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.

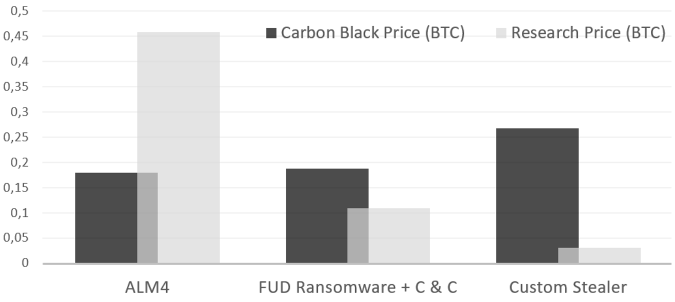


Fig. 1. Comparing costs between the results of this research and Carbon Blacks.

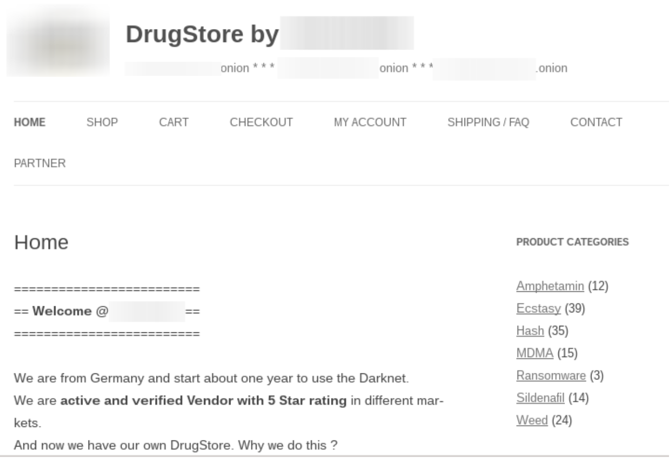
Prices in their report were listed in US Dollars, which made it difficult to make fair comparisons because BTC to USD exchange rates fluctuated a lot during the autumn of 2017.

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 SHOP CART CHECKOUT MY ACCOUNT SHIPPING / FAQ CONTACT PARTNER

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 ?

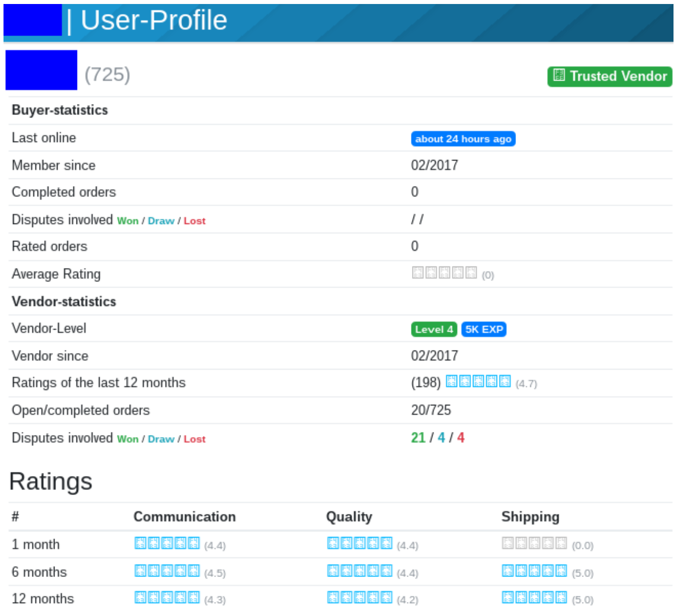
PRODUCT CATEGORIES

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.

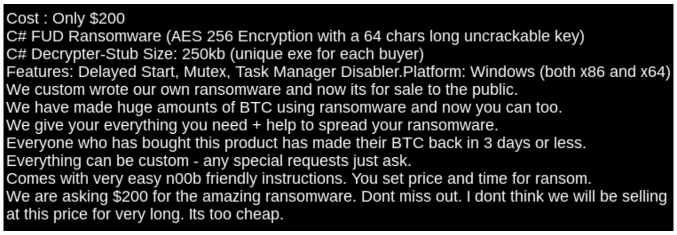
One specific feature we noticed for Dream Market, was that every vendor profile had its AlphaBay ranking listed (not as free text). It is unclear how this has been managed, but we can assume that there has been a collaboration between AlphaBay and Dream Market when AlphaBay was taken down. This could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

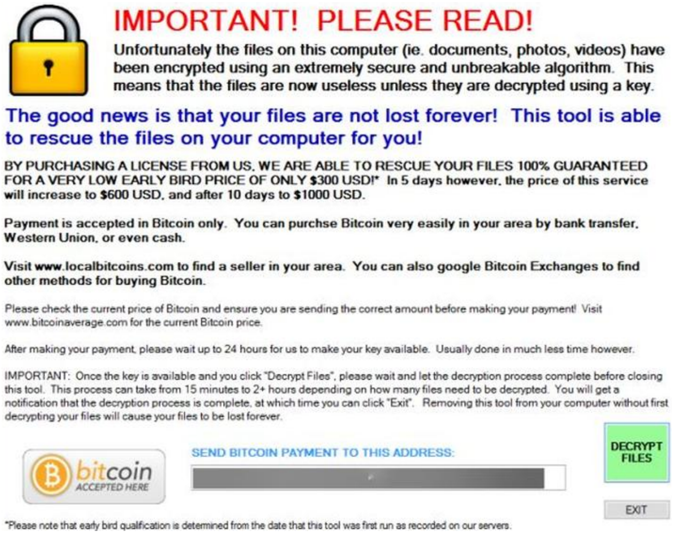
Different media was used by the vendors to market services to potential buyers, or illustrate how the RaaS works on a victim's computer. The type of media was limited to images attached to the service description or a link to a website with the video. No images were included in comments made by buyers.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

*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.

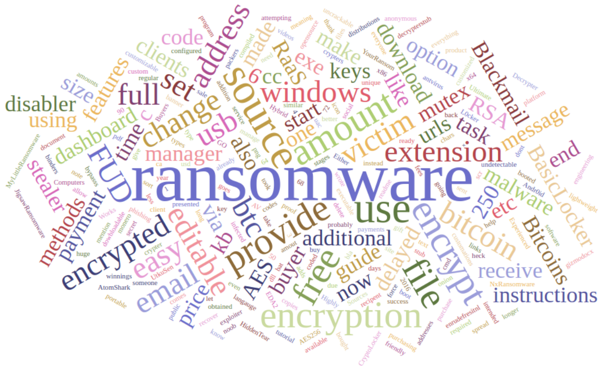


Fig. 6. Word cloud of the RaaS descriptions.

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.