an easy task and requires a rich experience with dark net communication. As mentioned in Section 4.1, investigative journalists and privacy advocates such as DeepDotWeb have reached with several dark net members and conducted interviews through PGP encrypted chats.

The interviews provided by DeepDotWeb focus on different members involved in dark net activities. Each interviewee offered a unique role and this role can be mapped to the list of actors presented in Chapter 2, Table 2.1. Most interviewees did not clarify whether or not they had a responsibility in the development and distribution of ransomware, nevertheless, their roles were a perfect match to the description of every actor. The interviews that were used for the empirical analysis are:

- **Market Admins:** Administrators of popular marketplaces
  - TheRealDeal Market
  - AlphaBay (Prior to July 2017 shutdown)
  - German Plaza
- **Marketplace Developer:** A developer that develops a marketplace infrastructure and websites on the dark net
- **Forum Moderator:** A moderator of a forum about insider trading. The forum is an *invite-only* forum.

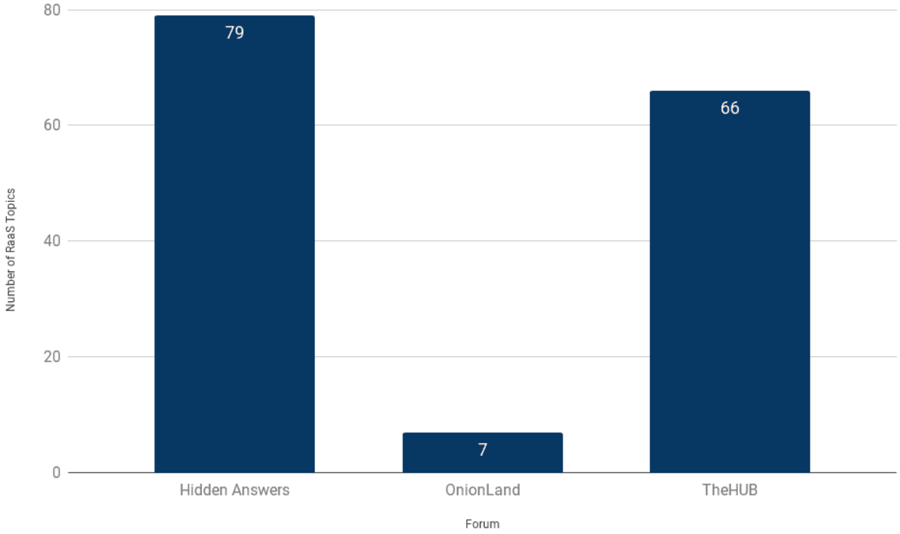


Figure 5.2: Number of topics discussing ransomware in the selected forums

- **Former Vendor**: An experienced dark net member offered carding services on the dark net. Was a member of the infamous Shadow Crew.
- **Money Launderer**: Provided laundering services for cryptomarket vendors to cash out their cryptocurrencies.
- **Ransomware Developers:** Developers of a ransomware posted through their own website. Many of the feedback imply that their ransomware is the typical work of a *script kiddie*.

5.2 Interpreting Dark Net Discussions

Interviews conducted by external sources and forum conversations were the main text used for interpretation. From the forum discussions, we looked into the interests of those who bring up the topic of ransomware, the intentions behind their .

5.2.1 General Overview of Forum Posts

From the forums selected, The Hidden Answers had a substantial number of posts about ransomware. The ransomware tag alone had 79 posts. The questions showed similarities and can be easily distinguished into the categories in Table 5.2.

Question Category	Description
Acquisition	The poster asks for a working ransomware for sale.
Create	The poster asks how to start developing a ransomware from scratch.
Scam	The poster asks whether a specific ransomware-as-a-service posted on the Tor network is a scam or not.
Code Help	Posters that are trying to develop a ransomware and are asking questions regarding the source code.
Discuss	General discussions on ransomware outbreaks and news articles
Author Partnership	Posters that claim that they have a working ransomware and are look for partners with contact info
Distribution Help	Posters that are asking for advice on distributing ransomware
Distribution Partnership	Posters that claim have a list of contacts and are looking for partners with a working ransomware
Decrypt Help	Victims infected by a ransomware and are looking for a decrypt key without paying the ransom

Table 5.2: Question categories in forum posts

The 79 ransomware posts were categorized into these 9 different question types to understand the overall interest of dark net members. The chart in Figure 5.3 shows the ratio differences between the categories. The majority of the posts were concerned about getting or buying ransomware. The least discussed topic was help on coding a ransomware.

The highest percentage was the acquisition category. This implies that more people are getting interested in easily acquiring ransomware than developing themselves, at least in English speaking forums.

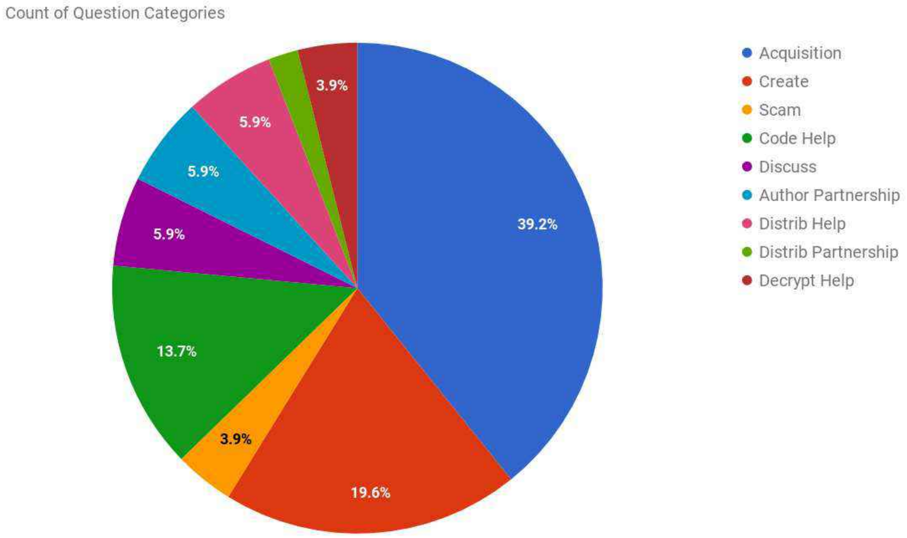


Figure 5.3: Chart of the question categories related to ransomware in the Hidden Answers forum

5.2.2 Ethical and Legal Inhibitions

Ransomware has successfully proved itself to be a good enough fraud for *easy money*. However, some dark netters in the forums have expressed their concern on the malicious exploitation from an ethical outlook. In a forum thread in which a member asks for technical help in coding a ransomware, the response received was labeled anonymous and it says:

“ I doubt I can dissuade you from this kind of moneymaking scheme, but perhaps a less harmful route is desirable? Mine litecoin or some easily mined cryptocurrency on infected machines? Uses some CPU power but otherwise they might not even know, and at worst costs them some power money. ”

The comment was inevitably downvoted. It does not come as a surprise, since it was flagged as anonymous user, this implies that this is not a popular opinion among dark netters. In fact, the top answer was a instructive help on the coding problem. The psychic opportunity costs as mentioned by Probasco and Davis [48] is very high in the case of ransomware, which may influence some dark netters to get involved in less damaging fraud.

The psychic costs are not the only factor that concerns the dark netters, but also the probability of apprehension and conviction. In another discussion thread, a user expresses eagerness to aquire ransomware. The response of user with a high level badge was as follows:

“My man, anything is possible. But don’t do anything dumb or illegal to get yourself in trouble. It isn’t worth it.”

Dumb or illegal is a common expression that is used multiple times in the dark net forums. An entire category that goes by the label *OPSEC*, short for Operational Security, focuses on security and safety issues for dark netters to avoid any action that is *dumb or illegal*. OPSEC is costly and the factors that determine its value is explained in more detail in Section 5.5.2. Users of the forums usually exchange ideas on how to combat possible legal convictions. The following answer in one of the threads gives insight on the extent of OPSEC:

“So you want to make it extremely difficult for an adversary to decrypt your data? The answer is not only simpler than one would think, but also preserves convenience. Start out with a minimum of 5 1-64 GB flash drives.

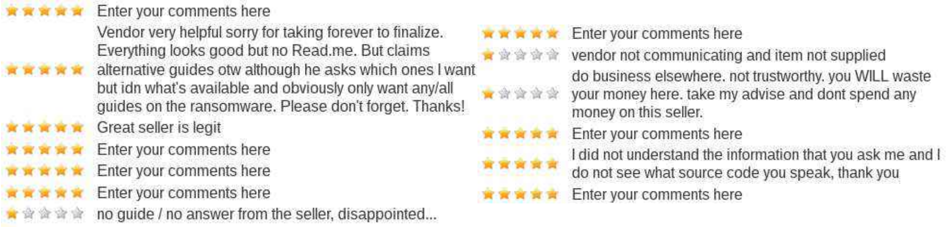
Setup full disk encryption on all of them using VeraCrypt. Use one long password on drive 1 (at least 32 characters) and keep track of the order of them. After the first, start using 64+ digit keys and storing the password for the next drive in the current until you get to the last one. You should create hidden volumes on each drive for plausible deniability. If court ordered to give up a password, you can give the password to the non hidden volume and your secret password placed in the hidden volume will never be found. For disk encryption type, use 3 in the cascade in whatever order you see fit. Research this for yourself. The last drive is where all your data will be. A good practice is to buy waterproof flash drives for the access chain, and a hardware encrypted external SSD for the end device. This will add a 4th layer of encryption on the end of the chain. To take it to the max, encrypt ascending passwords with your PGP key. Hide the access chain, except for the first drive, in random places (ifwaterproof, outside.) Memorize the first 32+ character key, this step is vital. If you made it through this tutorial, congrats. Your OPSEC is on point ”

In summary, ethical and legal restrictions are an important factor that influence the decision of a regular dark netter to take part in the value chain of ransomware-as-a-service. Some individuals may take part in less damaging activities of fraud or tasks that require storing or keeping of data or items that can be used against the individual in court.

5.2.3 Scam deals

The validity of ransomware sold on marketplaces was questioned throughout the research. Popular marketplaces list the number of purchases of a specific item. On average, all current ransomware-as-a-service items had purchases below 10. In addition, most of the information included in the description are redundant and have no unique deals compared to other items.

Items also lacked instructive feedback. The buyer’s username is obscured when viewing feedback and a 5 star rating plus a comment is presented. In some cases, buyers are open about their experience. Irrational feedback in some ransomware-as-a-service has supported the assumption that these RaaS items are indeed a scam. In Figure 5.4, 5 star ratings are not detailed in the sense that users do not share their attempts to distribute the ransomware. Those who are outspoken are the ones giving negative feedback.

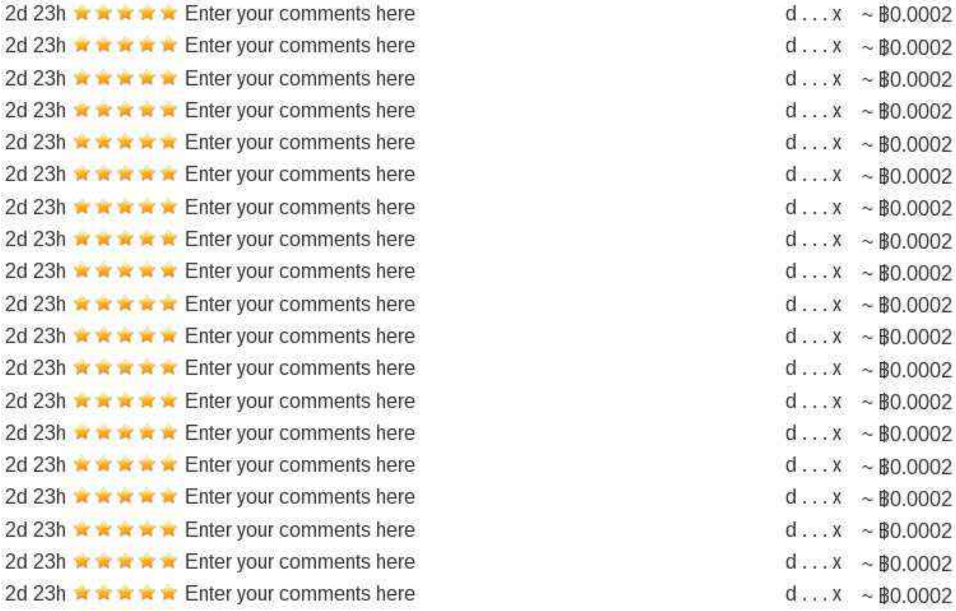


★★★★★ Enter your comments here
★★★★★ Vendor very helpful sorry for taking forever to finalize. Everything looks good but no Read.me. But claims alternative guides otw although he asks which ones I want but idn what's available and obviously only want any/all guides on the ransomware. Please don't forget. Thanks!
★★★★★ Great seller is legit
★★★★★ Enter your comments here
★★★★★ Enter your comments here
★★★★★ Enter your comments here
★☆☆☆☆ no guide / no answer from the seller, disappointed...

★★★★★ Enter your comments here
★☆☆☆☆ vendor not communicating and item not supplied
★☆☆☆☆ do business elsewhere. not trustworthy. you WILL waste your money here. take my advise and dont spend any money on this seller.
★★★★★ Enter your comments here
★★★★★ I did not understand the information that you ask me and I do not see what source code you speak, thank you
★★★★★ Enter your comments here

Figure 5.4: Product reviews of two different Ransomware-as-a-items

Vendor profiles in most dark net marketplaces include user reviews from all items sold by the vendor. Although most of the letters in the username of the buyer are replaced with asterisks, its easy to distinguish two feedbacks with the same username. When observing the reviews of one particular vendor with a high rating (Figure 5.5), the majority of the positive feedback came from one user with a username of *d****s*. A plausible explanation is that the high rating the vendor gained, was from an agreement with a user to buy the services and give 5-star ratings.



2d 23h ★★★★★ Enter your comments here d...x ~฿0.0002
2d 23h ★★★★★ Enter your comments here d...x ~฿0.0002
2d 23h ★★★★★ Enter your comments here d...x ~฿0.0002
2d 23h ★★★★★ Enter your comments here d...x ~฿0.0002
2d 23h ★★★★★ Enter your comments here d...x ~฿0.0002
2d 23h ★★★★★ Enter your comments here d...x ~฿0.0002
2d 23h ★★★★★ Enter your comments here d...x ~฿0.0002
2d 23h ★★★★★ Enter your comments here d...x ~฿0.0002
2d 23h ★★★★★ Enter your comments here d...x ~฿0.0002
2d 23h ★★★★★ Enter your comments here d...x ~฿0.0002
2d 23h ★★★★★ Enter your comments here d...x ~฿0.0002
2d 23h ★★★★★ Enter your comments here d...x ~฿0.0002
2d 23h ★★★★★ Enter your comments here d...x ~฿0.0002
2d 23h ★★★★★ Enter your comments here d...x ~฿0.0002
2d 23h ★★★★★ Enter your comments here d...x ~฿0.0002
2d 23h ★★★★★ Enter your comments here d...x ~฿0.0002
2d 23h ★★★★★ Enter your comments here d...x ~฿0.0002
2d 23h ★★★★★ Enter your comments here d...x ~฿0.0002
2d 23h ★★★★★ Enter your comments here d...x ~฿0.0002

Figure 5.5: The reviews in a vendor profile with a high rating

This assumption was further supported by a question posted on the OnionLand forum in which a user questions the validity of the services offered by software dealers on marketplaces.

“ Is there anyone or any vendor/market out there that isn’t a scam)? I mean, seriously!!! I’m beginning to think this whole Darknet is just an urban legend!! It seems so overrated, and to find someone genuine would be like something out of a movie!! Fuck, I’m even beginning to think that TOR is just a waste of space in my hard drive!! I’m not asking for direct links on here, but wrf!! Please give me something to go on, like a legit market or something, gotta start somewhere!! I already know the whole prepaid card market is a complete scam, but what about credit cards? Also, where are all the legit mag stripe card & software dealers, bulk blank card vendors, (maybe half of this stuff I can get on the Clearnet), dump data vendors and mentors that can collaborate with me and help me learn the tricks of the trade so that I can become a productive vendor of the REAL Darknet Society?? I don’t wanna become another shitbag scammer!! You may ask, "What’s in it for me")? I’ll tell you...BTC, a loyal partner, and a tiny bit of authenticity in a place that’s rampant with the fuckery!!! Now I know that there is no such thing as an escrow site for a referral to guarantee that I pay whoever for info, but for whatever it’s worth, my word is definitely guaranteed that if I do start to climb then those who helped/collaborated will climb with me as well. So please, please help me help you and help provide more authenticity to the Darknet!!! Any help would be much appreciated and will definitely be repayed!!! ”

The moderator of the forum responded that the true dark net lies through *invite-only spaces*. These spaces are either forums or IRC chats that do not allow easy access to the general public. To join these spaces, you either need an invitation link from a member within the circle or pay a fixed fee.

“ The "real" Darknet is nothing more than invite-only spaces and contacts that you aquire through XMPP.

The public space is supposed to be filled with scams and stupid products, because you don’t have to prove your worth to get into the public sphere.

The only way to experience the inner workings is to be able to convince others that you should be allowed into invite-only spheres as mentioned.

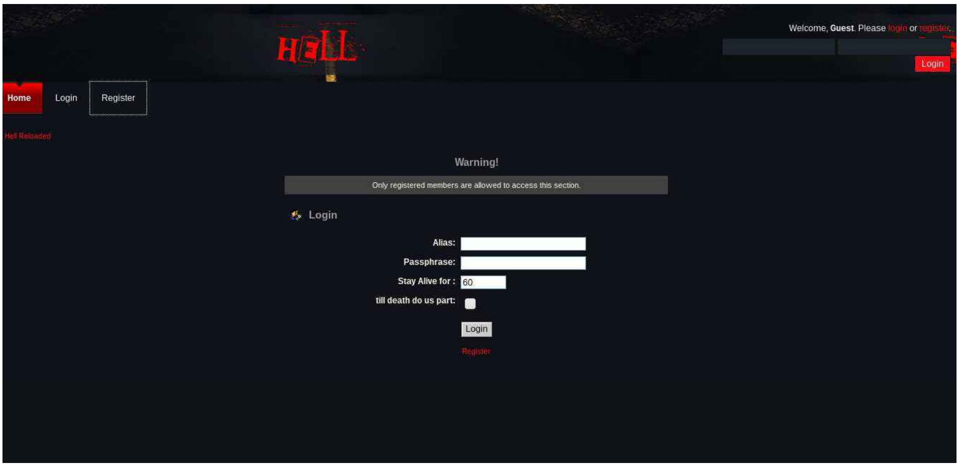
If you’re not valuable in any way though, nobody is going to reach out to you.

That’s just how things work. ”

This verifies the fact that most of the RaaS items sold on the dark net cryptomarkets are not genuine as marketed on cryptomarkets. The redundant descriptions and missing variant label and features makes it even more obvious. Notwithstanding that most vendors selling RaaS items are not specialized in ransomware. All of the highly rated vendors that do sell RaaS, mostly sell other services such as carding. Their interest in ransomware emerged lately, but they are not interested in a split deal of the ransom revenue with the buyer. The only way these vendors are making money out of RaaS, is by scamming any ill-informed user who is interested in ransomware.

5.2.4 Invite-only Forums

There were attempts to enter these enclosed circles of dark netters. A forum that goes by the name Hell (Figure 5.6) requested a payment of 0.01 BTC to register into the forum, or get invited by a member of the forum (Figure 5.7). Once the payer posts for the first time with informative input, the escrow is released back to its owner. A bitcoin address for the escrow payments was included in the registration page. Upon inspection, we notice a number of payments into and out of the wallet with similar value. However, the value fluctuates, we notice deposits of 0.5 BTC that are returned, and then 0.3, and finally 0.01.



Welcome, **Guest**. Please login or register.

Warning!

Only registered members are allowed to access this section.

Login

Alias:

Passphrase:

Stay Alive for : 60

till death do us part: □

Figure 5.6: An invite-only hacker forum

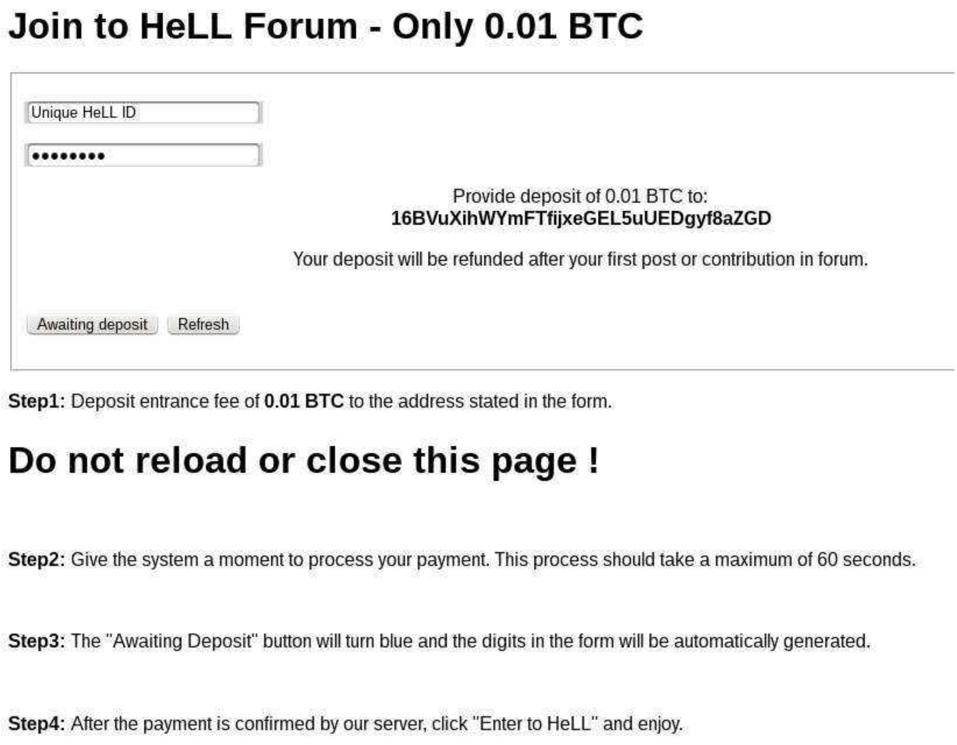
Privately sold ransomware was also published before when news erupted that the developer of Philadelphia ransomware distributed the ransomware in private chats on Alphabay. The chat was posted on the clearnet when a member compromised the machine of the buyer. The entire chat is in Appendix B.

This adds to Holt et al's [28] findings that highly skilled members are tightly close to each other through invite-only IRC's. With forums, new comers have a greater chance of learning and reaching out to highly skilled members. Individuals with limited expertise can eventually learn from their peers once they pay the entry fee despite its high cost.

To earn an invite, one must prove their skills by sharing previous projects. Sometimes the forum board members suspend invitations due to technical difficulties, but continue to be active on the forum. Members of the invite-only forums seem to work in groups and sell their hacking services through marketplaces. This assumption has been backed by the following answer to a post requesting an invitation to the Hell forum.

“ Unfortunately, an invite key is unlikely right now.

The forum is going through some changes.



Join to HeLL Forum - Only 0.01 BTC

Provide deposit of 0.01 BTC to:
16BVuXihWYmFTfijxeGEL5uUEDgyf8aZGD

Your deposit will be refunded after your first post or contribution in forum.

Step1: Deposit entrance fee of **0.01 BTC** to the address stated in the form.

Do not reload or close this page !

Step2: Give the system a moment to process your payment. This process should take a maximum of 60 seconds.

Step3: The "Awaiting Deposit" button will turn blue and the digits in the form will be automatically generated.

Step4: After the payment is confirmed by our server, click "Enter to HeLL" and enjoy.

Figure 5.7: Entry fee for Hell hacker forum

We’re in discussions about how to handle exactly what you are asking for.

Its possible that a section may be created for open sales and such. We’ll have to wait and see what the admins decide.

My suggestion is to go to a market, such as Real Deal. There are several good hackers, including some members of the Hell Crew, doing services there. Ask around the forum there.

Also, there are a couple of hackers that I know on Alphabay. Look up ’FliP’. TheyVe been around for years now, since the early days of the darknet. They have a good track record for as long as he’s been around.

You can also post on the classified section of Genesis. There are blackhats for sale, and some Hell Crew there as well. The address: ***********.

Othenrvise, if you have a specific Hellion in mind, I will send them a message for you. I will not give an invite, however. ”

5.2.5 Ransomware-as-a-Service versus Carding Services

Spreading ransomware is a fraud activity. However, it is not the most popular fraud activity, at least in English cryptomarkets and forums. The most popular item sold on cryptomarkets are drugs and narcotics, on average 30% of the total items. Ransomware-as-a-service is usually sold under the *Digital Goods* or *Services* category, but are not inumerable compared to other digital goods and services. In fact, the most popular digital good or service is carding, or credit card fraud. Figure 5.8 shows the number of items sold for every category in Dream Market. These items are usually sold in packages i.e. several cards are offered in an item. Other type of stolen accounts are even regarded as part of the carding service such as Paypal or subscriptions to paid services.

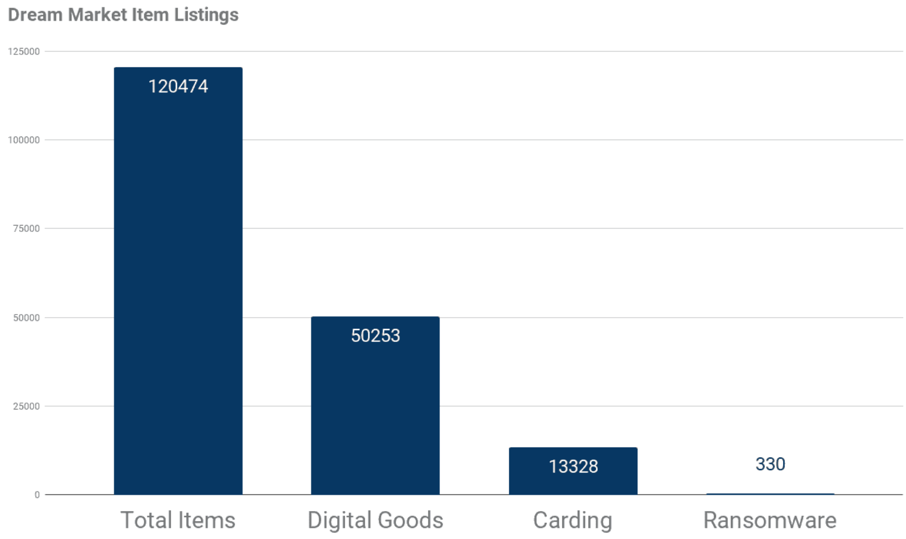
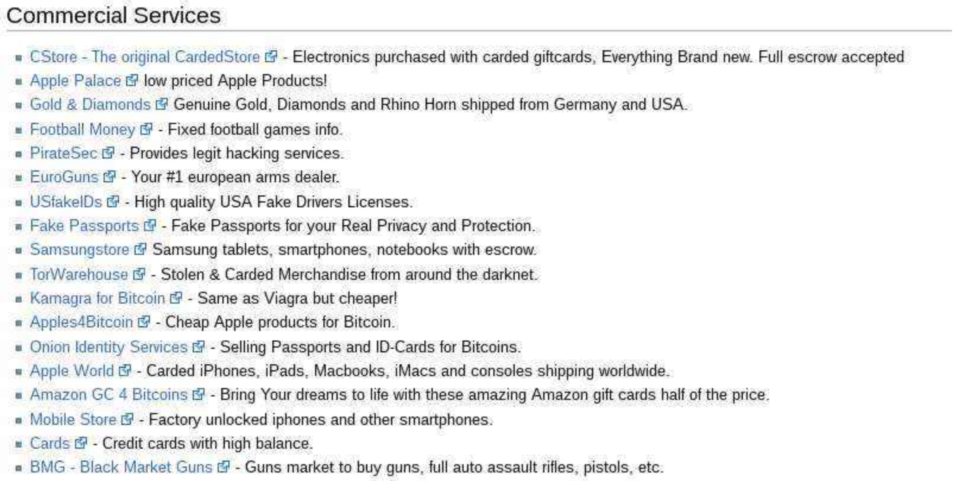


Figure 5.8: Count of items in the categories sold in Dream Market

The carding market was and still is at its highest in English-speaking marketplaces and forums. Carding services are also sold in privately-hosted websites, and there is a long list of hidden services as shown in Figure 5.9 Purchasing carding services has a low risk of getting scammed. The reason behind this is a rule of thumb recommended by experienced dark netters. Usually cards with a substantial amount of money such as 3000 US Dollars are sold for 120 US Dollars. To guarantee whether this is not a scam, buyers ask the vendor to deduct the price of the service from the total amount of money in the card instead of buying it in cryptocurrency.

Unlike RaaS items, the reviews on carding services are considered authentic since they are more expressive and are greater in number. In forums, users take the opportunity to share their experiences with a particular vendor. For example, the following quote from a post in a thread asking for authentic carding services:



Commercial Services

- CStore - The original CardedStore - Electronics purchased with carded giftcards, Everything Brand new. Full escrow accepted
- Apple Palace low priced Apple Products!
- Gold & Diamonds Genuine Gold, Diamonds and Rhino Horn shipped from Germany and USA.
- Football Money - Fixed football games info.
- PirateSec - Provides legit hacking services.
- EuroGuns - Your #1 european arms dealer.
- USfakeIDs - High quality USA Fake Drivers Licenses.
- Fake Passports - Fake Passports for your Real Privacy and Protection.
- Samsungstore Samsung tablets, smartphones, notebooks with escrow.
- TorWarehouse - Stolen & Carded Merchandise from around the darknet.
- Kamagra for Bitcoin - Same as Viagra but cheaper!
- Apples4Bitcoin - Cheap Apple products for Bitcoin.
- Onion Identity Services - Selling Passports and ID-Cards for Bitcoins.
- Apple World - Carded iPhones, iPads, Macbooks, iMacs and consoles shipping worldwide.
- Amazon GC 4 Bitcoins - Bring Your dreams to life with these amazing Amazon gift cards half of the price.
- Mobile Store - Factory unlocked iphones and other smartphones.
- Cards - Credit cards with high balance.
- BMG - Black Market Guns - Guns market to buy guns, full auto assault rifles, pistols, etc.

Figure 5.9: Domination of carding services on the list of privately-owned websites

“I bought a universal CC oft J-Connor on Dream Market. Put it in any ATM and withdraw as much as you want using any 4 digit code. It still works now and I bought it over a year ago. I think they do them for about $100”

Following this finding, a new question aroused, why is carding services more popular than ransomware? As part of the researcher’s immersion in forum, this question was submitted in one of the forums. The moderator responded with this answer:

“Creating ransomware is quite hard and tasking for most people, you don’t need to understand programming to type numbers into a HTML form.”

This could eventually mean that ransomware is developed by highly skilled programmers, but are unemployed or wish to have a freelance job. Countries with a high unemployment rate in computer science positions offer the perfect environment for individuals to join the underground economy of ransomware. As far as English-speaking countries are concerned, ransomware is not that popular. From an interview excerpt with a previous carder, American youths that are below the age of 21 get involved in carding services on the internet to publish fake IDs to acquire alcoholic drinks. Therefore, the interest in carding services in English marketplaces and forums are much popular than that of their Russian counterpart.

5.3 Actor Profiling

Attacker profiling was based on the interpretation of dark net member feedback on cryptomarkets, forum posts and most importantly the interviews. From this information, we could extract investigative and non-investigative facts that are useful for actor profiling. The factors listed in Section 2.1.1 were used as a framework for the following stakeholders. Not all of the stakeholders mentioned in Table 2.1 (Exchanger and Rogue Hosting) were profiled due to lack of information.

The sources used to create the profiles are listed in Table 5.3 and the deduced value chain is shown in Figure 5.10.

Profile	**Retrieved From**
Vulnerability Researchers	Interview with administrators of TheRealDeal market, a market that sells zero-day exploits. See Appendix A.1.
Malware Authors	Interview with the developers of the Tox ransomware. See Section 4.1.
Vendors	Based on findings in observations
Malware Distributors	Based on findings in observations
Website Designers	Interview with dark net developer. See Appendix A.3.
Money Mules	Interview with a dark net money launderer. See Appendix A.2.

Table 5.3: Modelling of Individual actors in the cybercrime economy

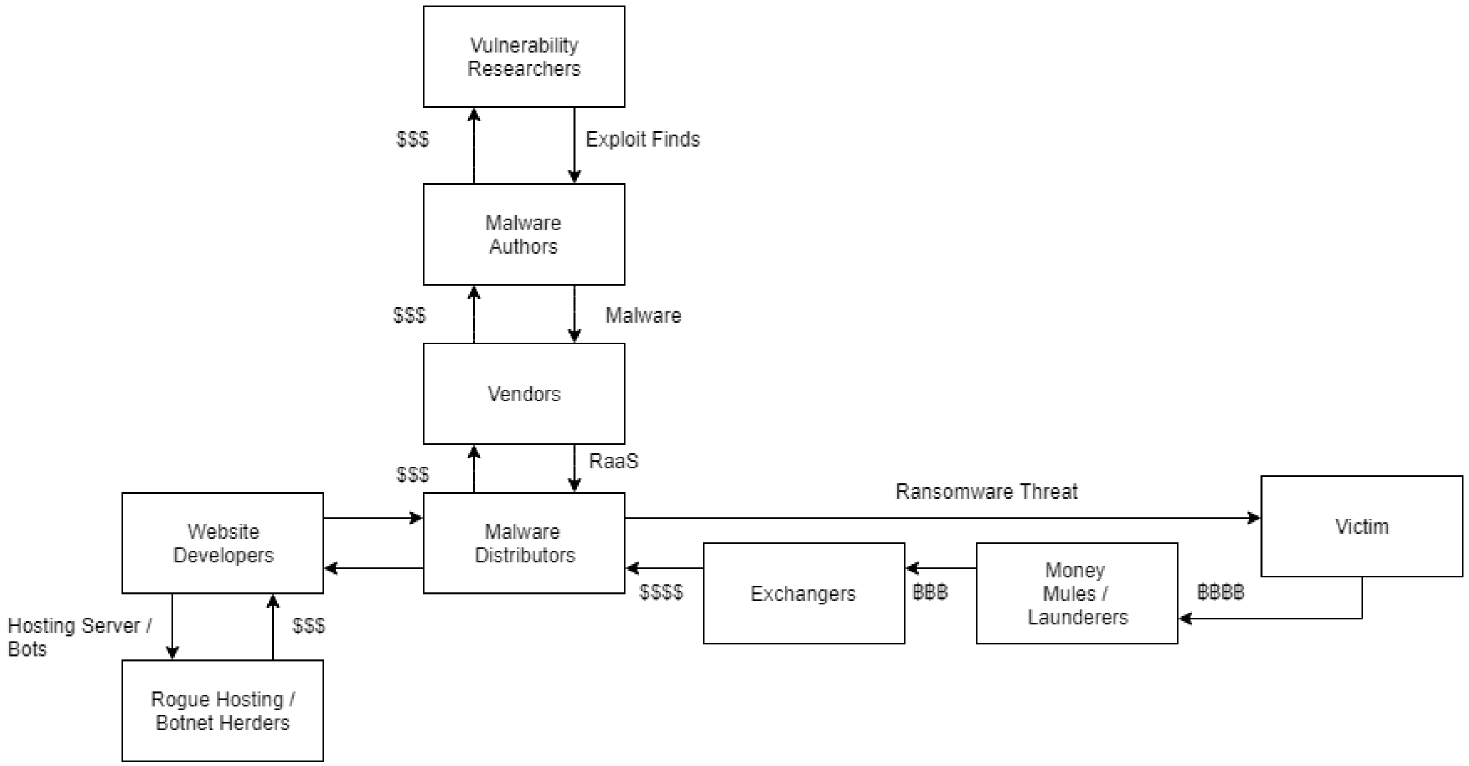


Figure 5.10: Value chain of the supply of ransomware-as-a-service in the underground economy

Vulnerability Researchers

Vulnerability researchers are members of the dark net who hunt for zero-day exploits. These offer entry points for the ransomware to decrypt files on a device. These researchers are technically sophisticated members with high expertise in hardware and software vulnerabilities, operating systems and software development skills. Information of the services they offer on the dark web is not publicly available for all to see, but exchanged in invite-only IRC servers. New cryptomarkets that sell zero-day vulnerabilities and offer a variety of hacking services are being hosted on the Tor network. TheRealDeal marketplace sold drugs along with digital goods to attract consumers to the marketplace, but the administrators promised that it will be removed when they have reached a substantial number of users. Another marketplace called German Plaza followed their footsteps and supported multiple languages including German and English.

Table 5.4: Vulnerability Researcher

Name:	Vulnerability Researcher
ID: TA.A.01	
Description: Searches for zero-day vulnerabilities and sells the information to others who can write exploit code	
Relationship: External	Region of Operation: Worldwide
Motive: Discover zero-day vulnerability	Intent: Deliberate, Malicious and Competitive
Capability: Advanced coding knowledge and skills	
Target Victim: Financial	
Action: Penetration testing of commerical computer and mobile operating systems and their updates	
Targeted Asset: Private Key leaks, Undisclosed vulnerabilities	
Objective: Maintain a high reputation within the marketplace, increase profits	

Malware Authors

Malware authors either work individually or in groups to develop ransomware varients. They use information provided by vulnerability researchers to code efficient encryption algorithms that are capable of locking an entire device in the shortest time possible. In the Appendix, a private chat between a ransomware author and an interested buyer is leaked and posted in a clearnet forum. The author attempts to sell a newer version of ransomware with the intention of infecting 20,000 devices. In another case, the authors behind Petya and Mischa ransomware tried to combat ransomware sales by leaking the private keys of their ransomware rival, Chimera. From that, we could devise an attacker profile:

Table 5.5: Malware Authors

Name:	Malware Author
ID: TA.A.02	
Description: Develops the malware	
Relationship: Internal	Region of Operation: Worldwide
Motive: Create efficient easily spread ransomware	Intent: Deliberate, Malicious and Competitive
Capability: Advanced coding knowledge and skills	
Target Victim: Financial	
Action: Writes the source code for encryption algorithm and user interface for customized ransomware	
Targeted Asset: Key leaks for rivalries,	
Objective: Develop ransomware that can spread to many computers as possible	

Vendor

Vendors can be authors, but some vendors have no knowledge on how to code and probably sell a wide range of products that are not necessarily digital goods. Some vendors offer technical support if there are bugs in the ransomware or the distributor is struggling to run it. These vendors are represented in Table 5.6.

Table 5.6: Vendor Attacker Profile

Name:	RaaS Vendor
ID: TA.V.01	
Description: Sells ransomware in marketplaces. Sometimes the developer of the ransomware takes this role. On other occasions, these vendors can also sell a variety of illegal products and services such as drugs, and carding services. Vendors either sell it on a variety of marketplaces or have their own personal platform	
Relationship: External	Region of Operation: Worldwide
Motive: MarketPlace Reputation	Intent: Deliberate and Competitive
Capability: Good network of cyber criminals or marketplace participants	
Target Victim: General Public	
Action: Campaign Tracking as a Service, Bitcoin Transaction Monitoring, Bitcoin Distribution	
Targeted Asset: Mass Market, Targeted Campaigns on Businesses or Governmental Institutions	
Objective: Maintain a high reputation within the marketplace, increase profits	

Malware Distributors

Distributors are sometimes outspoken in the dark net. They share outcomes of the distribution of a ransomware, and give feedback on ransomware purchases. Some distributors search for partnerships involving malware developers on forums. From the preliminary study, two profiles of malware distributors emerged; *novice* and *experienced* [7].

Table 5.7: Experienced Distributor Attacker Profile

Name:	Experienced Distributor
ID: TA.D.01	
Description: Buys the ransomware from the marketplace in the form of source codes, uses expertise to execute the source codes. There are several types of source code files, one that encrypts the files on a hard disc, another that displays the ransom etc.	
Relationship: Internal	Region of Operation: Worldwide
Motive: Financial Gains	Intent: Deliberate and Malicious
Capability: Good understanding of the source codes and how they work. Good at concealing their identity	
Target Victim: General Public or Targeted Businesses and Governmental Institutions	
Action: Distributing ransomware by social engineering. The ransomware is either sent through a spam email or in USB stick. Set price of ransom, deadlines and Bitcoin wallet address	
Targeted Asset: Mass Market, Targeted Campaigns on Businesses or Governmental Institutions	
Objective: Exploit a targeted individual/business or increase profit	

Table 5.8: Novice Distributor Attacker Profile

Name:	Novice Distributor
ID: TA.D.02	
Description: Buys the ransomware from the marketplace in the form of source codes, follows tutorials that are included within the package to exploit a computer	
Relationship: Internal	Region of Operation: Worldwide
Motive: Financial Gains	Intent: Deliberate and Malicious
Capability: Very week technical skills, little to no experience with distributing ransomware	
Target Victim: General Public	
Action: Distributing ransomware by social engineering. The ransomware is either sent through a spam email or in USB stick. Ses price of ransom, deadlines and Bitcoin wallet address	
Targeted Asset: Mass Market	
Objective: Increase profits	

Website Crackers/Designers

Installing a malicious website from a trustworthy website is a good way to distribute ransomwares. Web designers are responsible to recreate websites that look authentic to the user and could act as a trap. A developer's hourly rate in the dark net is very expensive. The high cost can amounts to other features such as developing the infrastructure of a dark net marketplace. This involves securing the anonymity of the users of the marketplace and protecting the marketplace from DDoS attacks.

Table 5.9: Website Developer

Name:	Malware Distributor
ID: TA.WD.01	
Description: Website Developer	
Relationship: External	Region of Operation: Worldwide
Motive: Develop a website mimicking an authentic website	Intent: Deliberate and Malicious
Capability: Has skilled knowledge in web development	
Target Victim: Financial	
Action: Develops a website for the victim to fall into downloading a malicious file	
Targeted Asset: Websites with a huge userbase	
Objective: Create a copy of a website to look as authentic as possible	

Money Launderers and Mules

The responsibility of a money launderer steal identities from individuals through social engineering mechanisms. The launderer then offers fake bank accounts opened with the stolen identities Vendors that sell illegal products and services on dark net marketplaces, deposit the Bitcoins they profited into the fake accounts and then cash it out. Law enforcement trace back these bitcoins to unsuspicious individuals. On some occasions, the money mules are part of the team of assailants in which they get a greater share for acting up as innocent individuals. For this role, two profiles were listed, one is a professional whereas the other is innocent.

Table 5.10: Professional Money Launderers

Name:	Professional Money Launderers
ID: TA.M.01	
Description: Stores ransom funds in an intermediary bank account for the assailant to cash out using fake identity	
Relationship: External	Region of Operation: Worldwide
Motive: Maintain high reputation	Intent: Deliberate
Capability: Can open fake bank accounts	
Target Victim: Financial	
Action: Opens a bank account for the assailant to cash out the ransom money	
Targeted Asset: Personal IDs of local citizens	
Objective: Open a bank account using an ID without the knowledge of the person and transfer money	

Table 5.11: Innocent Money Launderers

Name:	Innocent Money Launderers
ID: TA.M.02	
Description: Innocent Money Launderers	
Relationship: External	Region of Operation: Worldwide
Motive: No motive	Intent: Accidental
Capability: Is a normal citizen	
Target Victim: Financial	
Action: Shares own identity in a scam	

5.4 Pricing Scheme

Ransomware-as-a-Service items in marketplaces had different prices. The differences in prices across items are reflected in differences in encryption algorithm, vendor reputation, customizable options, partnership opportunities and external costs. Observations include a connection between these factors and the listed price in the marketplace.

The vast majority of the RaaS item listings in the cryptomarkets had redundant descriptions, hence, considered scam items. However, some ransomware items stood out as they were detected before in cyber security reports and articles. These ransomware variants were filtered out from the rest and their prices were recorded in US Dollars. Most of them were observed in AlphaBay old data dumps, but some were also actively sold in Dream and Agora. Figure 5.11 shows the ransomware variants and their prices.

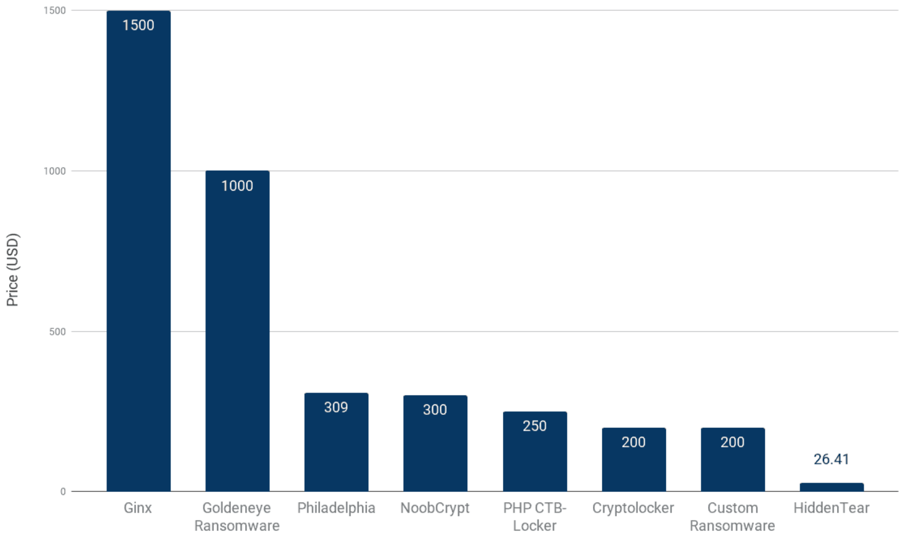


Figure 5.11: Prices of detected ransomware

Ransomware-as-a-service item prices do fluctuate over time. Gwern's crawled data dumps from AlphaBay have a very limited set of RaaS items since they were only from 2015. The number of ransomware items begin to gradually increase between the years 2016 and 2017 in other datasets. However, a prevalent change notice when tracking one item, was the increase of its price. This can be seen in Figure 5.12. This item seems to be developed by a group of french hackers that went by the name *mosh*.

The reason behind these abrupt changes in price is open for speculation. There are some connections that are evident, however, and can be justified as the reason behind the change. For instance, the price in the 22nd of April almost doubles in amount. What also increases at a similar rate is the number of views to that particular item. More members are becoming

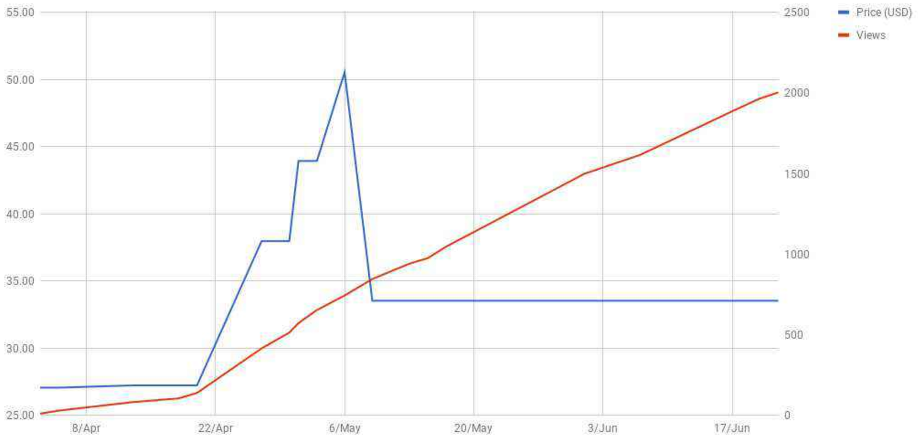


Figure 5.12: RaaS item price fluctuations on AlphaBay with the number of views to the item

interested in the service and probably have expressed it with the vendor. The vendor may have tried to take advantage of the sparked interest in ransomware and increased the price. The number of views continue to increase at a constant rate, however, there is no apparent reason behind the sharp decrease in the price in 6th of May. Possible reasons could be a release of a decrypter of the ransomware, or a rise in negative reviews by previous buyers. The dumps crawled by Gwern are incomplete, and therefore it is very difficult to come up with a concrete conclusion.

5.4.1 Customizable Ransomware

Customizable ransomware are a popular trend in the economy of ransomware-as-a-service. Figure 5.13 shows an example of a customizable ransomware that was identified in one of the private vendor markets. The set of features in the ransomware that can be modified by the customer include but is not limited to the following:

- Ransom amount in ransom
- Bitcoin wallet address
- Timer duration (i.e. the number of hours left before the ransom amount is doubled)
- Deadline (i.e. number of days left before all files are removed)
- Warning message to be displayed on the screen

Ransomware-as-a-service vendors are integrating innovative features to the service to attract potential buyers. These features offer a management interface in which the distributor can control and monitor ransomware infections on victims. The best example discovered during the netnographic study was that of Philadelphia Ransomware. It was mentioned

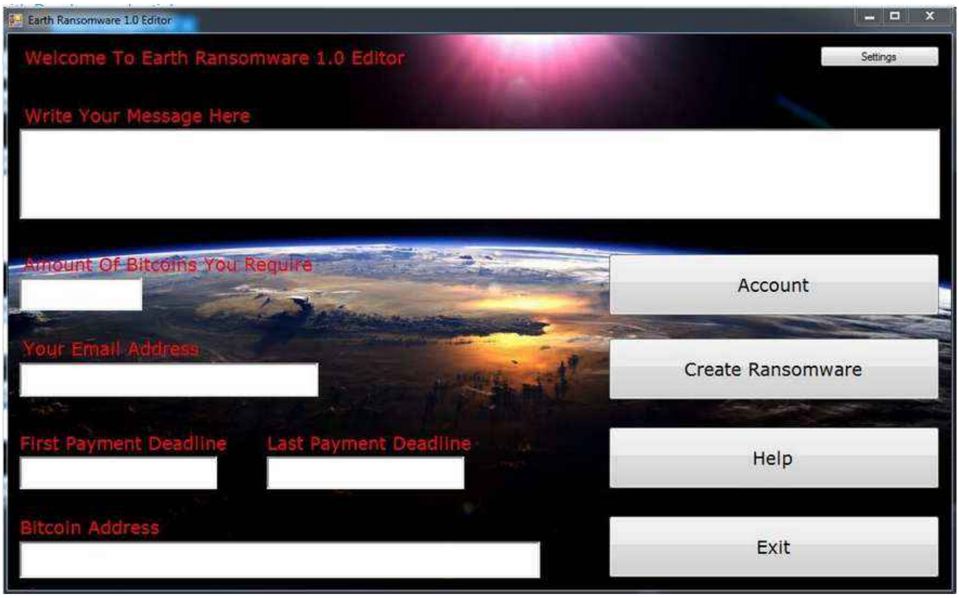
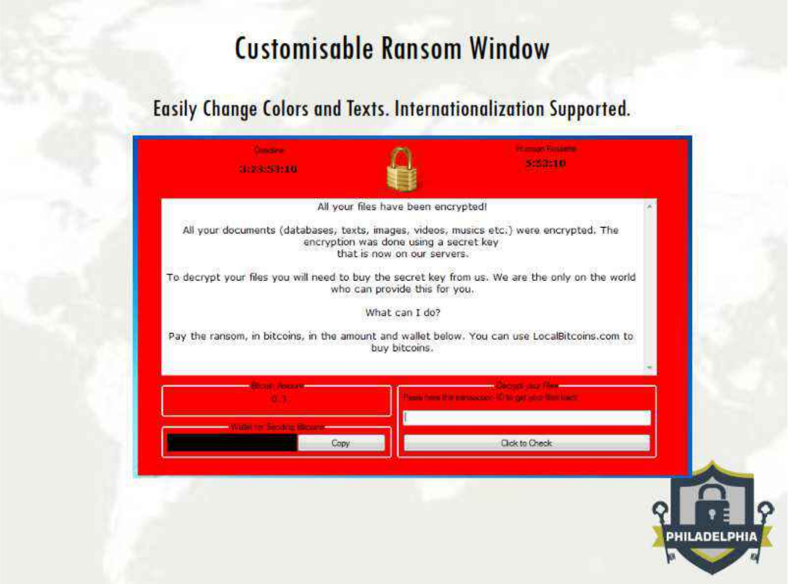


Figure 5.13: A customizable ransomware

before as the ransomware that was sold privately. Its management interface, coined as the "Headquarters" offered a wide range of options to the user. These were:

- Password protected login to the *Headquarters*
- Retrieve IP addresses of infected devices
- Retrieve geographical location of the victim
- Give mercy to victims with a press of a button
- Customizable ransomware window
- Group and filter victims and download PDF report summaries
- Unlimited and customizable builds (i.e. distributor can infect as many devices as possible)
- Depth of encryption on the victim's drive

Figures 5.14 and 5.15 show how user friendly the Philadelphia ransomware is with its concise user manual that can be easily understood by low-skilled members of the dark net. The overall interface looks intriguing and interactive. The headquarters has its own login screen which implies that a user account needs to be created. The ransomware screen displayed to the victims is customizable with options to change the background color. If the distributor suffered from high psychic opportunity cost, he/she can offer mercy to the victims by restoring access to their device without receiving the ransom.



Customisable Ransom Window

Easily Change Colors and Texts. Internationalization Supported.

Deadline

3:23:53:10

[illegible]

5:53:10

All your files have been encrypted!

All your documents (databases, texts, images, videos, musics etc.) were encrypted. The encryption was done using a secret key that is now on our servers.

To decrypt your files you will need to buy the secret key from us. We are the only on the world who can provide this for you.

What can I do?

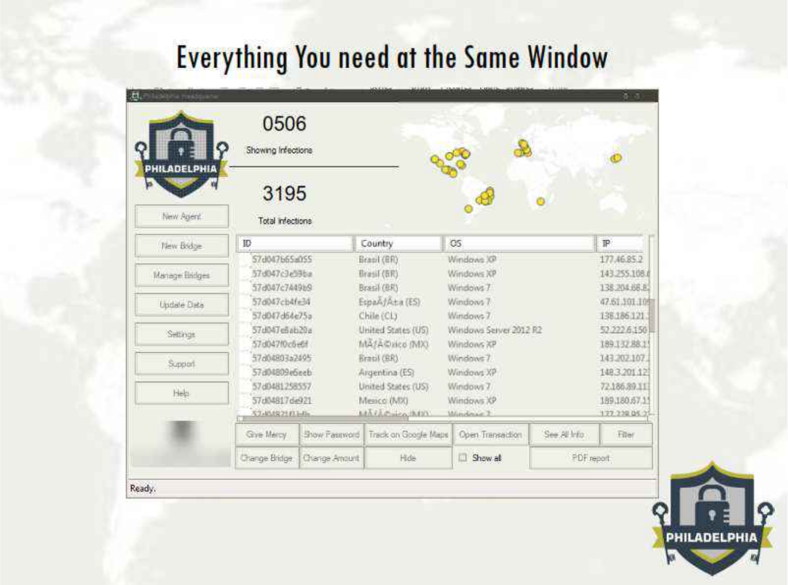
Pay the ransom, in bitcoins, in the amount and wallet below. You can use LocalBitcoins.com to buy bitcoins.

Bitcoin Amount: 0.1

Wallet for Sending Bitcoins: [redacted]

Decrypt your Files: Paste here the transaction ID to get your files back

Figure 5.14: Distributor can customize the displayed screen of the ransomware



Everything You need at the Same Window

0506

Showing Infections

3195

Total Infections

ID	Country	OS	IP
57d047b65a055	Brasil (BR)	Windows XP	177.46.85.2
57d047c3e59ba	Brasil (BR)	Windows XP	143.255.108.(
57d047c7449b9	Brasil (BR)	Windows 7	138.204.68.8
57d047cb4fe34	EspaÃ/Â±a (ES)	Windows 7	47.61.101.10
57d047d64e75a	Chile (CL)	Windows 7	138.186.121.
57d047e8ab20a	United States (US)	Windows Server 2012 R2	52.222.6.150
57d047f0c6e6f	MÃ/Â©xico (MX)	Windows XP	189.132.88.1
57d04803a2495	Brasil (BR)	Windows 7	143.202.107.
57d04809e6eeb	Argentina (ES)	Windows XP	148.3.201.12
57d0481258557	United States (US)	Windows 7	72.186.89.11
57d04817de921	Mexico (MX)	Windows XP	189.180.67.1

Ready.

Figure 5.15: Distributor can monitor the infection advances, and give mercy to victims

5.4.2 Partnership Deals and Competition

Price fluctuations might also be the result of partnerships. In the chart in Figure 5.3, 19.6% of posts on ransomware were of people looking for a partnership to either distribute or develop a ransomware. The terms of the split included a split of the ransom returns. This varied from 50%-50% to 30%-70%.

A ransomware variant that was sold by the name Ginx, was responsible for locking Mac OSX devices. Ginx was sold in three different prices on AlphaBay. The price differences were based on the percentage the vendor selling the ransomware would profit from the ransom received. The prices and partnership agreements are listed in Table 5.12.

Percentage Share	Price (USD)	Sold
%70-%30	1500	0
%60-%40	1000	0
%50-%50	500	3

Table 5.12: Ginx Ransomware AlphaBay Price Listing Variety

Tough rivalry between different malware authors can lead to partnerships against a dominant author in the market. The authors behind two prevalent ransomwares called *Petya* and *Mischa*, have grouped up to release a leak of 3500 decryption keys of another popular ransomware called Chimera. Leaking those keys puts Chimera off the market and offers leverage to the developers behind Petya and Mischa. In addition, their reputation is enforced by the fact that they were capable to attain those keys.

5.4.3 Hosting private vendor shops

Marketplaces impose *vendor fees* or *bonds* on users that wish to acquire vendor status on the website. Vendor fees vary from one marketplace to another. In addition to the vendor fees, there are commission fees imposed as a percentage deducted from every transaction in the marketplace. Some marketplaces distribute the value equally on either vendor or commission fees. The more popular the market is, the more expensive it is to handle your item sales as a vendor. With that being said, vendors need to compare the costs imposed between the marketplaces and select them based on the budget, and the expected revenue from selling on a particular marketplace. In the preliminary study, one particular finding showed price differences on two different market but sold by the same vendor. The reason may simply be because one marketplace charges a higher commission rate or vendor fee than the other. In Table 5.13, the commission rate and vendor fees for the selected marketplaces are listed.

- **Vendor Fee:** A registration fee imposed on users acquiring vendor status on a marketplace.
- **Commission:** On every transaction made in a market, there is a percentage taken

from the vendor's revenue by the marketplace administrators. This is mostly common in centralized markets.

Market	Commission	Vendor Fee	Rating
Wall Street Market	2 - 5	80	4.24
Dream Market	4	300	4.03
Berlusconi Market	2	Free / 250	3.67

Table 5.13: Dark Net Marketplace comparison based on commission and vendor fee

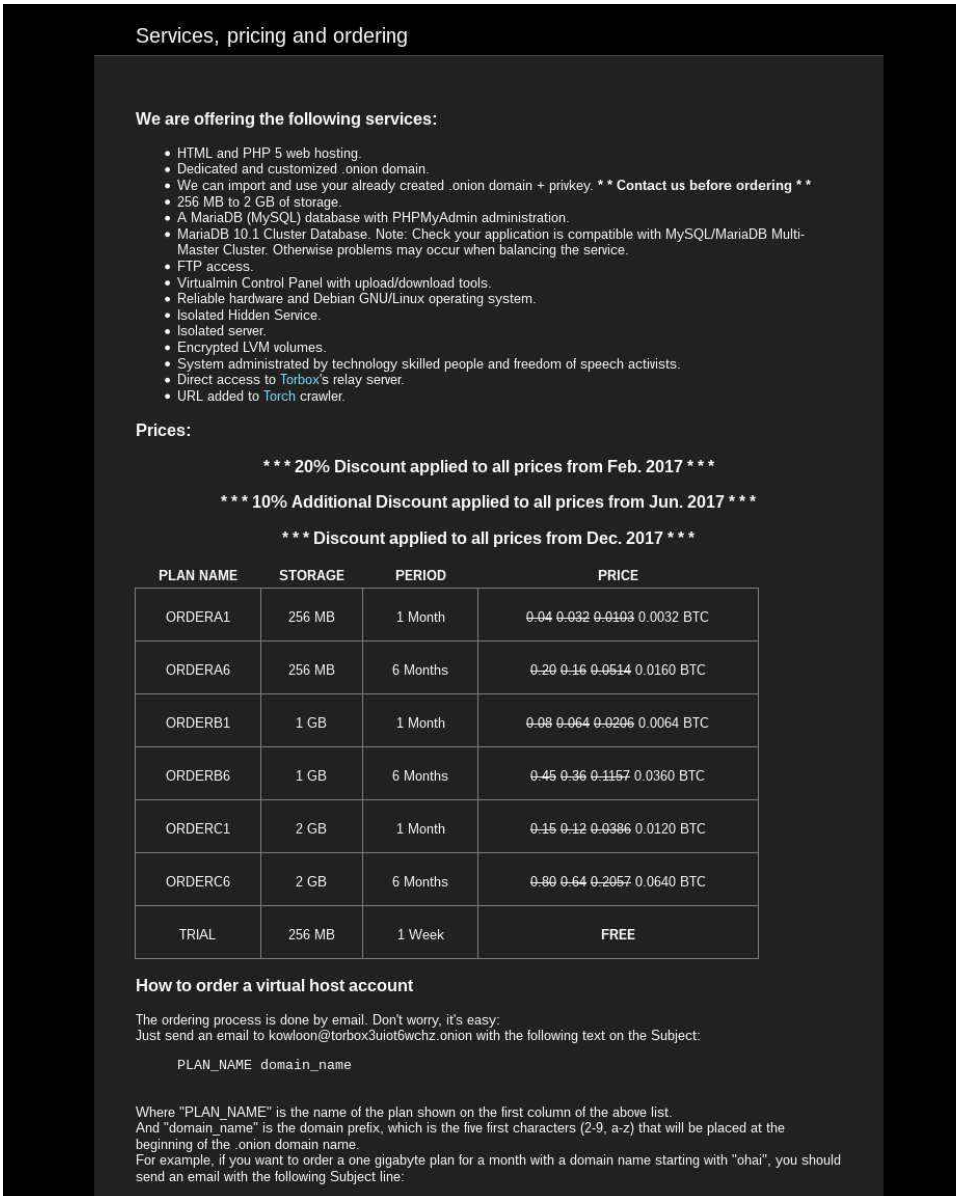
Vendor fees can be too expensive for new dark netters to start a business on the dark net. In a forum post, one user asks how to sell ransomware on the dark net while escaping the vendor fees imposed:

"where i can sell my ransomware at $ .. without vendor fee"

The forum moderator responds:

"Put up a website and do direct deals? I'm interested, could I have a look at your ransomware?"

Rogue hosting services have been introduced before by Yip [57]. Several hosting options are available on the dark net and all of them vary in prices and subscription packages. Figure 5.16 shows one of the rogue hosting services popularly advertised on forums. Those behind this particular service have organized a concise business plan to attract as many customers as possible by offering discounts and free trial for a week's use. For 6 months, an individual can host a website for the approximate price of 1000 US Dollars. This can save up to 800 US Dollars for the vendor, and eliminate any commission fees. When RaaS is hosted on a privately-owned website, the vendors market their product on forums that allow advertising of goods and services. During the research, several instances of privately owned vendor shops were noticed. Most of them are listed in Appendix C.1.



Services, pricing and ordering

We are offering the following services:

- HTML and PHP 5 web hosting.
- Dedicated and customized .onion domain.
- We can import and use your already created .onion domain + privkey. *** * Contact us before ordering * ***
- 256 MB to 2 GB of storage.
- A MariaDB (MySQL) database with PHPMyAdmin administration.
- MariaDB 10.1 Cluster Database. Note: Check your application is compatible with MySQL/MariaDB Multi-Master Cluster. Otherwise problems may occur when balancing the service.
- FTP access.
- Virtualmin Control Panel with upload/download tools.
- Reliable hardware and Debian GNU/Linux operating system.
- Isolated Hidden Service.
- Isolated server.
- Encrypted LVM volumes.
- System administrated by technology skilled people and freedom of speech activists.
- Direct access to Torbox's relay server.
- URL added to Torch crawler.

Prices:

*** * * 20% Discount applied to all prices from Feb. 2017 * * ***

*** * * 10% Additional Discount applied to all prices from Jun. 2017 * * ***

*** * * Discount applied to all prices from Dec. 2017 * * ***

PLAN NAME	STORAGE	PERIOD	PRICE
ORDERA1	256 MB	1 Month	~~0.04~~ ~~0.032~~ ~~0.0103~~ 0.0032 BTC
ORDERA6	256 MB	6 Months	~~0.20~~ ~~0.16~~ ~~0.0514~~ 0.0160 BTC
ORDERB1	1 GB	1 Month	~~0.08~~ ~~0.064~~ ~~0.0206~~ 0.0064 BTC
ORDERB6	1 GB	6 Months	~~0.45~~ ~~0.36~~ ~~0.1157~~ 0.0360 BTC
ORDERC1	2 GB	1 Month	~~0.15~~ ~~0.12~~ ~~0.0386~~ 0.0120 BTC
ORDERC6	2 GB	6 Months	~~0.80~~ ~~0.64~~ ~~0.2057~~ 0.0640 BTC
TRIAL	256 MB	1 Week	**FREE**

How to order a virtual host account

The ordering process is done by email. Don't worry, it's easy:
Just send an email to kowloon@torbox3uiot6wchz.onion with the following text on the Subject:

```
PLAN_NAME domain_name
```

Where "PLAN_NAME" is the name of the plan shown on the first column of the above list.
And "domain_name" is the domain prefix, which is the five first characters (2-9, a-z) that will be placed at the beginning of the .onion domain name.
For example, if you want to order a one gigabyte plan for a month with a domain name starting with "ohai", you should send an email with the following Subject line:

Figure 5.16: Rogue hosting service with offers and different subscription plans

5.5 Cost Benefit Framework of Dark Net Activities

The cost-benefit framework was devised based on the literature mentioned in the background study and the netnographic observations. In this section, the framework used to decompose costs and benefits are presented.

5.5.1 Decomposing Costs

The framework used to decompose costs imposed on victims of a malicious infection presented by [4] was sufficient enough to decompose the costs to run ransomware-as-a-service. The framework can be adjusted to be applicable for a cybercriminal perspective. These adjustments are based off the netnographic representation. The final framework is illustrated in Figure 5.17. The OPSEC (defence), indirect and direct costs are explained in further detail with examples on each.

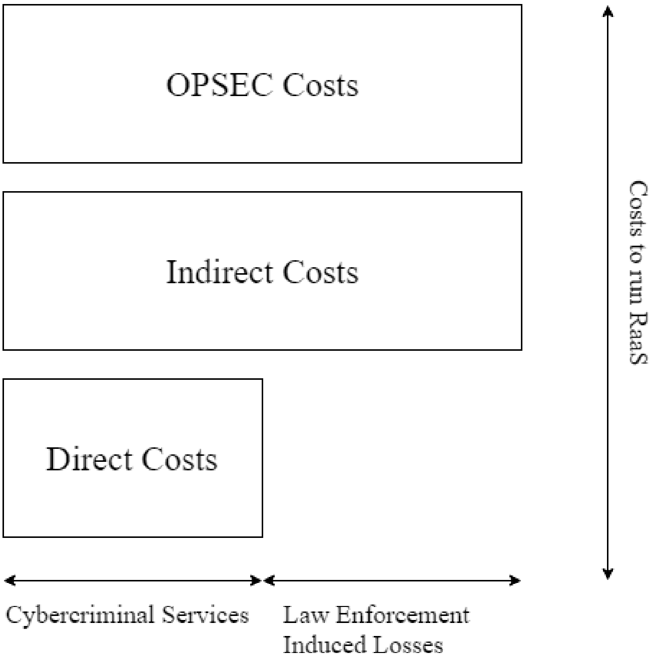


Figure 5.17: Cybercrime costs framework

5.5.2 Defence Costs

Operational Security or (OPSEC) is the process that identifies whether the person in contact with is someone to trust or an enemy spy. In other words, OPSEC is a precautionary process required to protect oneself from a possible arrest by law enforcement. In dark net forums, dark netters have openly discussed OPSEC recommendations and previous experiences of fallen dark netters who failed to protect themselves and were easily caught by law enforcement. OPSEC is a costly process and not investing money in it would result in undesired circumstances for the typical dark netter. Although OPSEC differs from the laws of one country to another, the best OPSEC as recommended in dark net forums are as follows:

- Legal costs
- Cryptocurrency Tumbling
- Hire *drops* for physical meetups
- Encryption of hard drives

Legal costs differ from one country to another. Developing nations that do not have strong law enforcement have low legal costs. However, an increase in international law enforcement cooperation may lead to higher costs. A rule of thumb is to acquire a lawyer to represent you in case of an unexpected arrest. These require

Cryptocurrency tumbling is a precautionary method used to conceal the transfer or cashing out large sums of cryptocurrency money. In case of physical meetups in other cases of fraud, a *drop* is hired to go instead of the cybercriminal. Lastly, in one of the quoted text, a forum member stressed out the importance to encrypt all hard drives that contain data that can be used for prosecution. While encryption algorithms are free to acquire, the time spent does cost money for the cybercriminal and therefore is regarded a cost.

5.5.3 Indirect Costs

Indirect costs are imposed when the cybercriminal has ignored a necessary precaution or experienced unfortunate circumstances that have a negative impact on the vendor's career in the dark net. Examples of indirect costs are:

- Prosecution charges
- Loss of reputation
- Marketplace scams

5.5.4 Direct Costs

Direct costs include expenses imposed on the vendor to develop the ransomware. These expenses are managed by the vendor and can be adjusted to suit the budget. Examples of direct costs are:

- Rogue Hosting Services
- Vendor fees

- Commission fees
- Exploit toolkits
- User Interface Development Services

5.5.5 Benefits of Ransomware-as-a-Service

The monetary benefit behind ransomware-as-a-service was very difficult to acquire considering the lack of literature and the discreteness of malware authors from the marketplace economy. The malware authors recognized in this research were those who were interviewed by DeepDotWeb and later turned out to be script kiddies. However, an attempt to compute the profit margin from accounts released by victims of ransomware variants was used for this research.

Computed Profit Margin

The profit margin per infection of ransomware variants can be calculated by including the cost of ransomware on cryptomarkets as the actual cost, and the ransom amount as announced by the victims. On average, the ransom is around 300 USD, however, some ransomwares place a low value, possibly due to the fact that it can be easily be decrypted. The profit margin for each ransomware can be calculated using the following equation:

$$P = (p_i - c)/c \tag{5.1}$$

- p_i is the ransom amount asked by victim i.
- c is the price of the ransomware-as-a-service items.

The equation represents a basic cost-benefit trend analysis. During the research, an attempt was made to compute the profit margin of the prominent ransomware-as-a-service mentioned in Figure 5.11. Not all could be computed since information relating to the ransom amount for every variant is unknown. However, the estimates are concluded in Table 5.14

Ransomware Variant	Price	Ransom Amount	Profit Margin
NoobCrypt	300	300	0%
PHP CTB-Locker	250	170	-32.00%
Cryptolocker	200	300	50.00%

Table 5.14: Profit Margin of every known ransomware variant, all prices listed in US Dollars

6

DISCUSSION

This Chapter includes a revision of the findings and the background study presented in the beginning of this report. Interpretation of the findings and empirical analysis are connected with the concepts mentioned in the literature reviewed. The Chapter ends with a brief explanation of the challenges and limitations faced during the research study.

6.1 Cost-Benefit Framework of Ransomware-as-a-Service

A cost-benefit framework of organized cybercrime presented by Anderson et al. [4] was adjusted and extended to be applied to the economy of Ransomware-as-a-Service. The proposed framework decomposes the costs into three categories; OPSEC, direct and indirect costs. Distinguishing the costs based on these categories constructs a flexible framework that can be applicable to the different cybercrime attacks. In addition, it considers factors that directly impact the success of cybercriminals.

One factor addressed in the background study is the level of development of the country in which the cybercriminal is committing these crimes. In developing countries, the psychic opportunity costs and legal costs are low on average. Individuals in these countries are eventually encouraged to partake in cybercriminal activities.

Legal costs and unemployment rate in the country has a direct impact on the prospects of a career on the dark net. As mentioned earlier, carding services are far more popular than ransomware-as-a-service items in English marketplaces and forums when it comes to fraud. Whereas some of the exploit kits and ransomware variants that have been introduced in the past few years are traced back to Russian forums. Russia compared to the English speaking countries, stresses out STEM subjects in their school curricula. However, the unemployment rate is high or the income of software development positions are satisfactory enough. This encourages more Russians to get involved in the dark net.

The development and distribution of RaaS is considered an act of digital fraud, and can be labeled as an organized cybercrime based on the definition presented by European Commission [22]. The cost-benefit framework used for organized cyber-criminal activities can be extended to ransomware-as-a-service. The costs imposed were deduced based on information shared by dark net members on dark net forums and from hidden services that are part of the underground economy value chain. The model was presented in Section 5.5.

Scarcity of research papers on the underground economy of RaaS has been a troubling issue throughout this research. The only reports to claim from the dark net are published by cyber security vendors such as the report written by Carbon Black [8]. These are not authentic sources since they are published mainly for marketing reasons.

In consequence, the extent to how accurate and precise this framework is can only be known once its applied to an actual case study in which an entire RaaS value chain has been exposed. As of writing this report, there is no such case study since many of the successful ransomware variants we know of today are developed by unknown miscreants that have not been identified. Those who have been arrested and charged worked solo and were not part of any value chain.

It is safe to say that the framework derived can be a promising start to cost-benefit analysis of ransomware-as-a-service, it constitutes the basic costs imposed on any cybercriminal on the dark net. This is backed by information in dark net forum posts.

6.2 Activities in dark net forums

Forums are a good source for anyone willing to start a business on the dark net. Public forums offer the opportunity for members to share knowledge and eventually improve their skills and create partnerships with other interested members. Getting into an invite-only forum requires history with dark net activity, and this could be achieved through prolonged discussions on the public forums.

The sociograph presented by Holt et al. [29] for connectivity and centrality of dark net members shows how the low-skilled hackers have fewer connections, but the highly skilled are aware of their peers. This is evident in forum activities. Those who acquire are indeed low-skilled and publicly post on forums, putting them at the edge of the sociograph. Whereas the highly skilled are usually active in invite-only forums or have been assigned to be the moderator of the forum.

In OnionLand, the forum moderator created a concise tutorial with classes on all sorts of issues regarding the underground economy of the dark net. This acts as an educational tool for any low-skilled dark net members. Once they've learned enough to buy and sell illegal goods, make partnerships and eventually become involved in an invite-only forum. With that being said, one additional point has to be added to the findings by Holt et al. [29] and that is *high-skilled members have the ability to strengthen low-skilled members on the dark net through forum discussions*.

6.3 Service Innovation in the Dark Net

Despite the fact that ransomware-as-a-service is not popular in English marketplaces and forums, the competition is still high in the dark net. Traces of RaaS with *revolutionary* features have been observed during the research and are mentioned in Section 5.4.1.

From this item, we can deduce that malware authors are striving to get hold of a high reputation and stable position in the dark net communtiy. Ransomware-as-a-service can evolve in the coming years to include more features that offer control to the distributor over the victims' devices.

6.4 Improving Threat Intelligence

The purpose of creating an actor profile is to identify the psychological aspects of every actor involved in RaaS. This was established from claims made by prominent dark net members in interviews conducted by DeepDotWeb. The questions asked by the interviewers were in sometimes not thorough enough to create an actor profile. Additionally, some of the feedback addressed in the interviews offer a different perspective of what the claims made by the interviewees. Forum discussions also contributed to the validation of some of these claims.

When profiling the actors based on the interviews, the roles presented by Yip [57] were used to make connections based on the responsibilities mentioned. Aside from marketplace administrators, the TheRealDeal administrators also mentioned how active they were in the dark net as researchers for zero-day exploits. This made it possible to create a profile for vulnerability researchers based on the interview with TheRealDeal actors.

The research industry must take part in forums and get hold of interviews similar to the ones conducted by DeepDotWeb. Mentioning that the interview is done for research purposes may not sound welcoming for many, but a trial is better than none. The outcomes of forum interviews and questions can benefit threat intelligence and attacker-centric modeling.

Ransomware is still the best method of fraud when it comes to distribution and profitability. Although businesses and individuals have invested more effort to combat any possible ransomware infection, changes in the cybercrime ecosystem need to be studied as this may lead to new cybercriminal offences. The Philadelphia ransomware incident shows how competitive the underground economy can be, and this can lead to creative methods to attract as many consumers as possible to buy ransomware-as-a-service.

With that said, dark net studies have been successful at estimating numbers with previous such as Silk Road and the underground economy of drug trafficking.

6.5 Netnographic study on the dark net

The netnographic framework presented by Kozinets Robert [34] was tied to social media examples in the book. In other words, Kozinets focused mainly on online communities that are open to the general public, and do not take part in illegal activities much like the members of the dark net. Consequently, the ethical considerations suggested by Kozinets' is inconsistent with the online community of the dark net.

Bakken [6] was a suitable source when considering the ethical implications. However, the research goals of this study differ greatly compared to that of Bakken [6]. Added to that, the method of netnographic representation was *Symbolic* and *Humanist*, no digital method to visualize the data was used.

Netnographic study is a good methodology to understand and experience the social structure of an online community. However, the framework presented by Kozinets must be adjusted for a more inclusive approach towards hidden communities in the dark net. The netnographic study was good to deduce which websites should the research be part of the immersion phase, and what are the expected outcomes.

6.6 Limitations

Research in the dark net imposes many threats that need to be considered. Attempting to apply into an invite-only forum is both difficult and may ensue a criminal act. Having said that, ethical implications made it really difficult to have a full experience on dark net forum posts.

English based dark net marketplaces and forums are more concerned with drug related items and carding services. However, Russian based forums and marketplaces could have offered more data for the empirical analysis. Language has, thus, been a major challenge. Using online translation services was not possible because this may increase the risk of interception.

To combat the limited timeframe invested in this research, data was retrieved from previous crawls made by other researchers. This was useful to compare the price tags of RaaS items across time. However, some of the data crawls were incomplete. For instance, Gwern's dataset lacked the images in the websites, and in some dates, crawls were not successful due to the marketplace's DDoS protection. The data visualized in this report used the complete crawls only.

Added to that, no other marketplace has reached the same level of success as AlphaBay. After its shutdown, there was no other method to access data from AlphaBay except through the data dumps provided by Gwern [26]. Although the data included in the data dump is appreciable, the AlphaBay crawls for ransomware were limited between the years 2011 and early 2016. Data after 2016 could have covered the effects of the Petya and WannaCry ransomware.

Aside from ethical implications, interaction with public forum members was also struggle. When posting a question in the forum and informing the members that this question is asked for research purposes, there would be no response to the thread. However, when using a different user account, asking the same question but not mentioning the intent behind it, many responses were received. The questions asked were basic to any new dark net member and did not go against my ethical position. This case shows how much dark net members do not prefer interacting with researchers.

Lastly, the limited time was a challenge. More findings could have been presented if the duration of this research was longer. Hopefully in the future, this research will continue and more information will be built on it.

7

CONCLUSION AND FUTURE WORK

This Chapter includes the conclusion with answers to the research questions based on the findings and discussion. The Chapter concludes with recommendations for future work on this research.

7.1 Conclusion

RQ1 What are the behavioural aspects of members involved in the underground economy of ransomware in the dark net?

From the information included in the interviews with prominent dark net members and discussion threads of dark net forums, an actor profile was presented in Section 5.3.

RQ1.1 What is the nature of the activities practiced by the online community within the dark web market forums?

With respect to ransomware-as-a-service, most members post topics on how to acquire the service. Members also share their experiences with vendors on purchases and give reviews on the quality of the products. Moderators give advice on how to combat vendor scams to the less-informed members of the dark net. The detailed interpretation of the observations is presented in Section 5.2.

RQ1.2 What are the economic incentives and risks behind the actions of darknet members?

The quality of the RaaS sold in popular marketplaces were questionable, thus imposing the idea that these vendors wish to scam any buyer on the dark net (Section 5.2.3). Others who have developed ransomware, host it on a privately-owned website and ask for share of the ransom revenue (Section 5.4.3). For some of the members, the psychic opportunity costs of distributing ransomware is very high (Section 5.2.2). These individuals prefer to take part in fraud with minor collateral damage. Lastly, many of the members either seek partnerships to build an economy of RaaS or damage the reputation of a fierce competitor (Section 5.4.2).

RQ2 What is the business model of Ransomware-as-Service?

The pricing scheme of ransomware-as-a-service has shed light on what impacts the value of the ransomware. The fees imposed on vendors that wish to sell their services on dark net marketplaces was also mentioned. This is explained in Section 5.4.

RQ2.1 What are the cost-benefit estimates of ransomware sold on the dark net?

Analysis of cost-benefit tradeoffs were based on a set of factors. The costs were split into three categories: OPSEC costs, indirect costs and direct costs. The costs that are categorized into one of these three were retrieved from forum data. The revenue was based on the victim's willingness to pay and the complexity of the encryption algorithm 5.5.

RQ2.1 What is the organizational structure of the economy of Ransomware-as-a-Service?

Based on the different roles identified in the interviews and forum discussions, an actor profiling was created and a value chain of the economy of ransomware-as-a-service was modelled in Section 5.3.

7.2 Recommendations for Future Work

This research is a promising start to the field of cyber security threat intelligence. However, cryptomarket research has yet to improve and more focus needs to be applied on the development and distribution of ransomware-as-service. The following points address what aspects need to be improved or added to the research.

7.2.1 Monitoring of Cryptocurrency Inflow

Tracking the amount of Bitcoin going into the wallets linked to a ransomware variant can give us better estimates on how much money is profited by the stakeholders involved in ransomware-as-a-service. A Twitter bot managed by Quartz tweets every amount of money deposited into and withdrawn out of one of the wallets of WannaCry [15]. Victim's can share the wallet key with cybersecurity experts, making it easy to retrieve.

7.2.2 Netnographic Study on the Russian Cybercrime Economy

As mentioned earlier, the dark net landscape differs greatly based on the citizenship of the cybercriminals. It was also mentioned by the interviewed dark net money launderer in Appendix A.2. Russian forums are known to have posts on exploit kits and RaaS being sold to its members. Including these forums to the netnography can give us insight to eh. It can give us insight on the different economic

7.2.3 Mining of Dark Net Marketplaces and Forums

Real-time crawling can offer real-time analysis of RaaS items on the dark net. As mentioned in Section 5.4, price fluctuations of a RaaS item was detected in the AlphaBay data dumps crawled by Gwern [26]. Extracting several instance of price changes can help us deduce a more precise assumption. Therefore, a real-time crawling algorithm developed specifically for dark net markets could be a good addition to this research.

BIBLIOGRAPHY

[1] Google scholar. `https://scholar.google.no/`. Accessed: 2018-05-16.

[2] Mendeley. `https://www.mendeley.com/`. Accessed: 2018-05-16.

[3] Scopus. `https://www.scopus.com/`. Accessed: 2018-05-16.

[4] Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., Moore, T., and Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy*, pages 265–300. Springer.

[5] Andy Greenberg (2018). Operation bayonet: Inside the sting that hijacked an entire dark web drug market. [Online; accessed 20-May-2018].

[6] Bakken, S. A. (2015). Silk road 2.0-a study of cryptomarkets in a deleuze-guattarian perspective. Master's thesis.

[7] Bayoumy, Y., Meland, P., and Sindre, G. (2018). A netnographic study on the dark net ecosystem for ransomware.

[8] Black, C. (2017). The ransomware economy. `https://www.carbonblack.com/wp-content/uploads/2017/10/Carbon-Black-Ransomware-Economy-Report-101117.pdf`. (Accessed on 10/16/2017).

[9] Blaze, M., Feigenbaum, J., and Lacy, J. (1996). Decentralized trust management. In *Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on*, pages 164–173. IEEE.

[10] Böhme, R. (2010). Security metrics and security investment models. In *International Workshop on Security*, pages 10–24. Springer.

[11] Cárdenas, A., Radosavac, S., Grossklags, J., Chuang, J., and Hoofnagle, C. (2009). An economic map of cybercrime.

[12] Ceci, F., Prencipe, A., and Spagnoletti, P. (2018). Evolution, resilience and organizational morphing in anonymous online marketplaces. In *AOM Specialized Conference, Big Data and Managing in a Digital Economy*.

[13] Choo, K.-K. R. (2008). Organised crime groups in cyberspace: a typology. *Trends in organized crime*, 11(3):270–295.

[14] Christin, N. (2013). Traveling the silk road: A measurement analysis of a large anonymous online marketplace. In *Proceedings of the 22nd international conference on World Wide Web*, pages 213–224. ACM.

[15] Collins, K. (2017). Victims of the wannacry ransomware attacks have stopped paying up.

[16] Deep Dot Web (2017a). Best vpn services: Vpn comparison chart. [Online; accessed 14-May-2018].

[17] Deep Dot Web (2017b). Deepdotweb. [Online; accessed 14-May-2018].

[18] Demant, J., Munksgaard, R., and Houborg, E. (2016). Personal use, social supply or redistribution? cryptomarket demand on silk road 2 and agora. *Trends in Organized Crime*, pages 1–20.

[19] dirtyfilthy (2017). Fresh onions tor hidden service crawler. `https://github.com/dirtyfilthy/freshonions-torscraper`.

[20] Dolliver, D. S. (2015). Evaluating drug trafficking on the tor network: Silk road 2, the sequel. *International Journal of Drug Policy*, 26(11):1113–1123.

[21] Ehrenfeld, J. M. (2017). Wannacry, cybersecurity and health information technology: A time to act. *Journal of medical systems*, 41(7):104.

[22] European Commission (2007). Towards a general policy on the fight against cyber crime.

[23] Everett, C. (2016). Ransomware: to pay or not to pay? *Computer Fraud & Security*, 2016(4):8–12.

[24] Fossheim, H., Ingierd, H., Elgesem, D., Ess, C., Larsson, A. O., LÃ1/4ders, M., Prabhu, R., Segadal, K. U., Staksrud, E., Steen-Johnsen, K., et al. (2017). Internet research ethics.

[25] Geddam, L. G., Doerr, C., Janssen, G., and van der Lubbe, J. (2017). Understanding the topological structure and semantic content of darknet communities.

[26] Gwern Branwen, Nicolas Christin, D. D.-H. R. M. A. S. E. P. A. D. L. S. D. K. V. C. V. B. W. M. M. S. G. (2015). Dark net market archives, 2011-2015. `https://www.gwern.net/DNM-archives`. Accessed: 2018-02-15.

[27] Hernandez-Castro, J., Cartwright, E., and Stepanova, A. (2017). Economic analysis of ransomware.

[28] Holt, T. J., Bossler, A. M., and Seigfried-Spellar, K. C. (2015). *Cybercrime and digital forensics: An introduction*. Routledge.

[29] Holt, T. J., Strumsky, D., Smirnova, O., and Kilger, M. (2012). Examining the social networks of malware writers and hackers. *International Journal of Cyber Criminology*, 6(1):891.

[30] Huang, D. Y., McCoy, D., Aliapoulios, M. M., Li, V. G., Invernizzi, L., Bursztein, E., McRoberts, K., Levin, J., Levchenko, K., and Snoeren, A. C. (2018). Tracking ransomware end-to-end. In *Tracking Ransomware End-to-end*, page 0. IEEE.

[31] Irwin, S. (2014). Creating a threat profile for your organization.

[32] Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., and Kirda, E. (2015). Cutting the gordian knot: A look under the hood of ransomware attacks. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 3–24. Springer.

[33] Kotov, V. and Rajpal, M. S. (2014). Understanding crypto-ransomware: In-depth analysis of the most popular malware families. Technical report, Tech. rep. Bromium.

[34] Kozinets Robert, V. (2015). Netnography. redefined.

[35] Kraemer-Mbula, E., Tang, P., and Rush, H. (2013). The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change*, 80(3):541–555.

[36] Kshetri, N. (2006). The simple economics of cybercrimes. *IEEE Security & Privacy*, 4(1):33–39.

[37] Kshetri, N. (2010). *The global cybercrime industry: economic, institutional and strategic perspectives*. Springer Science & Business Media.

[38] Laszka, A., Farhang, S., and Grossklags, J. (2017). On the economics of ransomware. In *International Conference on Decision and Game Theory for Security*, pages 397–417. Springer.

[39] Lee, J. and Lee, K. (2016). Spillover effect of ransomware: Economic analysis of web vulnerability market.

[40] Lewis, S. J. (2017). Dark web data dumps. `https://polecat.mascherari.press/onionscan/dark-web-data-dumps`.

[41] Liao, K., Zhao, Z., Doupé, A., and Ahn, G.-J. (2016). Behind closed doors: measurement and analysis of cryptolocker ransoms in bitcoin. In *Electronic Crime Research (eCrime), 2016 APWG Symposium on*, pages 1–13. IEEE.

[42] Markham, A., Buchanan, E., Committee, A. E. W., et al. (2012). Ethical decision-making and internet research: Version 2.0. *Association of Internet Researchers*.

[43] Martin, J. and Christin, N. (2016). Ethics in cryptomarket research. *International Journal of Drug Policy*, 35:84–91.

[44] Michael McKenna / Sigi Goode (2017). Alphabay crawl 20170128.

[45] Oates, B. J. (2005). *Researching information systems and computing*. Sage.

[46] Obreja, A.-R., Hart, P., and Bednar, P. (2016). Potential benefits of the deep web for smes. In Caporarello, L., Cesaroni, F., Giesecke, R., and Missikoff, M., editors, *Digitally Supported Innovation*, pages 63–80, Cham. Springer International Publishing.

[47] O'Gorman, G. and McDonald, G. (2012). *Ransomware: A growing menace*. Symantec Corporation.

[48] Probasco, J. and Davis, W. L. (1995). A human capital perspective on criminal careers. *Journal of Applied Business Research*, 11(3):58.

[49] Ritter, A. (2006). Studying illicit drug markets: Disciplinary contributions. *International Journal of Drug Policy*, 17(6):453–463.

[50] SingCERT (2016). Ransomware. `https://www.csa.gov.sg/singcert/news/advisories-alerts/ransomware`. (Accessed on 02/28/2018).

[51] Soska, K. and Christin, N. (2015). Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. In *USENIX Security Symposium*, pages 33–48.

[52] Sutcliffe, K. M. and Vogus, T. J. (2003). Organizing for resilience. *Positive organizational scholarship*, pages 94–110.

[53] Tuttle, H. (2016). Ransomware attacks pose growing threat. *Risk Management*, 63(4):4.

[54] van Wegberg, R., Verburgh, T., van den Berg, J., and van Staalduinen, M. (2017). Alphabay exit, hansa-down: Dream on? *TNO*.

[55] Whonix (2017a). Comparison with others - whonix documentation. [Online; accessed 14-May-2018].

[56] Whonix (2017b). Donot - whonix documentation. [Online; accessed 14-May-2018].

[57] Yip, M. (2010). *An investigation into Chinese cybercrime and the underground economy in comparison with the West*. PhD thesis, University of Southampton.

[58] Yip, M., Webber, C., and Shadbolt, N. (2013). Trust among cybercriminals? carding forums, uncertainty and implications for policing. *Policing and Society*, 23(4):516–539.

[59] Zhuge, J., Holz, T., Song, C., Guo, J., Han, X., and Zou, W. (2009). Studying malicious websites and the underground economy on the chinese web. In *Managing information risk and the economics of security*, pages 225–244. Springer.

Appendices

A Interviews

A.1 TheRealDeal Administrators

What can you tell us about yourself / your market? Ok, basically we consist of 4 partners who have a lot of experience in infosec. We have a lot of experience dealing in the clearnet when it comes to 0day exploit code, databases and so on .. But the problem is that 90% of these dealers are scammers. People with a lot of experience can always do their best to determine if what they are buying is real based on technical information and demos but some of these 'vendors' are very clever and very sneaky. We decided it would be much better if there was a place where people can trade such pieces of information and code combined with a system that will prevent fraud and also provide high anonymity.

We started off by using BitWasp, fully aware of its history and flaws, but since we have years of hands-on experience in the security industry and not much in web-design we decided it would be a good platform since we can make our own security assessments and patches while the whole multi-sig seems to work perfect. We also wanted to avoid involving other people in the project for obvious reasons and that was another reason why not to hire a web designer etc... although we might hire one off the darknet soon, just to improve the UI a little.

On our market you can currently find 0day exploits, that have no cve and have never been disclosed before, 1day fud exploits - exploits that have been published but modified to be undetectable by any anti-virus, 1day private exploits - exploits that have known CVEs but code was never released for them and also Infomation such as databases and remote admin tools. One of our vendors who messes around with GSM a lot is also going to post a listing for some very interesting hardware soon.

And why not use the digital items section on one of the existing markets like Agora where such items are being sold anyway? Never seen 0day exploit code on any of these markets. We actually tried selling such information and codes ourselves at some point but it seems that all people want on those markets is credit cards and tutorials on how to make money with credit cards. There are some IRC servers that are not easy to find or be invited to, where you can trade such items, but they are very hard to get to and we wanted to take a more 'open-market' approach IRC servers on the darknet i mean..

Are offering Multisig transactions? Yes, at this point in time we are offering only multisig transactions -We figured that you can't start a market with zero reputation and expect people to just deposit into a live wallet they have absolutely no control of, that sort of idea sounds crazy to us. We are also offering FE for vendors who join and have good reputation on other markets by the way.

Will you be offering other products on the market or just code / 0days / expoits? We recently added drugs due to the high demand, traditional for darknet markets, but we might consider removing this, we will have to see in the future. There is also a "services" category - anything can go there but we are hoping for some high quality blackhats to come forward and offer their services .. so anything from obtaining access to an email and getting a certain document and up to long term campaigns. Hardware category - for toys like fake cellular base stations and other physical ‘hacking’ tools. Information category for any kind of information, documents, databases, secret keys, etc.. We are also open to suggestions from our vendors :)

What is the vendor bond on the market? We are currently offering free vendor accounts for 24 hours or so... we would love to see some new listings and inactive accounts will have to be removed after a certain period of time. After that the fee will start at somewhere around 0.2-0.5 BTC until the market is stable and earned the right to ask for more.

A.2 Money Launderer

I seen you around many times, And I am still not sure what you do exactly - i know its something in the money laundering area. lol yeah for the most part. Well Im getting a bit of a fan base at the moment... Ever since users found out i was a female, they have been developing crushes on me... Ive been called the "Agora angel"

Of course we can never tell if you really are a female or just saying that as part of your OPSEC / Marketing - but i am sure it works well, it always does. Haha. well Ive been thinking of a way to anonymously post cleavage but its still in the works lol Haha.. Ive been asked to send my underwear... so I request like that is a little less shady...

So what do you do exactly? what can you tell us about your services? Sure, so pretty much I open up bank accounts with stolen identities, these people don’t know about it and thus vendors (or high frequent buyers) can use them to cash in and out Bitcoin as they wish. I also offer burn phones, and in the process of opening my own stolen Credit Cards/PayPal cash out operation.

How much do you charge for those services? The DIY kits for bank accounts are $999. However I do offer to complete the service for them for $1500. It seems a little pricey to most, but people are willing to pay for the anonymity of cashing out their funds :)

Let me explain the process as i understand it and tell me if i am right:

- **You steal people identities**
- **Open bank account with this ID somehow (you have do to it anonymously as well)**
- **Vendor deposit converted BTC into those accounts**
- **Vendor cashing them out using ATM’s and such?**

Pretty much. I offer all the tools in between as well to trade the bitcoin to cash at market rates with a coinjar account which is an Australian based version of btc-e.

Isn’t the last part is super dangerous for the vendor - i mean someone knows he owns a certain bank account so its easy to know the location where he is cashing out? not at all. Ive been using mine for almost a year now. Most ATMs in Australia don’t have cameras or anything. so you can walk up, withdraw no questions asked.

Are you offering your service only in AUS or international? The account is Australia based, but I do have an "international roaming" service available also

Who are your main customers? Mostly vendors, who need a way to cash out anonymously. and are sick of losing half their profits to LB traders lol. Ive also been approached by more darker members beyond our community but Im yet to get back to them lol

Darker members like...? People who specialize in robbing overseas banking institutions, electronically of course.

Can you estimate the size of your operation turnover? (i mean the amount of money laundered trough it) Close to 10k. which is OK considering I started in December. I cant speak for the amount of cash that has gone through bank accounts I have sold. Still new

This is not much at all . So you sold less than 10 packs of your service so far? Yeah, only a few. My main sellers are the ID's themselves, and burn phones.

Fake ID's? ID scans. So its a real person. Someone buys the info and gives it to a vendor to put on the fake ID. you can use it if you get pulled over by police, open PO boxes, apply for loans etc.

On which markets are you active? Agora mostly. Also on Evolution. Most of the business comes from Agora.

I have seen you are very active on Agora forums. Haha. yeah. I deal with their PR of sorts...

Like what..? i have not seen any active promotions from them Oh, haha no I mean like when they are going to be down and stuff like that, they usually tell me, so I can go on and spread the word lol

Your service also sounds like a good thing for market admins. Haha yeah, I keep an eye on the forums for them

Now, tell me a bout the people who have their identity stolen from them - don't you care it might get them into troubles? accounts with their names cashing out drugs money or ID's used for felonies. Lol well they don't know its been stolen... ignorance is bliss I guess. They don't know, but it can get them into troubles without them knowing, they will be the first to be contacted by police. Regardless of what people say, you cant have any morale in this game. I can offer quality customer service, but at the end of the day, I know what Im doing is wrong. and frankly I don't care...

Ok, as long as you understand that this is NOT a victimless crime. Haha absolutely not. Ive always been a bad girl ;)

I guess you provide the same service for stolen CC / PP ? Its a work in progress. I don't actually sell the details. I just help the card holder cash them out. I wrote my own tutorials for personal use, but I think there is a lot of false stigma around "cashing out".

How does one get stolen id's on the regular basis? do you steal them yourself? phish them from sites? I steal them myself. naughty as they come ;)

So you don't give the details - you just use them to open multiple accounts I do have to give some detail from the ID to the buyer, otherwise they wont be able to verify themselves if they need to contact the bank. but things like numbers and all that don't get released, I do charge extra for those.

I see... I would have guessed such service would be much more popular than you described. you have any idea why not? (my personal guess is that most vendors like to use their own methods) To be honest, I don't think many people know about my service. From what I have seen there is only me and one other vendor in the UK who does what we do. most people don't know its an option.

Which leads me to question i always ask - what made want to be interviewed? because I like attention ;) lol jks. that's that womanly side of me.

Do you think it will benefit you in terms of more customers or it might scare off potential customers? (i know there is no bad publicity...) I think it will benefit absolutely, Ive said before in the forums, all publicity is good publicity, plus there are people out there stealing my products at the moment, so I want people to know I am the legit guy (or girl lol). So its also benefiting the customer

What do you mean by stealing your products? There is a vendor on SR2 and Evo, who is reselling my bank accounts for $3000. They copied and pasted my listing details and everything - I found that out thanks to Grams ;)

That's actually a good thing no? you can sell more. Not necessarily. If something goes wrong (and touch wood it doesn't) the vendor reselling actually holds no liability for what happens, where as I offer customer support for after sale. the customer is actually getting ripped off. And Id hate to have that stigma wrapped around my product or service.

Anything else you would like to mention that we did not cover yet / you want to add / topics we need to discuss? Sure, Australian customs laws - something I am real passionate about

Why...? A lot of overseas vendors don't ship to Australia due to our "high border security" - quite frankly its a load of shit, American customs are more diligent than ours and people still send there.

So why is this stigma? Its a myth both vendors and (scamming) buyers need to nip in the bud. with all of today's new security features to combat losing bitcoin to escrow hacks etc, should give enough stance for vendors to allow orders to remain in escrow, If a vendor cannot get a package across an Australia border, than they really need to rethink their stealth methods. because if they can catch it anybody can. Vendors need to stop "selectively scamming" Australians and using the excuse that it was "intercepted by customs" when really they never sent it. And buyers need to tell vendors when they recieved their packages instead of saying it never arrived due to customs. it really deters both parties.

But this concept is so widely accepted. And i think not because of drugs even But because of strict policy about animals. I think a lot of people watch those "border security" type shows based in Australia, and think "holy shit that's tight". when really our postal system runs at that level of security capacity probably less than 10% per day.

I remember from SR1 days that it was very common to have packages missing to AUS... that's why vendors stopped sending there, its hard to say that all vendors want to give up on the AUS market.

Its a shame because they are losing a lot of potential customers. Drugs here cost 150% more than what you can get from America or Germany.

Well so you see that even the local (Non-DNM) market also reacts to the fact that its hard to get the drugs in. Ok an example is xtc pills. on the market, domestic, $30USD, street probably around $22USD. Germany less than $10USD

Obviously... Germany is next to Dutch, where its all produced We produce here too... Wholesale your looking at 15USD a pill

the precursors are probably expensive to import to Aus as well. I mean its very clear why its all expensive there, its an island, and an isolated one so getting stuff in is both expensive and risky. Haha the government is more focused on boat people at the moment than drugs, Drugs in the people people on the boats lol

A.3 Dark Net Developer

Who are you? (like type of person etc...) Best way to describe me would be to say I'm a freedom loving nerd. I've been involved with Bitcoin since it's early days having read the whitepaper not long after its release and have been in love with the concept ever since. I am also a avid cannabis user, so combining two of my passions seemed like a good idea.

You say you are into BTC from the very start, So i guess you did not buy back then...? (did not make early developer profits...) I was one of the unlucky ones who lost a lot on MtGox, I also spent a lot on weed before the madness of 2013.. FML.

What do you do for a living? I'm currently an unemployed web developer, I do a bit of freelancing on the side, but have dedicated myself to this project for the last 3 months or so. The stress and office working environment forced me to quit my job awhile ago, it just isn't for me.

What is the background story that made you decide you want to develop DNM's? The money you saw they generate or what? Well I've been using DNM's personally for many years (only cannabis) and have seen many come and go over that period. I would be lying if I said the money wasn't the driving factor though, we all have bills to pay right?

What is the background story that made you decide you DO NOT want to develop DNM's but rather sell the code? My family. I don't think I could handle the constant looking over my shoulder and god forbid being locked away like Ross.

Which other markets did you experience with? Ever worked for one of the existing / past markets? I've done some security work for a popular DNM which I can't name, but other than that I have only done clearnet Bitcoin related work over the past few years.

You say you have done some security work for past markets; Can you elaborate on this? (without revealing details about the market) I have done some bug bounties and received some decent coin for it, that's about it really.

What do you think on the current security of the active markets? its been a while since we encountered those hacks that were pretty common last year. I think DNM admins have done well in 2015, I think offering reward bounties has played a large part in that. But as for the markets that have been hacked in the past, it's impossible to tell if it was the work of hackers, or if those admins just pulled an exit scam and blamed it on hackers. It does seem like the perfect excuse doesn't it.

You think that someone that doesn't have the knowledge to write its own code could succeed with running a pre built markets? I would expect the buyer to have at least a basic understanding of the language. But then again that's not really my concern, I think as long as they or their partner/s can keep the servers online and not make any basic security mistakes then it shouldn't be an issue.

The price tag seems a bit high! Why? I do agree the price is high, but this is not exactly something you can call your local web development agency to create for you. The 100 BTC BIN price is just what I would like to get for it, not the minimum I'm willing to accept.

What makes your script better than available free scripts (need patching) like Bitwasp or its improved version Aflao? The code is completely bespoke. It is unique and not a 'clone' of anything. Btw, all JS has been removed from the website. Even though it wasn't a security issue since the code was there for everyone to see, I've taken it out to put peoples minds at ease. The layout/aesthetics haven't change too drastically and functionality is unchanged.

What type of features does your market offer that differentiate it from the existing markets? (if any) I think the main difference is that there is no registration or accounts needed, and vendors are hand picked.

Does it have multisig? No.

Will you provide continues support for the buyer? Only for a short period of time after the sale, but I will provide a full deployment/install guide and answer any questions relating to that. As soon as they're online and in business, that's where I walk away.

Had people interested so far? How many? There has been some interest, but nothing significant. There are 2-3 people who seem genuinely interested in purchasing this, but until the first staged payment is made then the offer still on the table and open to bids.

A.4 Forum Moderator

Can you tell us about KickAss forum? KickAss (KA) is a forum with talented hackers and coders on the deep web / dark net. The level of expertise in the forum is very advanced. Every single user in the forum is talented in a different niche. That is why we have an application process in play. We only accept the most advanced users. This process allows us to filter out the newbies, law enforcement, journalists, researchers, and lurkers. Over time, this process allowed us to interview some very talented users. Some of these users are very advanced in mathematics, economics, quantum, and entrepreneurship. Although please keep in mind, it is highly unlikely to enter the forum with irrelevant skills unless it is in demand of users inside the forum. KickAss is also known to have the most popular Insider Trading forum on the dark net.

Are you the admin of the whole forum or just the inside trading? I am part of the staff members of the forum. My responsibility and roles include moderating the Insider Trading forum and the General Discussion forum.

Tell us a bit what is inside trading? Insider Trading is a group or individual that possesses corporate information that has not yet been made public or possibly abandoned information. Because the information is not available to other investors, a person using such knowledge is trying to gain an advantage over the rest of the market by having approximately 100

What is your background in that field? I'm a self-taught cryptographer, economist, investor and entrepreneurial businessman. I don't believe in formal education systems. I believe that a human is given the opportunity to implement creativity to the process and structure of any type of education. You shouldn't be forced to learn something in a certain way. The more comfortable you are, the higher chance you're going to be passionate; which means you're going to learn more and also implement it in your life on a daily-basis. With those two, your means of knowledge is limitless.

How is the information obtained? I see that the only posters of info are the mods and not users? We are a team of seven, and continuously growing as the venture grows. One Economists & One Investor: They look suspicious companies, and future predictions. Three Serial Hackers: They obtain information relating to a potential movement in the market. Two Trading Analysts: They perform quality control and screen all information. KA Staff: After an extensive screening process, we post the information. It takes a lot of work and effort to post a successful published post. The risk of allowing users post their own stuff is risky to our customer's profit. Customer service is key, and we wish to deliver quality information. We'd like to give customers what they're paying for. Users are allowed to post feedback or question into every thread.

How does the insider trading forum works? To avoid any sort of leeching from occurring, we summarize the findings into a structured formality. The first part is summarizing the findings, and the connection to the whole timeline. Then we state the effected markets followed by whether to buy/sell or if the specific market will be going up or down. Then we indicate the important dates, followed by the important dates are stars. 1 to 5 stars, with 5 stars being the most important impact. We indicate the accuracy rate. We only release posts that are higher than 90

How much money have you made using these methods? It all differs, depending how much you leverage. Put it this way, everyone uses different amounts of leverage and risk. You have all the space for the highest percentile projection for trading on any market.

What does it take to get access to the inside trading forum? Your application must be jaw-dropping. We don't really care about your money. We care more about having the right users with the right talent using the Insider Trading sub-forum. You must indicate that you are applying for Insider Trading so we can give you the type of interview. Expect highly advanced questions about economics or trading. After the users have successfully passed an extensive difficult interview that contains challenges and questions to be completed. They are given the opportunity to pay 1 bitcoin a month for their subscription in the sub-forum. That is the exact reason why the staff is the only one allowed to post. The users have gone through a lot to gain membership access and are also paying for their service. They deserve to have accurate and high quality information.

How many members there are currently? There are over 15 investment firms using this sub-forum, and over 25 on-going renewed members. We can easily have over 1000 members, but most of them get declined in the interview stage. You do not pay, unless you pass your application stage.

Can you share any interesting success stories of inside trading? Many users use this to their advantage and leverage high. Some users have made enough for the year off a few well thought-out plans using our information. You can also see the users feedback on every post.

What makes you want to do an interview? Transparency is the reason many people lose there money, or don't understand the market. We make that all clear for you. KickAss forum currently has the most smartest users in the forum. If you are a hacker, stock/currency trader, or extremely talented at something that we could need; then this is the forum we've created for all of you to join. A forum full of smart people.

Why share that info on a forum and not just use it quietly? Its not taking a risk of the info falling into the wrong hands or reported? We do intense screening, having the tiniest suspicion on a user would qualify the user for rejection, and would not make it passed the application stage. Yes we also make money off of this forum, but most importantly we would like the most talented people in trading to join and we have been successful at that.

B Leaked Chat

Malware Distributor: whats the price maan??? :)

Philadelphia Author: But how I know you

Philadelphia Author: I can give discount

Philadelphia Author: $350 :(

Philadelphia Author: * :)

Philadelphia Author: You help me a lot

Malware Distributor: Thats great!

Malware Distributor: no problems mate...I like help others by nature :)

Philadelphia Author: Great guy :)

Malware Distributor: I will talk with my friend now...he must send me coins...or at max I will buy it on next Monday.. Lets' see how this best works.. :)

Malware Distributor: I have some questions..can i ask?

Philadelphia Author: Yes

Malware Distributor: Is encrrpyting algorithm is different than in Stampado?

Malware Distributor: I mean is it faster?

Philadelphia Author: Little more faster

Philadelphia Author: But all ransomwares work in same way

Malware Distributor: Are you considering to make a low-level ransomware?

Malware Distributor: I mean which will encrypt whole HDD not files

Malware Distributor: Anyway very interested in this man :)

Philadelphia Author: Ransomware cant encrypt all HD because can corrupt system

Malware Distributor: I mean like this one: *clearnet URL*

Philadelphia Author: This only rewrite MBR

Philadelphia Author: No big deal

Philadelphia Author: and is no automatic payment

Malware Distributor: ok, but I would be really happy to see how your Philadelphia works..with its nice-looking panel :)

Philadelphia Author: yes friend :)

Philadelphia Author: I start spread today

Philadelphia Author: I want infect 20k today

Philadelphia Author: Until now

Philadelphia Author: 2,7k

Philadelphia Author: infected :)

Malware Distributor: wow great

Malware Distributor: As you are programmer and maybe you know....where can I rent exploit kits such as Angler and Neutrino?

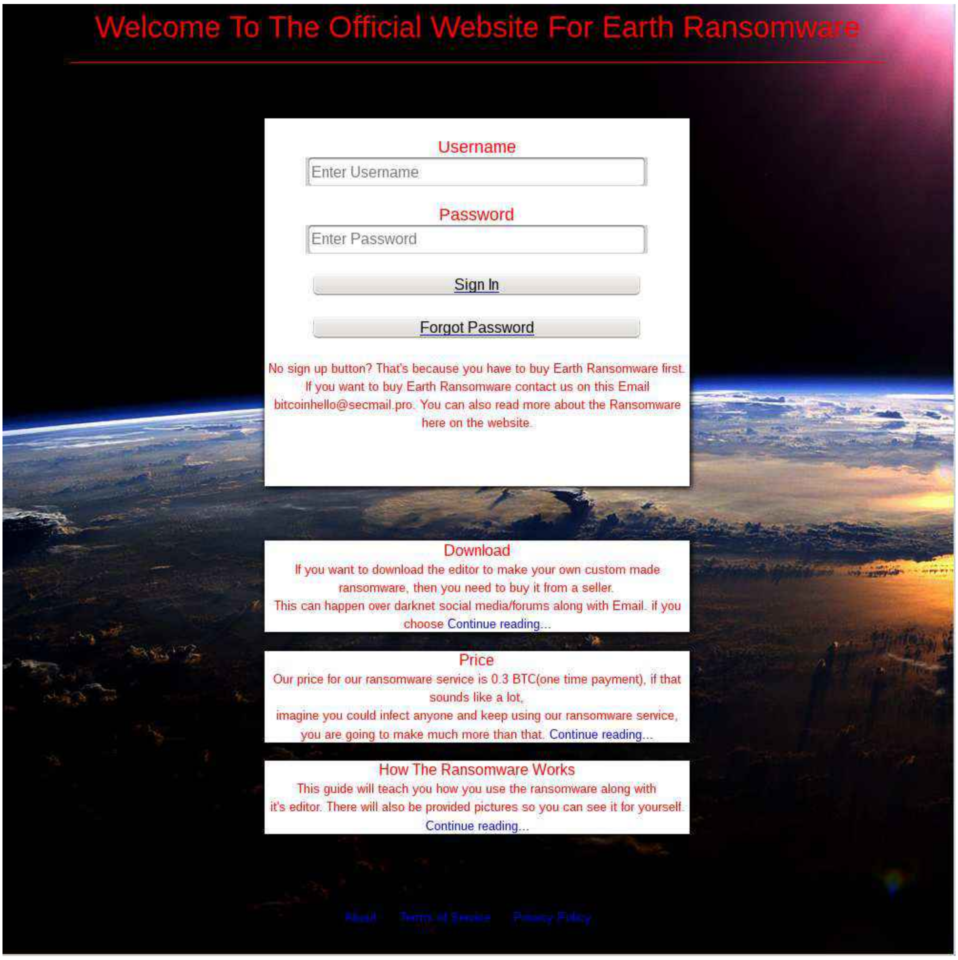
Malware Distributor: do you know any marketplaces or links?

Philadelphia Author: Yes

Philadelphia Author: I use neutrino

C Screenshots

C.1 Private Vendor Shops



Welcome To The Official Website For Earth Ransomware

No sign up button? That's because you have to buy Earth Ransomware first. If you want to buy Earth Ransomware contact us on this Email bitcoinhello@secmail.pro. You can also read more about the Ransomware here on the website.

Download

If you want to download the editor to make your own custom made ransomware, then you need to buy it from a seller.
This can happen over darknet social media/forums along with Email. if you choose Continue reading...

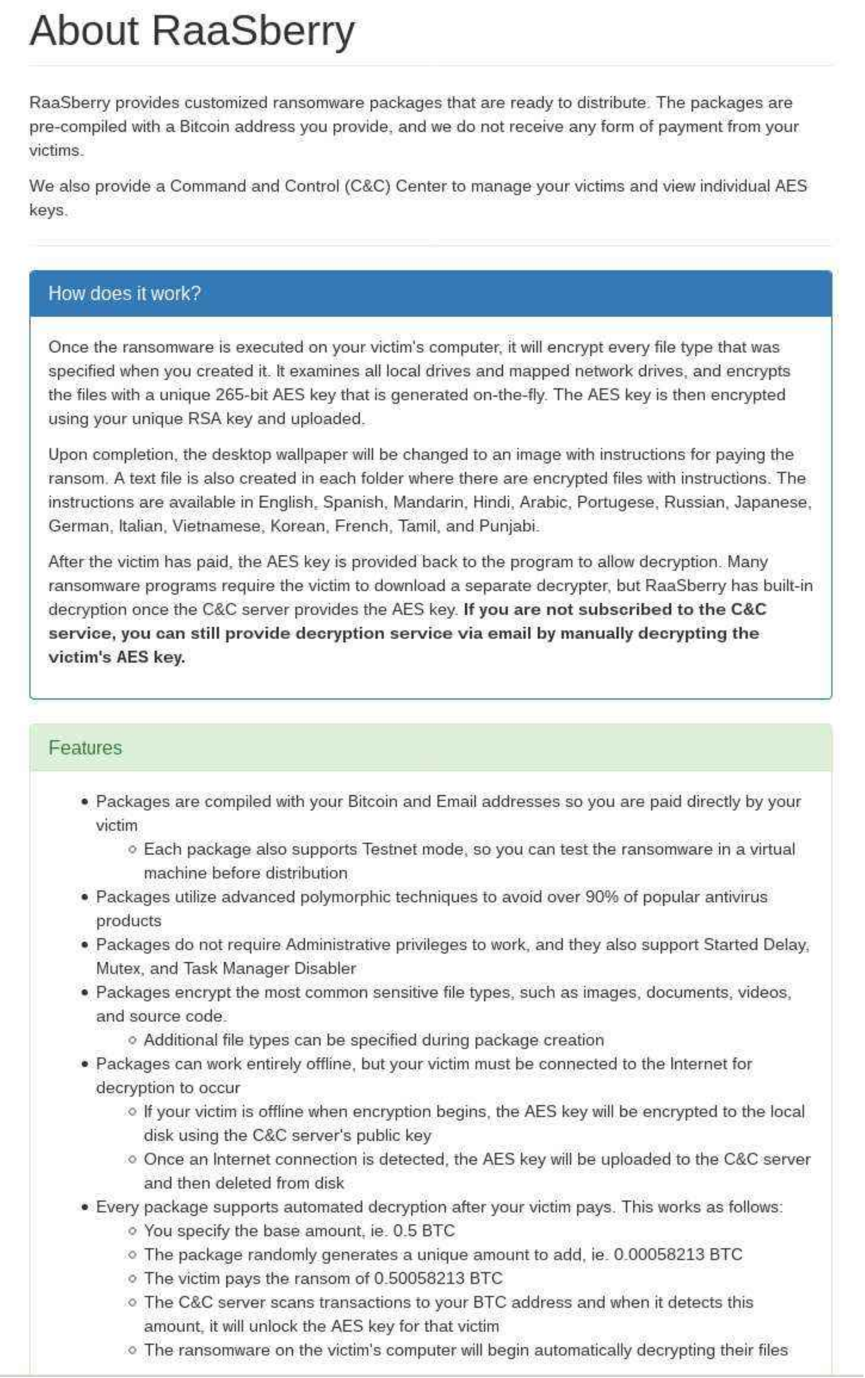
Price

Our price for our ransomware service is 0.3 BTC(one time payment), if that sounds like a lot,
imagine you could infect anyone and keep using our ransomware service, you are going to make much more than that. Continue reading...

How The Ransomware Works

This guide will teach you how you use the ransomware along with it's editor. There will also be provided pictures so you can see it for yourself. Continue reading...

Figure 1: Earth Ransomware Customizable



About RaaSberry

RaaSberry provides customized ransomware packages that are ready to distribute. The packages are pre-compiled with a Bitcoin address you provide, and we do not receive any form of payment from your victims.

We also provide a Command and Control (C&C) Center to manage your victims and view individual AES keys.

How does it work?

Once the ransomware is executed on your victim's computer, it will encrypt every file type that was specified when you created it. It examines all local drives and mapped network drives, and encrypts the files with a unique 265-bit AES key that is generated on-the-fly. The AES key is then encrypted using your unique RSA key and uploaded.

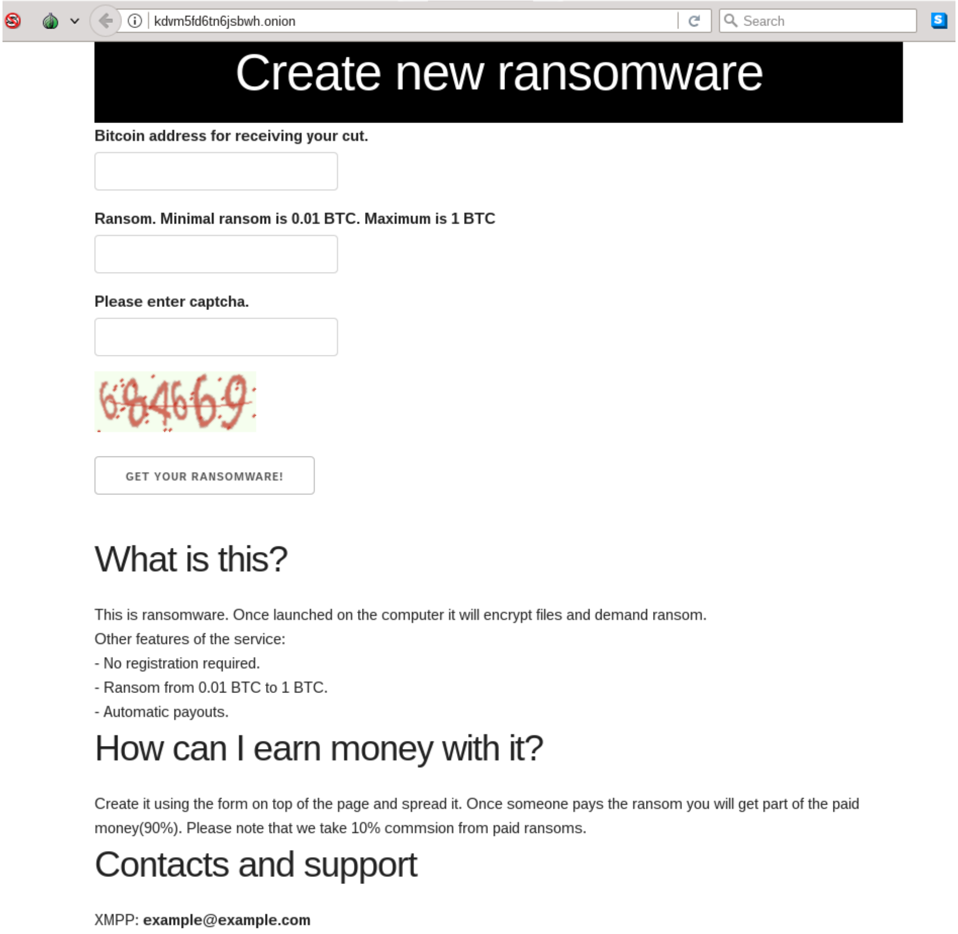
Upon completion, the desktop wallpaper will be changed to an image with instructions for paying the ransom. A text file is also created in each folder where there are encrypted files with instructions. The instructions are available in English, Spanish, Mandarin, Hindi, Arabic, Portugese, Russian, Japanese, German, Italian, Vietnamese, Korean, French, Tamil, and Punjabi.

After the victim has paid, the AES key is provided back to the program to allow decryption. Many ransomware programs require the victim to download a separate decrypter, but RaaSberry has built-in decryption once the C&C server provides the AES key. **If you are not subscribed to the C&C service, you can still provide decryption service via email by manually decrypting the victim's AES key.**

Features

- Packages are compiled with your Bitcoin and Email addresses so you are paid directly by your victim
  - Each package also supports Testnet mode, so you can test the ransomware in a virtual machine before distribution
- Packages utilize advanced polymorphic techniques to avoid over 90% of popular antivirus products
- Packages do not require Administrative privileges to work, and they also support Started Delay, Mutex, and Task Manager Disabler
- Packages encrypt the most common sensitive file types, such as images, documents, videos, and source code.
  - Additional file types can be specified during package creation
- Packages can work entirely offline, but your victim must be connected to the Internet for decryption to occur
  - If your victim is offline when encryption begins, the AES key will be encrypted to the local disk using the C&C server's public key
  - Once an Internet connection is detected, the AES key will be uploaded to the C&C server and then deleted from disk
- Every package supports automated decryption after your victim pays. This works as follows:
  - You specify the base amount, ie. 0.5 BTC
  - The package randomly generates a unique amount to add, ie. 0.00058213 BTC
  - The victim pays the ransom of 0.50058213 BTC
  - The C&C server scans transactions to your BTC address and when it detects this amount, it will unlock the AES key for that victim
  - The ransomware on the victim's computer will begin automatically decrypting their files

Figure 2: RaaSBerry Private Vendor



Create new ransomware

Bitcoin address for receiving your cut.

Ransom. Minimal ransom is 0.01 BTC. Maximum is 1 BTC

Please enter captcha.

What is this?

This is ransomware. Once launched on the computer it will encrypt files and demand ransom.
Other features of the service:
- No registration required.
- Ransom from 0.01 BTC to 1 BTC.
- Automatic payouts.

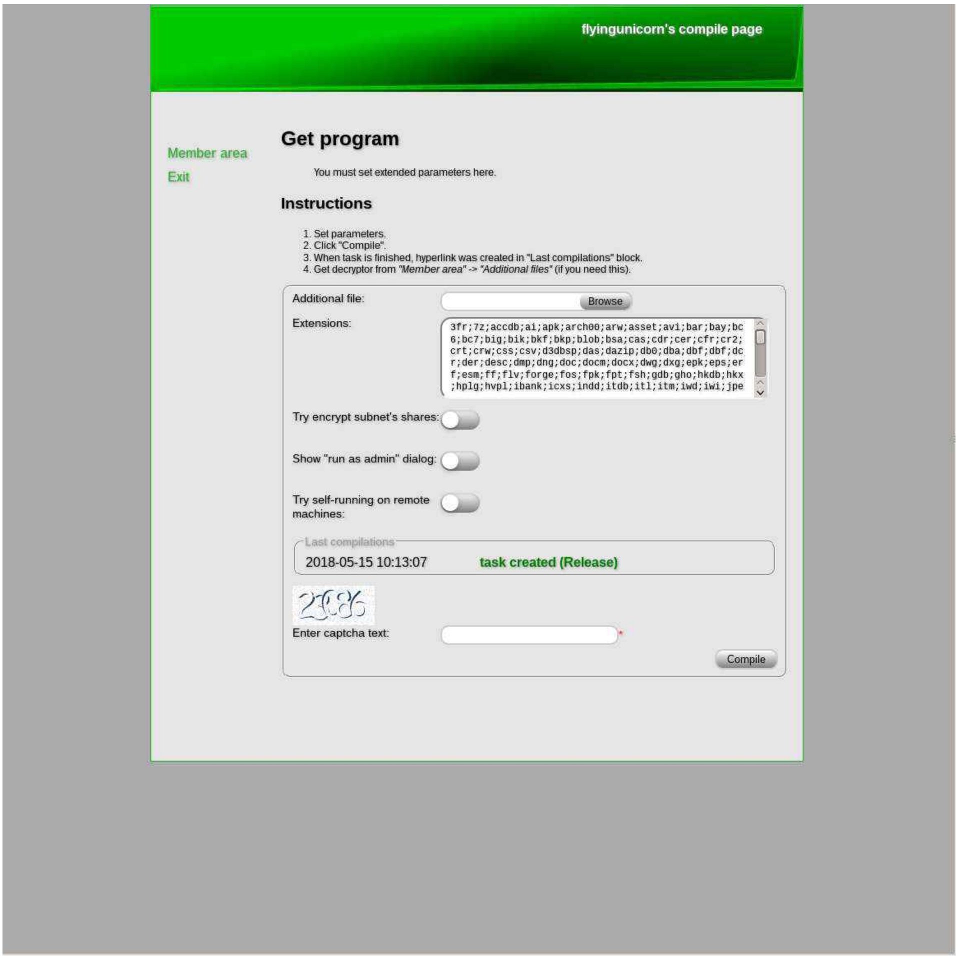
How can I earn money with it?

Create it using the form on top of the page and spread it. Once someone pays the ransom you will get part of the paid money(90%). Please note that we take 10% commsion from paid ransoms.

Contacts and support

XMPP: **example@example.com**

Figure 3: Script Kiddie work



Get program

You must set extended parameters here.

Instructions

1. Set parameters.
2. Click "Compile".
3. When task is finished, hyperlink was created in "Last compilations" block.
4. Get decryptor from *"Member area"* -> *"Additional files"* (if you need this).

Additional file:

Extensions:

```
3fr;7z;accdb;ai;apk;arch00;arw;asset;avi;bar;bay;bc
6;bc7;big;bik;bkf;bkp;blob;bsa;cas;cdr;cer;cfr;cr2;
crt;crw;css;csv;d3dbsp;das;dazip;db0;dba;dbf;dbf;dc
r;der;desc;dmp;dng;doc;docm;docx;dwg;dxg;epk;eps;er
f;esm;ff;flv;forge;fos;fpk;fpt;fsh;gdb;gho;hkdb;hkx
;hplg;hvpl;ibank;icxs;indd;itdb;itl;itm;iwd;iwi;jpe
```

Try encrypt subnet's shares: ○

Show "run as admin" dialog: ○

Try self-running on remote machines: ○

Last compilations

2018-05-15 10:13:07 task created (Release)

Enter captcha text: *

Figure 4: Free program

D Published Paper on Preliminary Study

The next page is a paper of the preliminary study that took place in Fall 2017 and was published in Cyber SA 2018 [7].

A Netnographic Study on the Dark Net Ecosystem for Ransomware

Yara Fareed Fahmy Bayoumy[1], Per Håkon Meland[1,2], and Guttorm Sindre[1]

[1]Norwegian University of Science and Technology, Trondheim, Norway
Email: {yarab,per.hakon.meland,guttorm.sindre}@ntnu.no

[2]SINTEF Digital, Trondheim, Norway
Email: per.h.meland@sintef.no

***Abstract*—For more than a decade, businesses and private citizens alike have been tormented by an online phenomenon that has changed our stance on cyber security. Ransomware, malicious software that demands payment in exchange for a stolen functionality, has grown beyond expectations. The development and distribution of ransomware is stimulated by social networks active in the Dark Net. From the cyber criminal perspective, this is an ideal platform to participate in a business ecosystem, either as an author, vendor or distributor of ransomware. Within the Dark Net, they can find forums and marketplaces that offer complete secrecy and concealment of the user's identity. Studying the activities taking place within the Dark Net sites can improve our situational awareness on upcoming threats and how we can defend against them. In this research, a netnographic study was done to obtain useful data such as observations of the marketplace economies and reflections on the social interactions between the different stakeholders involved in the creation and distribution of ransomware.**

I. Introduction

To reduce uncertainty about cyber attacks, you should follow Sun Tzu's saying *"know your enemy and know yourself"*. To *know yourself* is a matter of identifying your own system functionality, security barriers and exploitable vulnerabilities, something that can be achieved through activities such as design review, code inspection and testing. To *know your enemy* on the other hand, is more of a challenge due to the obfuscated and hidden nature of cyber adversaries. This includes their identity, capabilities, motivation, tactics and techniques, which can be coined as the *fog of cyber war*. To get rid of this fog, we need to apply different security techniques. *Threat modelling* [1] typically involves techniques where someone, e.g. a security expert or system owner, tries to think like an attacker in order to determine how a systems can be attacked and exploited. This is often based on prior experiences, but the general unavailability and unreliability of historical data makes it difficult to estimate the likelihood of attacks, especially in areas with rapid technology advances. *Attacker profiling* is the process of identifying the attacker's skills, and determining the availability of tools and resources sufficient to commit an attack [2]. It has previously been proved to be an effective parameter for quantitative security analysis [3], for instance, knowing the skills of the attacker can help identify the sequence of actions in threat modelling. *Threat intelligence* is a complementing area where we try to monitor, detect and react to existing or emerging menaces or hazards to our assets [4], and share this knowledge with the wider security community so we can collectively be better prepared. Threat intelligence approaches also include *User Behaviour Analytics* (UBA), which tracks anomalous behaviour of online users [5]. All this information can give us insight into current attack trends and hindsight knowledge, but it would be an added value to have reliable foresight into expected attacks in the near future to prioritize which security measures to implement.

The purpose of our research is to raise cyber situational awareness by observing the cyber crime enabling markets and related social activities found on the Dark Net. The Dark Net succeeds in obscuring one's identity, therefore it offers a safe harbour for criminal activity. Understanding the business models of cyber criminals can help us understand their motivation and capabilities, and subsequently improve our knowledge about likelihoods of threats without relying so much on historical data. This is related to Anderson's research direction *econometrics of wickedness* [6], to which we can associate a series of papers and reports (e.g. [7], [8], [9], [10], [11], [12]). Several papers describe the value chains that are involved in developing and offering cyber crime products and services. For instance, Kraemer-Mbula et al. [13] do this for credit card and identity theft, Yip [14] studies Chinese Trojan malware development, and Konradt et al. [15] focus on phishing attacks. Little has been done to document the actual organization of such services and costs incurred within the Dark Net. One notable exception is a study of markets for identity credentials performed by Spagnoletti et al. [16].

Our approach has been to perform a netnographic study, which is the online counterpart of ethnography, and involves making descriptive observations and interpretation over a social group in their natural environment over a period of time. The contribution of this paper is a thorough analysis of the hidden services of the Dark Net that are responsible for planning cyber security attacks, particularly ransomware. This includes the social structure of the different participants and their roles, and the product costs found on the Dark Net marketplaces. Our results have been aligned with other related work, in particular a similar study reported by Carbon Black [17].

Section II gives background information about the Dark Net, which is our study environment, and ransomware, which is the commodity we are interested in. Section III explains our research method, while section IV describes and interprets the most important findings. In Section V, we revisit our research questions and discuss the limitation we encountered. Section VI concludes the paper.

II. Background

A. The Dark Net

The *Deep Web* is a collection of websites and content that are not indexed by commercial search engines such as Google and Bing. Most of the Deep Web is perfectly legitimate, and can be thought of as information that does not have a direct link leading to it. The *Dark Net*, or *Dark Web*, constitutes a small portion of the Deep Web that is deliberately hidden and cannot be accessed with regular web browsers. TOR (short for *The Onion Router* is the most prominent network on the Dark Net, and can briefly be explained as a volunteer driven, encrypted overlay network. The network keeps data of the users location and network usage hidden by onion routing (Goldschlag et al. [18]), making use of thousands of relay nodes to support online privacy and anonymity. Content is accessed using the free Tor Browser, which is a fork from Mozilla Firefox, and thus has the same look and feel as most regular browsers.

Though the original intent of the TOR network may have been driven by idealism, it is now predominately used by criminals conducting transactions of illegal goods and services such as drugs, arms, murder and child pornography. According to a study from 2016, 57% of .onion sites facilitate such criminal activity (conservative classification) [19]. Lately, the Dark Net has also become soaring with marketplaces that provide security breaching services. Organized crime has taken benefit of the anonymity feature presented by the Dark Net [20], specifically the Tor network, to hide their illegal activities. In addition to that, more novice cyber criminals are beginning to partake in such activities due to the affordable entry level and prospect of attaining great sums of money. A 2017 study by Europol [21] points out that Dark Net meeting places and marketplaces is a key environment for cyber criminals, allowing access to the skills and expertise of other members of the community.

Fortunately, global law enforcement organizations do succeed in penetrating and shutting down what is clearly illegal marketplaces. For instance, on the 20th of June 2017, the Dutch National Police and Europol managed to locate and seize the infrastructure of *Hansa*, the third largest criminal marketplace on the Dark Net [22]. Later the next month, the FBI and DEA-led operation *Bayonet* arrested the creator and administrator of *AlphaBay*, the largest marketplace with over 200 000 users and 40 000 vendors. On the other hand, Ceci et al. [23] refer to a number of studies showing that such external shocks do not really affect the dimension and growth of the Dark Net markets, as they are able to adapt and survive through the concept of *continuous morphing*.

B. Ransomware

Ransomware is a type of malicious software (short: *malware*) that demands payment in exchange for a stolen functionality. The most prevalent ransomwares make use of file encryption as a means for extortion, before asking for a ransom to get the files decrypted [24]. Other types completely lock the users out of their devices, but this strategy can hinder the victim in actually paying the ransom. Examples of well-known ransomwares are *Reveton* (tried to pass off as an enforcement authority claiming a fine), *CryptoLocker* (heyday of 2013, early example of Bitcoin ransoms), *WannaCry* (hit more than 300 000 devices in 150 countries in May 2017, attributed to North Korea), *Petya* (discovered in 2016, overwrites master boot records instead of file encryption) and *GoldenEye* (a variant of Petya that severely affected Ukraine in 2017) [25].

According to Europol [21], ransomware, together with *information stealers*, are the two most dominant malware threats, and the development and propagation of such software sits at the core of cyber-dependent crime. Security experts have estimated that $1bn was deposited into Bitcoin wallets associated with ransomware cyber criminals in 2016 alone. This makes it an incredibly lucrative business and is why criminals are now looking beyond the humble personal computer to more valuable targets such as governments, the utilities industry and larger companies [26]. In 2016, the average ransom demand was $1077, which is a triple from 2015 and an indication that the attacks focus more on businesses than individuals [27]. Furthermore, the emerging number of ransomware strains multiplied 4.3 times from Q1 2016 compared to the same period in 2017 [28].

In the early days of ransomware, cyber criminals developed and distributed ransomware for their own use. This business model has evolved into more specialised tiers, and our research has applied a stakeholder model based on [17] with the following characteristics:

- **Authors** are developers who write the ransomware source code. Ransomware instances are often based on a type or a family, and tailored according to customer demand. Authors do also provide customer support in some cases.
- **Vendors** do marketing and sale of ransomware on online marketplaces. This can be a ready-made product or customizable builder that is charged up front, or Ransomware-as-a-Service (RaaS). RaaS is basically renting out the software for a relatively low fixed price a week, and taking an additional cut of every ransom that is paid. Authors can also be vendors, but then they become more exposed.
- **Distributors** buy or get hold of the ransomware and distribute it through means such as spam emails, remote desktop connections, USB sticks or infected websites. Distributors are the highest risk takers since they perform the actual fraud. We also distinguish between *novice* and *experienced* distributors based on their technical skills.

RaaS is increasing in popularity [21], and has become very much similar to mainstream retailing and affiliate programs.

For instance, the *Satan* ransomware can freely be downloaded from the Dark Net, the ransom amount can be set by the distributor, and the vendor receives 30% of the proceeds via Bitcoin [29].

III. Research method

Netnography is a qualitative research direction that involves the researchers' visual perception and reflections of a community of users active on the Internet, in our case, the Dark Net in particular. There is a lot of ongoing research on automatic crawling and extraction of quantitative data from the Deep Web (see for instance [30]), but the challenges related to hidden, invisible and non-indexable content make access to hard data very limited. We therefore chose to apply a grounded theory approach [31] to get an understanding of the phenomenon at hand. In order to pertain a systematic approach, we have applied a netnographic framework defined by Kozinets [32], which suggests a set of phases/activities to be followed throughout the study. Within netnographic literature, the ideological ecosystem of the underground economy would be classified as a *topical issue network*. The participants involved are physically disconnected from each other and do not have an interactive shared conversation among themselves due to the large population of registered users and the necessity to maintain anonymity. What unites them is the shared interest in a particular topic.

The remainder of this section summarizes the initial preparation phases of the study. *Introspection* is when we defined research question and expected outcomes, during the *information phase* we considered ethical questions, which is followed by *inspection and selection of data collection sites*. The *interaction strategy* defined how we were to capture and index data.

A. Introspection

Introspection is a reflective process in which the researchers start by defining their own pre-understandings, personal judgements and previous experiences related to the study. These were to a large extent related to threat modelling and a motivation to look for new data parameters that can supplement historical data and expert opinions. Our intellectual curiosity was also triggered by the unexplored information potential of the Dark Net. Our impression has been that a lot of the information is greatly influenced by what is presented by mainstream media, and lacks an empirical foundation.

We expected that observing the forums and online markets within the Dark Net would give us an improved insight on how ransomware stakeholders communicate, the costs incurred on services and products needed to perform an attack, and the structure of organized crime. These observations would be perfectly aligned with the parameters needed for attacker profiling and threat prediction. Based on this, we formulated the following research questions:

1) *What is the nature of activities practiced by the online community within the Dark Net marketplaces and forums?*
2) *How can cost data from the Dark Net be beneficial to the threat modelling process?*

B. Information

Ethical dilemmas pertain to the study of online communities. It gives rise to a number of questions that vary from legal considerations to the impact of international boundaries. More issues begin to surface when research observations and interactions are done in the Dark Net.

The services sold in the markets are publicly posted for all to see. However, the personal identity of the seller is strictly confidential and all sellers go about with their activity using random pseudonyms. The seller is a suspected perpetrator of a possible crime that may drastically cost organizations huge sums of money and even worse, put people's lives at risk if they target for instance health care systems. Asking for a user's permission to be a participant is therefore a precocious task.

To avoid all possible legal risks that could be imposed, we decided to avoid direct communication with the users, and only record data as passive observers. Martin and Christin [33] stress two important reasons for this; firstly, the research after publication will not be pertinent to any proof for prosecution against any individual. Despite the fact that the collected information can be useful to capture the criminals, it is best advised not to mingle in such affairs. Secondly, there will be no need to ask for permissions because there will be no contact with the participant.

The pseudonyms of the users have been censored from our research data. To avoid supporting criminal activity, we decided to avoid any financial purchases of products and services sold throughout the Dark Net.

C. Inspection and selection of data collection sites

To narrow the surface of the netnographic study, we needed to select a set of sites to immerse ourselves in. Searching for suitable websites required more than a simple search of terms such as "cryptomarkets" and "dark net markets" in the surface web. Fortunately, a website that goes by the name *DarkNet Stats* or *DNStats* offers a list of the most popular Dark Net websites with statistics related to uptime and availability. We made our selection based on a set of factors defined by Kozinets [32], where *relevance*, *activity/uptime* and *data richness* weighted the most. We assigned scores ourselves based on available data and selected the three top websites explained below. Information was also gathered from related research, such as Bakken's work on the cryptomarkets in the Dark Net [34] and Carbon Black's report on the ransomware economy [17]. Our observation period was from October to December 2017.

1) Wall Street Market: This marketplace was established in 2016 and contains a variety of goods ranging from narcotics to computer crime. Table I shows an excerpt of the inventory list from our observation period. Most of the bots and malware services are RaaS, and some of the security software are paid tutorials on how to become a hacker or how to develop exploitative code for beginners. Wall Street Market ranked low for the factor *active* because it was slow to browse and load. Opening a web page on this market could take as much as 5 minutes.

TABLE I
WALL STREET MARKET PRODUCTS AND SERVICES (NOV 2017).

Services (528): Social Engineering (19), Carding (107), Coding & Graphics (8), Other (394)
Software & Malware (144): Botnets & Malware (38), Exploits (6), Kits (14), Security Software (14), Other (72)
Security & Hosting (19): Hosting (6), VPN (4), Socks (3), Other (6)

2) Dream Market: Dream Market has been around since 2014, but it was not until AlphaBay was shut down in Operation Bayonet in the summer of 2017 that it became among the most popular marketplaces. At the start of our observation period, Dream Market was properly functioning and preferred over Wall Street Market because its quick response time and similar content.

Despite of this, the number of services on Dream Market were fewer than Wall Street Market, and most of them were old. In the beginning of November 2017, we started to observe a lot of website downtime. This was followed by an announcement that Dream Market was to be shut down due to a compromise by law enforcement agencies. Though unplanned from our side, this event allowed us to observe a migration of users and services during our study period, which was interesting by itself. A few mirrors of Dream Market still exist today, but are not regarded as trustworthy by the community.

3) Intel Exchange: This is the only website we selected that is not a marketplace, but a forum in which individuals discuss general topics ranging from the availability of marketplaces and their statuses to illegal activities, hacking methods and conspiracy theories. We included this site because it is the only forum that allowed members to promote their services. Other forums often restrict this feature to avoid data leaks of personal information that can help law enforcement track individuals. Alternatively, these forums suggest links to marketplaces for individuals to promote their services. For this reason, we gave Intel Exchange a high rating for its richness in data.

D. Interaction strategy

The Dark Net websites contain data of a wide range of products and services sold to members, but dominating products such as cannabis and PayPal accounts were irrelevant to our study. Therefore, the search keyword we used within the marketplaces and forums was simply "ransom", followed by manual filtering and inspection.

Data was recorded using a spreadsheet, field notes and screen captures. It was chosen to do this manually because this has been a discovery process of the irregular and unfamiliar structure of Dark Net markets. Our data were classified based on the service sold, its price in Bitcoins (BTC), marketplace, vendor account name, product description and field notes. RaaS price listings were recorded to retrieve cost data and compared to other studies for verification. The culture of the Dark Net community involved in the production of ransomware was analysed based on observations of textual data.

IV. RESULTS AND INTERPRETATION

A. Cost data

During the course of the observations, we recorded information about 20 distinct RaaS that were announced for sale on the aforementioned Dark Net marketplaces. Many of the RaaS offered similar features in their service package, such as customization. All prices were listed in Bitcoins, with one exception; a type of FUD (*fully undetectable*) ransomware was sold in US Dollars, so we had to make a conversion using the rate at that time (1 BTC = 16381.7 USD). The most expensive RaaS noted was the *Alm4* ransomware, which roughly costed 0.458 BTC. Vendors of Alm4 set the high price due to their notable reputation on several marketplaces. The cheapest was the *6 Bitcoin ransomware easy money*, which was commonly sold by different vendors across several markets.

Some of the observed RaaS products were also documented by Carbon Black in August/September 2017 [17]. In Figure 1, we have compared our findings on some of the most popular RaaS products with their data. This was useful to verify the credibility of the observed RaaS, i.e. they were not honey pots created by law enforcement officials to hunt down possible buyers of the illegal service.

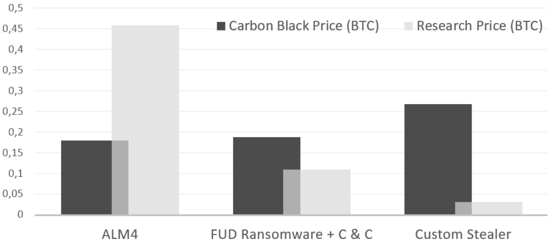


Fig. 1. Comparing costs between the results of this research and Carbon Blacks.

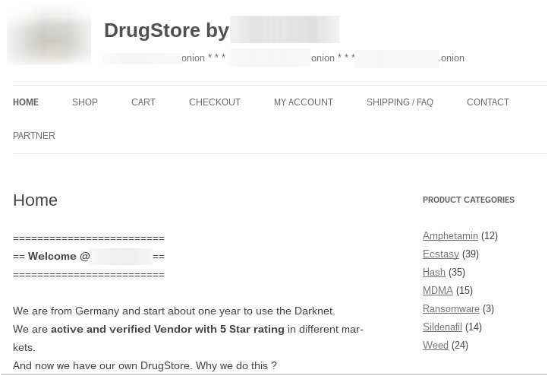
Prices in their report were listed in US Dollars, which made it difficult to make fair comparisons because BTC to USD exchange rates fluctuated a lot during the autumn of 2017.

An indications of different prices set to the same item on two different markets was discovered on one occasion. Prices between Wall Street Market and Dream Market were considerably the same. However, one of the RaaS in Wall Street Market, offered a link in the description to another market called *Berlusconi*, which showed a huge difference in prices. The price listed in Berlusconi was 0.000724 BTC, whereas in Wall Street Market it was 0.000436 BTC. This gives rise to the assumption that different marketplaces may apply commissions on services sold, and the vendors apply it to service costs. However, this should not be considered as a fact, since this was observed only once.

B. Actor data

Information concerning the different stakeholders involved in the development, selling and distribution of RaaS were also identified. This includes the vendor user profiles in the Dark Net marketplaces, background and interests of distributors, and lastly, the language used by the vendors to attract customers. Observations related to authors were too sparse to make any significant conclusions.

1) Vendors: In all marketplaces, vendors are assigned badges or experience points/levels. These are calculated based on the ratings given to them by their customers after a successful transaction. When the vendor is rated high, the more trustworthy the vendor is perceived. We made an interesting observation that the majority of RaaS vendors with high ratings have this because of their drugs and ecstasy related sales in the past, and not because of ransomware. This leads us to believe that, unlike ransomware authors, vendors are not specialists on cyber crime, but general risk takers that benefit from a wide range of sales. Figure 2 shows a vendor that sells ransomware besides hash and weed on his own website. Ransomware is the only digital product sold here, which signifies how profitable it is compared to other illegal services.



[redacted] DrugStore by [redacted]

[redacted] onion * * * [redacted] onion * * * [redacted] .onion

Home

========================
== **Welcome @** [redacted] ==
========================

We are from Germany and start about one year to use the Darknet.
We are **active and verified Vendor with 5 Star rating** in different markets.
And now we have our own DrugStore. Why we do this ?

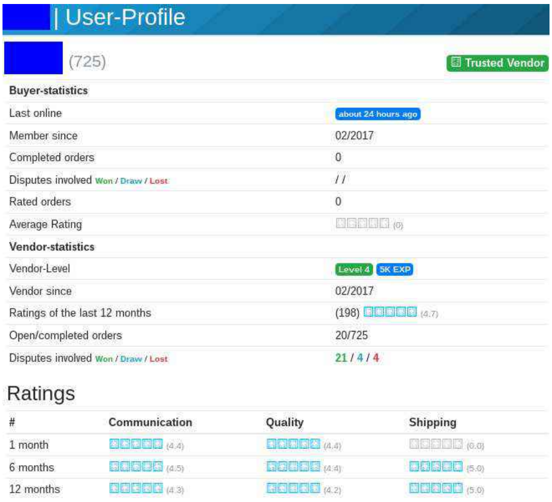
PRODUCT CATEGORIES

Amphetamin	(12)
Ecstasy	(39)
Hash	(35)
MDMA	(15)
Ransomware	(3)
Sildenafil	(14)
Weed	(24)

Fig. 2. Example of a popular vendor that sells illegal drugs and ransomware.

Others have managed to gain average high ratings from selling other cybercrime-as-a-service items such as the trading of intellectual property or hacking of targeted individuals/businesses. Perceived trustworthiness does probably not only depend on the high rating, but also the quantity of successful purchases. Figure 3 shows a popular and trusted vendor on Wall Street Market. This vendor has managed to sell 725 items since February 2017. Most services provided by this vendor were related to fraud, the latest services sold were ransomwares.

It seems that the same vendors are selling their products and services across many marketplaces, although often with different usernames. Inspection of vendor user profiles indicated that they tended to also reveal their different usernames for other popular marketplaces. The reason is likely to market the quantity of successful sales and thus maintain reputation across the underground network.



[redacted] | User-Profile

[redacted] (725) Trusted Vendor

Buyer-statistics	
Last online	about 24 hours ago
Member since	02/2017
Completed orders	0
Disputes involved Won / Draw / Lost	/ /
Rated orders	0
Average Rating	☆☆☆☆☆ (0)
Vendor-statistics	
Vendor-Level	Level 4 5K EXP
Vendor since	02/2017
Ratings of the last 12 months	(198) ★★★★★ (4.7)
Open/completed orders	20/725
Disputes involved Won / Draw / Lost	21 / 4 / 4

Ratings

#	Communication	Quality	Shipping
1 month	★★★★★ (4.4)	★★★★★ (4.4)	☆☆☆☆☆ (0.0)
6 months	★★★★★ (4.5)	★★★★★ (4.4)	★★★★★ (5.0)
12 months	★★★★★ (4.3)	★★★★★ (4.2)	★★★★★ (5.0)

Fig. 3. Vendor statistics of one of the most popular sellers of digital goods.

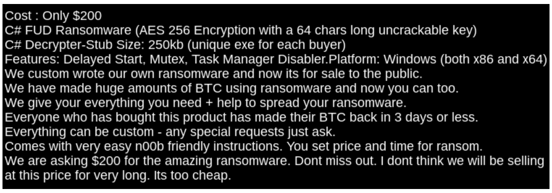
One specific feature we noticed for Dream Market, was that every vendor profile had its AlphaBay ranking listed (not as free text). It is unclear how this has been managed, but we can assume that there has been a collaboration between AlphaBay and Dream Market when AlphaBay was taken down. This could be an indication that marketplaces do not operate independently.

2) Distributors: All marketplaces conceal the identity of the buyers of a particular product or service. The usernames of the buyers who place comments and ratings on a given RaaS were hidden from the general public. However, the customer segment vendors are targeting can be easily characterized as they explicitly mention who can use these services in the service description.

A number of RaaS specify the required level of distributor expertise. Most of them insist that only experienced distributors should meddle with their product or service. Others target the less knowledgeable by offering detailed guides in *pdf* format and video tutorials. In Figure 4, a FUD ransomware description clearly mentions that it has been made for *noobs*, an internet slang term used to label novice beginners. From our recorded data of 20 RaaS, the target distributor ratio was 35% novice and 65% expert.

C. Use of media

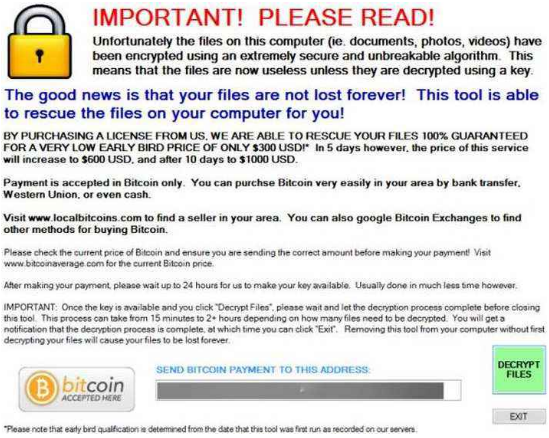
Different media was used by the vendors to market services to potential buyers, or illustrate how the RaaS works on a victim's computer. The type of media was limited to images attached to the service description or a link to a website with the video. No images were included in comments made by buyers. The following explains the types of media we observed and the concepts behind them.



Cost : Only $200
C# FUD Ransomware (AES 256 Encryption with a 64 chars long uncrackable key)
C# Decrypter-Stub Size: 250kb (unique exe for each buyer)
Features: Delayed Start, Mutex, Task Manager Disabler.Platform: Windows (both x86 and x64)
We custom wrote our own ransomware and now its for sale to the public.
We have made huge amounts of BTC using ransomware and now you can too.
We give your everything you need + help to spread your ransomware.
Everyone who has bought this product has made their BTC back in 3 days or less.
Everything can be custom - any special requests just ask.
Comes with very easy n00b friendly instructions. You set price and time for ransom.
We are asking $200 for the amazing ransomware. Dont miss out. I dont think we will be selling at this price for very long. Its too cheap.

Fig. 4. A RaaS package that includes detailed tutorial for novice buyers.

1) Images: Images attached to the service provides a presentation of what the ransomware would look like once it infected the victims computer. Figure 5 shows a basic ransomware with instructions on how to buy Bitcoin if the victim does not have prior knowledge of the cryptocurrency. Other information include the ransom amount in USD and the time left until the ransom is increased. In some cases, vendors attached images of tools used to build the customized software included in the RaaS.



IMPORTANT! PLEASE READ!

Unfortunately the files on this computer (ie. documents, photos, videos) have been encrypted using an extremely secure and unbreakable algorithm. This means that the files are now useless unless they are decrypted using a key.

The good news is that your files are not lost forever! This tool is able to rescue the files on your computer for you!

BY PURCHASING A LICENSE FROM US, WE ARE ABLE TO RESCUE YOUR FILES 100% GUARANTEED FOR A VERY LOW EARLY BIRD PRICE OF ONLY $300 USD!* In 5 days however, the price of this service will increase to $600 USD, and after 10 days to $1000 USD.

Payment is accepted in Bitcoin only. You can purchse Bitcoin very easily in your area by bank transfer, Western Union, or even cash.

Visit www.localbitcoins.com to find a seller in your area. You can also google Bitcoin Exchanges to find other methods for buying Bitcoin.

Please check the current price of Bitcoin and ensure you are sending the correct amount before making your payment! Visit www.bitcoinaverage.com for the current Bitcoin price.

After making your payment, please wait up to 24 hours for us to make your key available. Usually done in much less time however.

IMPORTANT: Once the key is available and you click "Decrypt Files", please wait and let the decryption process complete before closing this tool. This process can take from 15 minutes to 2+ hours depending on how many files need to be decrypted. You will get a notification that the decryption process is complete, at which time you can click "Exit". Removing this tool from your computer without first decrypting your files will cause your files to be lost forever.

SEND BITCOIN PAYMENT TO THIS ADDRESS:

[redacted]

*Please note that early bird qualfication is determined from the date that this tool was first run as recorded on our servers.

Fig. 5. Customized Stealer ransomware.

2) Videos: Video tutorials were usually added to the RaaS package sold to novice distributors. For instance, videos show how the ransomware works once the victim downloads it and unknowingly installs it on a personal computer. One video we inspected showed how all files on a Windows 7 computer were encrypted once a particular .exe file is activated. The victim can then access some parts of the OS and perform necessary actions to pay the ransom. This video was linked to the service description of a popular RaaS, and had more than 1,400 views since July 2016.

D. Hermeneutics

The qualitative approach employed during this study involved the decoding and interpretation of textual data. This data included comments made by the distributors, threads posted by forum members, and the description of the RaaS packages provided by the vendors.

1) Forum conversations: Posts and comments made on the popular forums were insufficient to fairly interpret the interactions among the stakeholders involved in RaaS. A possible explanation for this is the strict moderation of Dark Net forums that disallow any attempts to market or sell products or services. Intel Exchange was our main observation site since it does not enforce these restrictions. However, activity surrounding ransomware was quite low. From time to time, users would ask about the process of buying ransomware or which is the best marketplace. Most answers are cliché, and thus not significant in a research context. What we found to be interesting though, was how some forum users went searching for partners in the development or distribution of ransomware. For example, in the quote below, a user (maybe a would-be author?) publicly asks for partners and openly mentions that he/she is interested in cyber-security related software.

> *I'm currently still learning some stuff about cyber-security. Although I'm already familiar with linux, metasploit, nmap and other software. Send me a mail to s*******@m*******.com*

In another forum, a user wants to provide a list of emails and companies that can be infected by a USB stick in return for a ransomware.

> *Looking for a partner to supply ransomware i have huge email lists and some select companies to infect via usb for more payoff. almost completed this on alpha but alpha bay has been down now for days and doesnt seem to ever be on again.*

In response to this request, another user (whom we assume is an author and/or distributor) wants to have more information in order to consider the deal.

> *What OS is being targeted, Do you have access to the corporate AV server(would make it a cakewalk)? Would you (by hand) be deploying provided malware via usb, on-site at said "companies physical locations or in a data center, if so under what jurisdiction? How much verified intel is known about the infrastructure of targeted "companies"? Besides countless emails like Nigeria, it has a low success rate. I am trying to assess the value of target data before I speak. Good luck!*

Unfortunately, the rest of this thread has been discontinued due to forum restrictions. The user that started the thread was ultimately banned from posting any further.

2) Service Reviews: Comments and reviews on purchases were in general homogeneous and short. Most comments would just praise the vendor for their service. Some customers were open about their intent behind buying the RaaS. The quote below was posted by a distributor claiming to have bought the ransomware for vengeance, but it can be disputed whether this motive is true or not, or if it justifies the action.

> **** is an excellent and trustworthy vendor. The instructions are clear. The malware is powerful and the suggested distribution techniques are both*

> *creative and effective. Potential buyers must be familiar with using malware. I'M NOT IN THIS FOR THE MONEY. I lost a friend in Iraq, so I'm going to target ISIS/ ISIL/ Daesh/ Al Qaida and their sympathizers/associates with this. F*** you ISIS and anyone else who wants to hurt the US and our allies.*

3) Service Descriptions: We applied a simple method proposed by Kozinets [32] to perform textual analysis. This was to use word frequency analysis to signify the most common words and to visualize this in a word cloud. Figure 6 shows our resulting extraction from all the RaaS service descriptions supplied by the vendors.

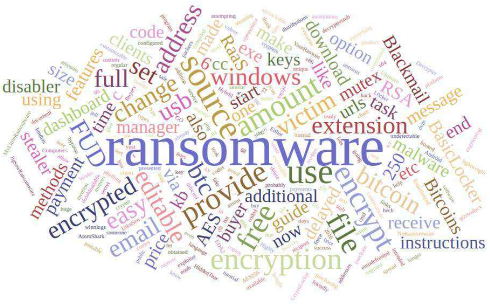


Fig. 6. Word cloud of the RaaS descriptions.

Besides the term *ransomware*, terms such as *windows* and *AES* imply that most ransomware target Windows OS and the files are encrypted using AES. Most common ransomwares are the Blackmail and FUD types. Added to that, many RaaS provides instructions for distributors on how to build the source code. Bitcoins/BTC clearly overshadows other currencies, while we saw in non-malware related forums that *Monero* is gaining a lot of ground for drug transactions.

V. Discussion

A qualitative, netnographic study is a suitable approach to get an understanding of social phenomena based on limited sets of unstructured data. However, results from such a study should be considered to be more in the line of indications and norms rather than cold hard facts. We would like to mention the main limitations we encountered, and that can pose a threat to the validity of our investigations.

In general, analysis on qualitative data can be questionable when it is difficult to verify the reliability of the collected data. Most of the data collected for this research is based on observations of the Dark Net, however, some services may be a hoax or a decoy placed by law enforcement officials to attract possible ransomware distributors. The best way to make sure that offers were not made by fake vendors, was by focusing on users that had high reputations on the marketplaces. This filtration limited the vendor data.

The tightly closed structure of the Dark Net imposed tough barriers that were virtually impenetrable as long as the researchers are passive observers. It seems like authors of ransomware are highly sensitive to exposing their activity to the Dark Net community. Some forums and platforms that these authors are known to be active on, required either an invitation code from a registered user or an overpriced registration fee as high as 1 BTC. Consequently, it was difficult to attain enough data about the development and maintenance of ransomware source codes. This means that the author stakeholder we set out to investigate is still somewhat of a dark horse.

The marketplaces on the Dark Net are global. Some marketplaces are only offered in one specific language or offer products and services to a particular country and do not ship abroad. For instance, some of the most popular and widely spread ransomwares originate from Russian marketplaces that are written in the Russian language. Therefore, a linguistic bias was limiting this research. We could have employed automatic translation engines to somewhat overcome this, but even better, having a team of researchers with knowledge of different languages and cultures would provide less biased reflections and observations. We would also like to point out that there are online communities that are involved in the creation and distribution of malicious software that exchange information outside of the Dark Net. This has been out of scope for us, but we know from the research of Holt et al. [35] that communication practices differ from one community to another based on their local preferences. For instance, Russians cyber criminals tend to prefer Internet Relay Chats (IRC) or forums to communicate, whereas Turkish peers use instant messaging methods and email.

We chose to dig deep into just a few of the most popular and stable sites for malware instead of crawling for data among the thousands of sites that were available. We also limited our observations to a few months. Scaling-up the scope of this research is currently ongoing and future work, but we believed that this initial study was necessary to establish an empirically founded benchmark. The Dark Net has mostly been referenced in academic papers for other trending topics that are hardly related to cyber security, such as drug trade or child sexual abuse. To obtain a greater dataset, we would need to automate the data collection to a greater extent. We also believe that monitoring the data collection sites for a longer time span would probably offer information about cost data fluctuations with respect to external factors such as competitiveness, consumer demand and supply of quality source codes. This analysis can also be based on data dump archives, which are available for a lot of the Dark Net marketplaces.

Regarding our first research question, we believe that we were able to observe and classify the main social activities, especially related to the vendors and distributors of ransomware. The second research question guided us to attain knowledge about how cheap it is to obtain a RaaS, as the investment cost can be as low as zero. This tells us that almost any motivated attacker is a potential threat, while costs and capabilities are lesser obstacles.

As a final point, we believe that the Dark Net ecosystem for ransomware is a topic deserves attention and continued research. It seems to be growing to maturity, and supports a set of specialized stakeholders that relate to similar market forces as ordinary businesses. This is despite that law enforcement agencies are continuously taking down illegal sites. According to Europol [21], the availability of cybercrime tools and services on the Dark Net appears to be growing relatively faster than more established market commodities such as drugs.

VI. Conclusion

The objective of this research has been to attain a broad understanding of the activities within the Dark Net that expand the economy of cyber crime, specifically ransomware. The activities of vendors and distributors can be directly observed, while the ransomware author is typically a dark horse. Though the majority of ransomware target experienced distributors, a significant portion is also made for novice distributors, who are offered simple step-by-step guides on how to attack their victims. The same ransomwares seem to have the same price across different marketplaces, and vendors refer to their various user names in an openly manner. It seems like a large portion of the ransomware vendors have built their reputation by selling drugs and other illegal goods, not necessarily ransomware. The transfer of vendor statistics from one marketplace to another is a clear indication that administrators are in contact with each other, or might even be part of the same crews. Despite numerous takedowns by law enforcement agencies around the world, the ransomware ecosystem is growing and evolving. A continuous analysis of the popular types ransomware sold to distributors can give an early warning on attacks-soon-to come and thus improve our cyber security situational awareness.

References

[1] A. Shostack, *Threat modeling: Designing for security*. John Wiley & Sons, 2014.

[2] C. Phillips and L. P. Swiler, "A graph-based system for network-vulnerability analysis," in *Proceedings of the 1998 workshop on New security paradigms*. ACM, 1998, pp. 71–79.

[3] A. Lenin, J. Willemson, and D. P. Sari, "Attacker profiling in quantitative security assessment based on attack trees," in *Nordic Conference on Secure IT Systems*. Springer, 2014, pp. 199–212.

[4] Webroot, "Threat intelligence: What is it, and how can it protect you from todays advanced cyber-attacks?" 2014. [Online]. Available: https://www.gartner.com/imagesrv/media-products/pdf/webroot/issue1_webroot.pdf

[5] S. Angeletou, M. Rowe, and H. Alani, "Modelling and analysis of user behaviour in online communities," in *International Semantic Web Conference*. Springer, 2011, pp. 35–50.

[6] R. Anderson, "Security economics: a personal perspective," in *Proceedings of the 28th Annual Computer Security Applications Conference*. ACM, 2012, pp. 139–144.

[7] A. Cárdenas, S. Radosavac, J. Grossklags, J. Chuang, and C. Hoofnagle, "An economic map of cybercrime," 2009.

[8] D. Florêncio and C. Herley, "Sex, lies and cyber-crime surveys," in *Economics of information security and privacy III*. Springer, 2013, pp. 35–53.

[9] M. Goncharov, "Russian underground 101," *Trend Micro incorporated research paper*, p. 51, 2012.

[10] C. Herley, "The plight of the targeted attacker in a world of scale." in *WEIS*, 2010.

[11] T. Cymru, "The underground economy: priceless," *login*, vol. 31, no. 6, December 2006.

[12] A. K. Sood, R. Bansal, and R. J. Enbody, "Cybercrime: Dissecting the state of underground enterprise," *IEEE internet computing*, vol. 17, no. 1, pp. 60–68, 2013.

[13] E. Kraemer-Mbula, P. Tang, and H. Rush, "The cybercrime ecosystem: Online innovation in the shadows?" *Technological Forecasting and Social Change*, vol. 80, no. 3, pp. 541 – 555, 2013, future-Oriented Technology Analysis. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0040162512001710

[14] M. Yip, "An investigation into chinese cybercrime and the underground economy in comparison with the west," Ph.D. dissertation, University of Southampton, 2010.

[15] C. Konradt, A. Schilling, and B. Werners, "Phishing: An economic analysis of cybercrime perpetrators," *Computers & Security*, vol. 58, pp. 39 – 46, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404815001844

[16] P. Spagnoletti, G. Me, F. Ceci, and A. Prencipe, *Securing national e-ID infrastructures: Tor networks as a source of threats*, F. Cabitza, C. Batini, and M. Magni, Eds. Springer, 2018.

[17] Carbon Black, "The Ransomware Economy," October 2017.

[18] D. Goldschlag, M. Reed, and P. Syverson, "Onion routing," *Communications of the ACM*, vol. 42, no. 2, pp. 39–41, 1999.

[19] D. Moore and T. Rid, "Cryptopolitik and the darknet," *Survival*, vol. 58, no. 1, pp. 7–38, 2016. [Online]. Available: https://doi.org/10.1080/00396338.2016.1142085

[20] L. Dishman. (2015) The new face of organized crime. [Online]. Available: http://www.slate.com/articles/technology/ibm/2015/06/the_new_face_of_organized_crime.html

[21] Europol, "Internet Organised Crime Threat Assessment (IOCTA)," 2017. [Online]. Available: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017

[22] ——. (2017) Massive blow to criminal dark web activities after globally coordinated operation. [Online]. Available: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation/

[23] F. Ceci, A. Prencipe, and P. Spagnoletti, "Evolution, resilience and organizational morphing in anonymous online marketplaces," in *To appear in: AOM Specialized Conference, Big Data and Managing in a Digital Economy*, 2018.

[24] A. Gazet, "Comparative analysis of various ransomware virii," *Journal in Computer Virology*, vol. 6, no. 1, pp. 77–90, Feb 2010. [Online]. Available: https://doi.org/10.1007/s11416-008-0092-2

[25] Wikipedia contributors, "Ransomware — Wikipedia, the free encyclopedia," 2018. [Online]. Available: https://en.wikipedia.org/wiki/Ransomware

[26] C. Srinivasan, "Hobby hackers to billion-dollar industry: the evolution of ransomware," *Computer Fraud & Security*, vol. 2017, no. 11, pp. 7–9, 2017.

[27] Symantec, "Internet Security Threat Report," vol. 22, April 2017.

[28] Proofpoint, "Quarterly Threat Report Q1 2017," 2017.

[29] P. Ducklin, "Satan ransomware: old name, new business model," naked security, 2017. [Online]. Available: https://nakedsecurity.sophos.com/2017/03/07/satan-ransomware-old-name-new-business-model/

[30] D. K. Sharma and A. Sharma, "Deep web information retrieval process," *The Dark Web: Breakthroughs in Research and Practice*, p. 114, 2017.

[31] J. Corbin and A. Strauss, "Grounded theory research: Procedures, canons and evaluative criteria," *Zeitschrift für Soziologie*, vol. 19, no. 6, pp. 418–427, 1990.

[32] R. V. Kozinets, *Netnography*. Wiley Online Library, 2015.

[33] J. Martin and N. Christin, "Ethics in cryptomarket research," *International Journal of Drug Policy*, vol. 35, pp. 84–91, 2016.

[34] S. A. Bakken, "Silk road 2.0-a study of cryptomarkets in a deleuze-guattarian perspective," Master's thesis, University of Oslo, 2015.

[35] T. J. Holt, A. M. Bossler, and K. C. Seigfried-Spellar, *Cybercrime and digital forensics: An introduction*. Routledge, 2015.