Vendor Communication Themes in Darknet Ransomware-as-a-Service (RaaS) Advertisements

Taylor Fisher[1]
fishe516@msu.edu

Zacharias Pieri[2]
zpieri@usf.edu

C. Jordan Howell[2]
cjhowell@usf.edu

Roberta O'Malley[2]
Omalley14@usf.edu

Lauren Tremblay[3]
Lauren.tremblay16@gmail.com

Mohamed Dawood[3]
mohamed.dawood@student.giu-uni.de

[1] Michigan State University
655 Auditorium Rd, Room 557
East Lansing, MI 48824

[2] University of South Florida, Sarasota Manatee
8350 N Tamiami Trail
Sarasota, FL 34243

[3] University of South Florida, Sarasota Cybersecurity Lab Member[3]
8350 N Tamiami Trail
Sarasota, FL 34243

Corresponding Author:
Taylor Fisher
School of Criminal Justice, Michigan State University
Baker Hall
655 Auditorium Rd, Room 557
East Lansing, MI 48824
Fishe516@msu.edu

Abstract

In online illicit marketplaces, the Ransomware-as-a-Service (RaaS) industry is experiencing rapid growth. While traditionally ransomware was deployed by adept cybercriminals to lock or encrypt network assets, subsequently demanding a ransom for the decryption key, at present, RaaS is being marketed on darknet platforms as a pre-built, user-friendly form of ransomware. This study employs a thematic analysis of RaaS advertisements on darknet market to discern patterns in vendor communication with potential customers. The most common theme identified was victimization, appearing in 70% of the dataset, underscoring the nature of RaaS products as instruments of criminal activity. Victimization was commonly combined with other themes to persuade users to make a purchase. These findings provide critical insights into the commodification of ransomware and reveal the strategic mechanisms employed by vendors to attract both novice and experienced cybercriminals. The growing trend of RaaS highlights the ongoing professionalization of cybercriminal activities and underscores the necessity of cross-disciplinary research in addressing network security concerns.

Keywords: Ransomware, Ransomware-as-a-Service (RaaS), Darknet Markets, Cybercrime

Vendor Communication Themes in Darknet Ransomware-as-a-Service (RaaS) Advertisements

Abstract

In online illicit marketplaces, the industry to Ransomware-as-a-Service (RaaS) is experiencing rapid growth. While traditionally ransomware was deployed by adept cybercriminals to lock or encrypt network assets, subsequently demanding a ransom for the decryption key, at present, RaaS is being marketed on darknet platforms as a pre-built, user-friendly form of ransomware. This study employs a thematic analysis of RaaS advertisements on darknet market to discern patterns in vendor communication with potential customers. The most common theme identified was victimization, appearing in 70% of the dataset, underscoring the nature of RaaS products as instruments of criminal activity. Victimization was commonly combined with other themes to persuade users to make a purchase. These findings provide critical insights into the commodification of ransomware and reveal the strategic mechanisms employed by vendors to attract both novice and experienced cybercriminals. The growing trend of RaaS highlights the ongoing professionalization of cybercriminal activities and underscores the necessity of cross-disciplinary research in addressing network security concerns.
issues of network security.

Keywords: Ransomware, Ransomware-as-a-Service (RaaS), Darknet Markets, Cybercrime

1. INTRODUCTION

The online illicit marketplace consisting of darknet websites aimed at selling illicit goods and services provides a convenient platform for the commercialization of ransomware-as-a-service (RaaS). Ransomware is a malicious software type that encrypts data on the victim's network and blocks their access until a ransom is paid. With RaaS, hackers build ransomware using their own proprietary code, then advertise and sell the malicious code, typically on the darknet. Ransomware attacks pose a threat to both individuals and organizations, typically targeting critical infrastructure and organizations which house sensitive information (e.g., financial institutions, hospitals, etc.). In 2021, a ransomware group attacked the Colonial Pipeline, a critical piece of American infrastructure that provides oil to the East Coast, collecting over 100 GB of data in just a few hours. The attackers demanded a ransom of 75 bitcoin, or approximately $4.4 million USD. An attack of this size, even with the ransom being paid in a matter of hours, shut down the pipeline for multiple days, triggering a country-wide state of emergency (Beerman et al., 2023). These types of attacks put critical resources and infrastructure at risk and threaten data security for a wide range of organizations. An online market for RaaS products has developed, gaining momentum across a variety of darknet marketplaces. RaaS widens the array of illicit actors and creates opportunities for those with limited technical expertise to become operationally active in ransomware attacks.

Before the development of RaaS, ransomware attacks were exclusive to a group of seasoned cybercriminals with advanced network intrusion skills. The commercialization of ransomware has led to a widespread adoption of ransomware as an attack vector. It is now possible for someone without the skillset to develop their own malware to carry out a ransomware attack using a prebuilt ransomware package bought on the darknet. The darknet is

notorious for hosting criminal behavior due to its advanced privacy structure and it plays a key role in the commodification of malicious tools and services.

The growth in RaaS products follows the larger growth of cybercrime-as-a-service, where sophisticated attack capabilities are being made available to users regardless of their skill level (Shulman, 2010). The technical barriers to engaging in ransomware attacks have been reduced, leading to a growth in threats to both government and industry. This growth highlights the professionalization of ransomware markets, where increasingly sophisticated individuals are profiting from the development of their tools, thus exposing the difficult task facing law enforcement in preventing cyber-attacks against critical infrastructure. Law enforcement and IT personnel work to respond to and prevent cyber-attacks, however, without insight into the behavior of the attackers, their goals, the tools they are using, and the exploits they are taking advantage of, it would be difficult to resolve the conflict without paying the ransom in the hope that the hackers restore access. RaaS has been identified by some scholars as a "modest" threat, suggesting that the RaaS products may not be worthy of attention from law enforcement, and other types of threats may be a better focus of limited law enforcement resources (Meland et al., 2020). These types of research outputs fail to take the market as a whole into consideration, instead focusing on a small subset of RaaS products and markets. As of 2023, RaaS is on the rise and specialized law enforcement units are targeting common uses of RaaS products (Chainalysis Report, 2024). The recent takedown of the Hive, a ransomware group known for the provision of RaaS products, exemplifies the importance of understanding the influence of the darknet marketplace for these products and how vendors use this platform to communicate with potential customers.

In this study, we conducted a systematic analysis of 105 ransomware advertisements from 49 vendors that were posted across 26 darknet marketplaces. Through a thematic analysis of the ransomware advertisements, we identify patterns in how these vendors communicate with potential customers about their product, their use, and the vendors' role in providing them. These themes inform our understanding of the market for RaaS, offering critical insight into the commodification of ransomware and its growing accessibility to illicit actors with limited technical expertise. The results reveal an extensive network of RaaS vendors operating across a variety of markets, underscoring the broadening reach of ransomware within the online illicit economy. This analysis is critical in understanding the commercial dynamics of the proliferation and widespread adoption of ransomware and is significant for developing more effective strategies for cyber security and law enforcement to mitigate the growing threat posed by these illicit networks.

2. LITERATURE REVIEW

2.1.1 Darknet Illicit Marketplaces

The *darknet* is typically associated with portions of the internet that are unindexed, or not recorded in any central repository (like Google). While various platforms exist (e.g., Invisible Internet Project (I2P)), The Onion Router (TOR) is the most commonly used. Initially developed by the Navy (though now operated as a nonprofit), TOR provided a protected form of communication to allow agents to communicate with each other in an anonymous manner (Tor Project, 2024). The key was to facilitate enough traffic so that the military communications on the network were masked and therefore undetectable by adversaries. Importantly, TOR operates on a shared network of nodes, which bounce traffic multiple times, thus “anonymizing” the network traffic. While this would anonymize traffic to an average computer user, the network

can be identified and thus sources of illicit content can be tracked down, providing an opportunity for law enforcement to find the sources of illicit goods and services being sold on the darknet. Similar to Bitcoin, while initially difficult to trace, time has shown that it is still difficult to remain truly anonymous on the internet. The ability for the darknet to mask users' network traffic comes from its layered network that produces unindexed website access. Unindexed websites (called onion sites, due to their *.onion* domain) cannot be found using traditional search engines like Google or Bing. While there are legitimate uses of the darknet (e.g., news sources providing wartime updates to users in countries with censored internet access), the layered network allows for masking of network traffic, thus making it a key platform in the proliferation of illicit goods and services.

The difficult-to-trace nature of the darknet makes it a hub for criminal activity. Research suggests that even with conservative estimates, roughly 57% of TOR websites facilitate criminal activity related to drugs, guns, murder for hire and other criminal services, and child pornography file sharing (Moore & Rid, 2016). More specifically, the darknet provides an opportunity for hackers to benefit from the network of like-minded individuals. While the darknet provides a unique platform for forums related to criminal activity (Kamphausen & Werse, 2019), the current study focuses on the darknet as a marketplace for illicit goods and services to be sold. These goods include both the product of successful hacks (i.e., data breach content files) and ransomware.

Markets that are housed on onion sites typically house vendors in the same way websites like Amazon or Etsy would. Vendors with specific products or services to offer will host their advertisements on the marketplace website, providing an opportunity for users of the website (i.e., potential customers) to search for a single product among multiple vendors. Vendors

typically will specialize in one category of goods (i.e., drugs or guns; Soska & Christin, 2015; stolen identity products; Howell et al., 2022). Research has also shown that the trust signaling (i.e., security of the product and trust in the vendor) varied dependent on the type of goods/services provided, suggesting that vendors offering fraud related products may have innate concerns like liability for criminal activity (Laferrière & Décary-Hétu, 2023).

2.2.1 Ransomware

Ransomware is a type of malicious software that encrypts or blocks a victim's access to data unless the victim pays a ransom to regain access. The ransom amount varies, ranging from a few hundred to thousands of dollars, and payment is typically requested in cryptocurrency such as Bitcoin, which makes tracking these payments back to offenders difficult (Datta & Acton, 2024; Madhira et al., 2023). For instance, a report by Palo Alto Networks and Unit 42 (2023a) found that among the cases investigated by their emergency response team, the median ransomware payment demanded by cybercrime offenders was $650,000 USD, with demands ranging from $5,000 USD to $50 million USD.

Ransomware is a major security threat for individuals and businesses, creating major interruptions in business and resulting in lost revenue. According to the Federal Bureau of Investigations Internet Criminal Complaint Center's Internet Crime Report (2022), there were 2,385 reported incidents of ransomware, resulting in losses of over $34.3 million USD in 2022. These figures only represent reported incidents, and the actual number of attacks is likely much higher. According to IBM, a data breach costs on average $4.8 billion (IBM Security, 2024), making the loss of any data a huge concern for both government and industry. In addition, ransomware can also be used to mask espionage and intellectual property theft against large corporations conducted by nation-states (Palo Alto Networks and

Unit 42, 2023b; Holt et al., 2023). For instance, the 2017 WannaCry ransomware attack was attributed to North Korean state-sponsored hackers, with the goal of acquisition of funds from their victims (Turner et al., 2019). Other nation-state sponsored attacks, like the 2014/2015 attack against the US Office of Personnel Management by a Chinese-state-sponsored hacking group, are focused on stealing valuable data. In this attack, the hackers captured information related to background checks, resulting in the loss of 22 million individuals' data (Fruhlinger, 2020).

Individuals may lose personal and sensitive data, such as images, documents, and financial information due to ransomware. In other situations, ransomware offenders may threaten to publicly expose data on the darknet, which can result in reputational harm and possible legal action against companies (Palo Alto Networks and Unit 42, 2023b). When nation-states are targeted, ransomware can also impact national security and critical infrastructure. For example, fuel supplies on the US East Coast were significantly disrupted in 2021 as a result of the ransomware attack, allegedly performed by Russian hackers, on the Colonial Pipeline (Hobbs, 2021). The attack caused widespread disruption, prompting Colonial Pipeline to temporarily halt pipeline operations in order to control the damage. This incident caused fuel shortages in various areas, resulting in panic buying and subsequent price increases at petrol stations (Hobbs, 2021). In another example, Costa Rica was hit by two large-scale ransomware attacks in 2022, putting the country in a state of emergency. This attack was attributed to the Conti ransomware, a prolific RaaS operation that was first exposed in 2020. The group initially targeted the Ministry of Finance, but over time they caused significant disruption to both government services and the country's trade industry. After demanding $10 million, this RaaS product continued to encrypt various agencies' data, requiring the halt of operations (Burgess,

2022). The RaaS market poses a threat to critical infrastructure through both disruption and dissemination of valuable data, thus threatening the operations of healthcare systems, transportation networks, and utilities (Datta & Acton, 2024; Ghayoomi et al., 2021; Adams-Collman, 2018).

Cybercrime offenders may infiltrate systems and steal data using an assortment of tactics, such as social engineering schemes designed to trick employees into allowing offenders remote access to their systems (Palo Alto Networks and Unit 42, 2023b; Gallegos-Segovia, et al., 2017). In most instances, cybercriminals will deploy malware that encrypts a company's files and delivers a ransomware note after the initial company breach (Palo Alto Networks and Unit 42, 2023a). In Figure 1, the WannaCry ransomware showed a message on user devices stating that their information had been encrypted and that to decrypt the files they would need to pay the ransom. These encryption schemes are increasingly delivered with harassment and other extortion threats where the hackers threaten to publicize information. In addition, it is becoming more common for the ransomware attack to focus on data theft, as opposed to simply disruption of the network (Palo Alto Networks and Unit 42, 2023b). Hackers will threaten to disseminate the data stolen or even just the nature of the attack, often resulting in harm to reputation for the companies affected (Möller, 2023).

Governments and organizations all over the world are taking action to combat the threat of ransomware. The Biden administration in the US has issued an executive order to strengthen cybersecurity for critical infrastructure and federal agencies (White House, 2021) and in 2022 the Ransomware act was passed, requiring the Federal Trade Commission to report on cross-border complaints involving ransomware, with a specific emphasis on state-sanctioned ransomware attacks from key adversaries (i.e., Russia, China, North Korea, and Iran;

Ransomware Act, 2022). Additionally, in 2023 the United States put out a joint statement with the International Counter Ransomware Initiative (CRI) which described efforts to combat ransomware from a global perspective. The initiative aims to develop technical capabilities and information sharing infrastructure to assist in ransomware attacks that span multiple countries (White House, 2023). Ransomware continues to threaten critical infrastructure and personal privacy making it a growing concern of law enforcement as the ransomware as a service (RaaS) market grows.

2.2.2 Ransomware-as-a-Service (RaaS)

Ransomware users traditionally had to have the skill level necessary to not only send ransomware but complete the required reconnaissance to know which networks (and what areas of those networks) are worth targeting. With RaaS, now a larger number of less technically skilled computer users can use ransomware to target their adversaries without having to build the malware themselves. Novice users will not be able to make changes on the fly adjusting to new revelations about the target and their network's structure (Baker, 2023). This also means that code being used against multiple targets is likely to be consistent, making it easier for law enforcement and other cybersecurity professionals to use the same patch, or fix, for one network across other potential targets. While truly customized ransomware can be stopped and removed from a network, this fix would only work for that specific type of ransomware. Now with proprietary ransomware code being used against multiple targets, the patch or fix that stops the attacker on one network will likely work on others as well. This makes RaaS uniquely defendable as compared to its more unique, customized ransomware that is not sold for personal use.

RaaS can follow different models, typically left up to the vendor providing the service. These models typically determine the ownership of the ransomware product itself (a one-time license use or a monthly subscription for a flat fee), and how the profits from the attack will be split (either no profit sharing or an established split, with 20-30% going to the ransomware developer; Baker, 2023). The darknet marketplace provides a platform for ransomware developers to sell directly to users interested in buying RaaS products. This marketplace allows vendors with different RaaS models to reach customers and advertise their RaaS products. From 2016 to 2018, the advent of Ransomware-as-a-Service (RaaS) enabled individuals with minimum technological ability to construct and disseminate their own ransomware. This change democratized the ransomware landscape, boosting its prevalence (Gunn, 2024). RaaS is one component to an overall movement towards cybercrime as a service, in which cybercrime has become more automated, organized, and accessible to individuals with limited technical skills (Sood & Enbody, 2013). Within this framework, stolen data and cybercrime services, such as a Distributed Denial of Services (DDoS) attacks, stolen credit card numbers, and malware are sold for profit by vendors online (Holt & Lampke, 2010; Shulman, 2010; Sood & Enbody, 2013).

One of the most successful and impactful RaaS products was the GandCrab ransomware. Introduced in 2018, hackers utilized a variety of strategies to not only avoid detection but make the attack more efficient (Palo Alto Network and Unit 42, 2021). The Russian hacking community showed advertisements offering access to its affiliate program, where users can use the ransomware to target their own adversaries, with 30-40% of the revenue going back to the developer. The affiliates then get access to a full web panel and technical support. GandCrab was successful because they continuously adapted their products to fit the evolving landscape,

including the ability to function without internet access, making it a key player in the RaaS market. Although considered a dual threat for combining file encryption capabilities with data theft tools, the GandCrab RaaS eventually retired, stopping service to the affiliate program in June 2019. At this point, the FBI was able to provide the decryption key to the devices still impacted by the RaaS. It is reported that the GandCrab RaaS product infected nearly 50,000 computers, mostly in Europe (Palo Alto Network and Unit 42, 2021). The unique ability for offenders to "retire" before being caught exemplifies the difficult nature of investigating online crimes which utilize anonymous platforms.

2.3 Law Enforcement Response to RaaS

The proprietary nature of RaaS code makes the response by law enforcement and cybersecurity professionals more straight forward than if the ransom came from a single actor. For example, in the takedown the HIVE, a ransomware variant which targeted more than 1,500 victims in over 80 countries, the FBI were able to infiltrate the group's computer networks and obtain the decryption keys. This effort thwarted over $130 million in active ransom demands, thus leaving the HIVE RaaS products obsolete (DOJ, 2023). Although receiving over $100 million in ransom payments prior to being shut down, the HIVE exposed the concept of a shared decryption key, where once the decryption process was understood, the FBI were able to decrypt over 1500 victims' networks (DOJ, 2023). By targeting RaaS providers, law enforcement and cybersecurity professionals can target a widespread attack with a common response. Put differently, if RaaS was a venom that suddenly found its way into thousands of humans, once doctors can find an antivenom that works for one patient, it can be recreated for others. The same concept applies here with decryption mechanisms developed by ransomware authors. This ability

to respond to large scale attacks without unique fixes or patches makes RaaS a valuable target for law enforcement to prevent widespread impact.

2.4 Current Study

The purpose of this study is to 1) explore and describe the different markets, vendors, and ransomware advertisements that exist on the darknet while assessing the extent of the ecosystem for RaaS products, and 2) to conduct qualitative analyses on ransomware advertisements to more fully understand how ransomware is being marketed and sold to buyers. In this paper, we provide a comprehensive examination of the growing Ransomware-as-a-Service (RaaS) market through a systematic analysis of ransomware advertisements. With over 100 advertisements collected and analyzed, the vendor provides central themes of information to communicate with potential customers about their product, including information about legality of the product and its victimization potential. The findings offer critical insight into the commodification of ransomware, where ransomware has become increasingly available to threat actors with limited technical skills. The themes identified in this paper suggest that vendors engage in strategic communication practices that appeal to both novice and seasoned cybercriminals. The contributions of these findings to both theory and practice are discussed.

3. METHODS

3.1 Data and Procedure

The data used in this study comes from 105 ransomware advertisements posted by 49 unique vendors across 26 darknet marketplaces. Data were collected in November 2022 and all markets were hosted on TOR. Darknet markets were identified through a combination of TOR search engines and previous studies. Onion sites (i.e., markets) can be difficult to find because they migrate to different onion links to avoid detection by law enforcement. Search engines for

TOR rely on crawlers, or automated internet browsers which document different content depending on their programming. These crawlers are designed to find and track onion websites as they move through different URLs to avoid detection.

To find new markets on search engines and to identify whether the market sells ransomware, a series of keywords were developed which allowed researchers to find relevant markets. Keywords included: ransomware, ransom, ransomware pack, and custom-made ransomware. These keywords were commonly seen as tags across platforms which indicated that these products were likely to be the most relevant to the current project. Markets were included if they had at least one advertisement for ransomware and were in English. One limitation of the current approach is that any markets in a foreign language were not able to be included. The limitations of the data collection process are discussed in further depth in section 5.2 below. Each advertisement was inspected so that only advertisements that specifically sold ransomware (as opposed to general advertisements for other forms of malware) were retained for analysis.

For each advertisement identified as ransomware there was a specific set of variables gathered from each market, vendor, and advertisement. The list of variables was adjusted as pertinent information was found on later advertisements[1]. The final list of variables included within the database: *market name, onion link, vendor name, tags, price (USD), price (BTC), crypto accepted, language, operating system (OS), description*[2]*, target audience, rating (product), rating (vendor), ransom amount, creation date, vendor creation date, total vendor*

[1] Darknet markets are inherently volatile due to the constant change in URLs. Whether vendors choose not to disclose information until after purchase or simply choose to leave markets as they move around, it is common for advertisements to be missing information. No discernable patterns among the missing data existed in this dataset, although an assessment of when and why vendors choose to withhold information would be a valuable addition to the literature.

[2] On some markets, the description encompassed all the variable information. On other markets, variables like operating system or language were included as tags. For this reason, any information about the vendor/product was recorded and the coding process identified the specific variables regardless of their source. Although markets may have similar structures, the information provided to prospective customers varies across markets.

sales, and *total product sales.* These variables provide insight into the market for RaaS on the darknet. Each description is analyzed for common themes, resulting in six identified themes. Each variable is broken down further in the following section.

3.2 Database Coding

3.2.1 Data Sources

Each advertisement typically consists of an image and a description. Data coding and analysis were focused exclusively on the written description, whether provided in the image or in the body of the advertisement itself. An example advertisement for a RaaS product is shown in Figure 2. On some markets this description was one collective paragraph or section on the page. Other markets included tags (n=29) which helped provide insight into the product types. Tags were used to identify product type, including "custom-made ransomware," "ransomware pack," "hacking," and "DDOS." Tags allowed the product to be searched for on markets where it was present. This could make markets easier to manage, making them more enticing to users. The presence of tags which index the products on the market indicates a level of sophistication by the market administrators.

Other sources of information include the product description. This was recorded and any information which informed the following variables was coded accordingly. In addition to these variables, the descriptions were analyzed qualitatively to identify common themes among advertisements. The results show six common themes across advertisements, which are described in more detail in section 4.2.

3.3.1 Market Characteristics

Market name: Collecting market name allows us to connect vendors across different ransomware marketplaces and to assess the number of active markets on the darknet that sell

ransomware. A market was retained for analysis if they had one or more advertisements for ransomware. A total of 26 markets were included in the dataset. These markets were found through a combination of previous studies' master lists and TOR search engines. Key terms used to search for markets were also used to identify advertisements for relevant products on the market[3].

Onion links: The onion link for each advertisement was collected to provide a source for each Raas product. To mitigate against the volatility of the darknet— in which onion links become defunct, inaccessible, or move overtime—screenshots for each advertisement were taken and recorded as well.

Accepted Crypto Currency: Most RaaS products are bought and sold through crypto currencies. This variable captures the type of currency accepted as payment for Raas products as specified by the advertisement.

The type of crypto accepted speaks to the sophistication of the market, where more developed markets are likely to accept a wider range of crypto currencies. It was common for advertisements to use Bitcoin to advertise the price of a product as it was the most common crypto currency used among markets. This is why the price of products are recorded both in USD and BTC below.

3.3.2 Vendor Characteristics

Vendor Name: The vendor's name was coded to understand the reach of more productive vendors within the larger markets. Collecting market and vendor names allows us to track vendors across markets and to see where markets, vendors, and products overlap. Over 26

[3] The current project did not include any communication platforms on which vendors sold ransomware products unless they were specifically a darknet marketplace. For example, it is common for individuals to sell illicit goods through Telegram channels, but those would not be included in the current dataset.

markets, there were 49 unique vendors identified that sold ransomware products. The most prolific vendor had 15 advertisements across multiple markets, with three vendors tied for second place with seven listings each.

3.3.3 Advertisement Characteristics

Price (USD & BTC): Price of RaaS products were included in the database. The price of the ransomware products was recorded to show the range of prices across the market for RaaS. Most products posted their price in both USD and crypto, while others only listed one or the other. In those instances, coders used a bitcoin converter to translate the price accordingly. This information provides insight into the cost of RaaS products and how accessible they are to buyers. Bitcoin was the most common crypto currency which is likely why most advertisements included their price in Bitcoin even if other crypto currencies were accepted by the market. The price in USD was collected to provide an easier comparison in a common currency.

Language and Operating System (OS): This information was not always readily available but was coded when possible. Only 14 product advertisements provided which language they were written in. Similarly with operating system (OS), only 23 advertisements included for which operating system they were designed. The language the product is written in and the operating system it is designed for are incredibly important for anyone looking to carry out a ransomware attack. It is unclear whether vendors would provide this information upon further inquiry, but our project did not include direct contact with vendors.

Target Audience: Target audience was coded to describe the type of network or organization that the product was designed for. Only six of the advertisements included data on the target audience.

Ransom amount: Most advertisements rather than providing a specific amount advertised as "build your own" meaning the customer could set the ransom amount to whatever they wanted. The buyer is able to set the ransom amount and currency accepted. Rather than discussing specific numbers, descriptions of ransom amount typically related to "making a lot of money."

3.3 Analysis Plan

The goal of this study is to explore and describe the features of RaaS products advertised on the darknet and to provide a more detailed qualitative examination of these advertisements. The first portion of the analysis includes descriptive analyses of markets, vendors, and advertisements, paying specific attention to the above study variables. Understanding these characteristics allows us to further describe the realities of how ransomware products are sold online.

The second portion of the analysis consists of a thematic analysis of the product descriptions (Braun & Clarke, 2006; Nowell et al., 2017). Within this process, two coders engaged in multiple readings and re-readings of the product descriptions. Coding decisions were discussed, with any potential issues or inconsistencies identified and addressed until agreement was reached by both coders. Thus, the qualitative coding process was reflexive and rigorous, involved multiple readings of each advertisement, an initial coding framework, and meetings between the coders to discuss the process, identified codes, categories which derived from the groupings of codes, and the themes that emerged as a result of the analysis. In total, six themes were identified. This process allows us to further understand how RaaS products are advertised to buyers, which provides important information concerning the market for RaaS on the darknet and who these products are advertised for.

4. RESULTS

4.1 Descriptive Features of Ransomware Advertisements

The market for RaaS identified in this study consisted of 26 markets, with 49 vendors posting a total of 105 advertisements for ransomware. Each advertisement was hosted on a TOR website and included some type of RaaS product. Typically, this was a build your own or customizable ransomware product where the malware could be used against any target for any amount of ransom, in any form of cryptocurrency[4]. Advertisements were all on English speaking markets, where other illicit goods were sold (e.g., drugs, guns, credit cards and other stolen information). The most common vendor was found on 15 different listings for ransomware, with three other vendors following, tied at seven listings each. The markets determine which crypto currencies are accepted. Bitcoin was the most common but other accepted crypto currency included Monero (XMR), Dogecoin (DOGE), Bitcoin Cash (BCH), Ethereum (ETH), Tether (USDT), Litecoin (LTC), Dash (DASH), and Zcash (ZEC).

Within the posted product description, vendors advertised reported income varying from $0-$3,000 based on the ransomware products they sold on the markets. This income refers to the amount of money a potential customer can expect to earn using this ransomware product. This was calculated by the total sales of each product and the price of the product. Products varied in price from $1-$1,437, with a mean price of $75.10. Product information on operating system was rare, as was information on language. Products reported a range of operating systems including Windows (most common), Linux, Mac, and Android. Advertisements also showed a range of programming languages, including Python, C, and Visual Basic (.NET). Only six advertisements provided information on potential targets but those mentioned included hospitals, businesses, big

[4] It is unclear whether this is true in practice. Without purchasing the ransomware and doing a forensic analysis of the code, we cannot be sure that the product does in fact work across all network types and can be fully customized.

companies, commerce, and BTC owners. These findings, although rare across advertisements, show the range of options available in RaaS products and how many potential skillsets a hacker might need. The RaaS market allows customers to find products designed specifically for their needs, something that a traditional hacker would need to build themselves after months of reconnaissance.

4.2 Qualitative Analysis of Ransomware Advertisements

Thematic analysis of the product descriptions of 105 ransomware products yielded six core frames which captured the central themes represented in ransomware products. Themes identified include victimization, customization, legality, assurances and guarantees, feedback solicitation, and money motivators. Given that ransomware products are malicious software with the purpose of extorting money from those attacked, it is unsurprising that the strongest code was that of victimization, which was represented across 70% of the dataset. A significant majority of the product descriptions were explicit that the products were designed with malicious intent to target individuals, businesses, and healthcare providers among others, and geared toward extracting financial grain from those affected.

While there were variations to each of the product descriptions, for example some contain all the six core frames, and some (a much smaller proportion) only one, for the most part each contained at least three frames, and followed similar logic - that of convincing someone to purchase the product. While each code may be seen as a standalone frame that has analytical value in its own right, the most effective product descriptions are the ones that knitted together aspects of the different frames to present a compelling rationale for why the product should be purchased, and some even functioned as coherent narratives for motivating purchase.

While each of the core frames will be discussed individually below, it should also be understood that in many of the products the frames intersect to help move along an individual to purchasing the product. The most elaborate and coherent of the product descriptions do this through creating a vision for what the product will achieve. Given that products are fairly explicit about the victimization aspect, a purchaser will understand that the product is to be used for malicious intent. It is at this point that the other core frames start to come into play. Customization, for example, serves the purpose of highlighting the flexibility of a product to fit the needs of the user, while assurances and guarantees function to ease the mind of the purchaser as to the legitimacy of the product, and that compensation is available should anything not work to satisfaction. Other frames work in different ways, for example money motivator operates in two ways - firstly to indicate that the purchaser stands to make substantial financial gain from the product, and secondly, in some cases, to add financial incentive to increase the likelihood of quick purchase. To reinforce the image of a capable product, some descriptions explicitly sought positive feedback from users with the promise of gifts for such reviews. The one code that stood out as being distinctly different was that of legality. Ransomware products are directly intended to target individuals in a malicious way and as such those who use them could stand to be prosecuted under various laws. A number of products sought to distance the vendor from any potential prosecution through advising that the product was solely for educational purposes, even while often outlining all the illicit uses for the product.

4.2.1 Victimization

As already noted, the importance of victimization to ransomware product descriptions cannot be underestimated. Indeed, this frame was present in approximately 70% of the product descriptors, and often appeared multiple times across each product description where it was

present, with a total of 198 mentions across all cases. It is without doubt that those purchasing ransomware products will have done so with the explicit intent of enacting a cyber-attack on other individuals or organizations for financial gain. In several cases, the notion of victimization was made explicit in the product titles, with use of words such as “ultimate blackmail”, “fraud”, “exploit”, and “locks screens”. Most references to victimization, however, were found within the main body of product descriptions, for example product #62 was particularly explicit in outlining the process of victimization that could be enacted through the purchase of the product:

> “Ransomware is a form of malware where [a] person attack[s] [a] victim[‘s] system with malicious code. Their intent is to lock [the victim] out of the system and encrypt important and sensitive data...Further, they demand ransom before they provide a decryption key for your locked system and encrypted data.”

The explanation of ransomware locking up systems which then force a victim to pay the hacker to unlock a system or to restore data is consistent across a number of cases. This is seen, for example, in product #105, “Ransomware will lock all files in the computer and unlock them after payment…Victim will have no choice but to contact you via email for payment”. In product #103, the description explains ransomware as a form of “cryptovirology” that “threatens to publish the victims’ personal data or to perpetually block access to it unless a ransom is paid.”

The purpose of outlining the many ways in which a potential victim could be inconvenienced, from having their system locked up, to the publication of their personal data, serves to reinforce the virility and efficacy of the product. It serves to reinforce in the mind of the purchaser that the product has the capacity to inflict damage in a way that will result in payment. In this sense, while victimization is explicit as its own category, it should be noted that victims are often seen as a means to an end. The product descriptions do not assume that a purchaser will

conduct a cyber-attack for the mere pleasure of inflicting inconvenience to others, but rather for a financial goal. The high presence of victimization language within the description of products mirrors the new emergence of ransomware as a service, indicating that many of these tools are being sold to a target audience of individuals who may not have the technical background to breach data systems and build their own malware to encrypt files and data. Instead, those with little technological skills can purchase a ransomware attack.

Most product descriptions are non-discriminatory when it comes to victim identification. This is because a seller likely wants a purchaser to think about potential victims in either an expansive way or does not wish to disrupt whatever image of victims that a buyer has in mind. There was one notable exception in the dataset, with one product (#40), explicitly focusing on Chinese targets.

The developers of this new virus have modified the simple code of the experimental ransomware to create something a little bit more dangerous. The virus is primarily targeted at Chinese audience though it might easily spread throughout other countries as well. It is different from other viruses of the same category because it uses never-before-tried methods of storing the victim's data and the file decryption key. For that, it uses Google Docs, which is also used as the virus's Command and Control server as well.

4.2.2 Money Motivator

Money (both in terms of financial gain from use of a product, and financial incentive to purchase a product), emerged as a strong theme present in approximately 47% of product descriptions. As with the victimization code, the money motivator code often appeared multiple times in product descriptions, with a total of 74 mentions. Victimization and money often appear in conjoined ways throughout the product descriptions with a clear path from victimization to

financial gain. In several product descriptions, some targets are even suggested, for example, companies, centers of commerce, and hospitals. Product #21 is explicit in this regard, noting that the product in question "is by far the best ransomware ever" and this is because it is the "Best Tool ever to Make HUGE money. You can send it to all big companies, commerce, hospital."

Dozens of other product descriptions note that with ransomware "you can make your own money", or "make some great money", or "best tool ever to make HUGE money". In this regard, the purchasing of a product can be seen as an investment for the purchaser and even with the purchaser viewing themselves in an entrepreneurial capacity. This line of thinking is encouraged in product #92, with the description projecting an image of the professionalization of hacking, "We are the only [product] that provide[s] a FREE Anonymous C&C Dashboard via Onion to manage your Clients." In addition to this a number of product descriptions refer back to ransomware products that made media headlines, highlighting again the potential for large sums of money to be made. This was seen in product #65, "Do you remember wannacry? They earned over $100,000 from ransoms".

In addition to making financial gain from potential victims, money is used as a way to incentivize purchase of a product. This is seen in product #12 with a promise of the "NEXT 10 ORDERS PAY ONLY $8 THEN PRICES GO BACK UP TO $95." Product #29 notifies potential purchasers of a unique promotion, "For now price is 55 usd, after 10 sales price will be 1500 $, hurry up get it while it's cheap". This demonstrates that there can be intense competition in the ransomware market, and that sellers are aware that introducing incentives might have the potential of increasing sales.

4.2.3 Customization

The second most significant code to emerge from the dataset is that of customization and refers to any instance in which a product could be modified to fit the needs of the purchaser. This code was present in 41% of the dataset and was mentioned 147 times. The customization code was frequently interlinked with that of financial motivation, as modifications to a given product have the capacity to increase financial gain. Several product descriptions note the ease in which ransomware can be edited to "set your own price and email and extensions and message and timer, etc." Others noting the global orientation to the ransomware market stress the ease of language customization of their products. This was clear in product #59, "Chaos is multi language ransomware which means you can translate your note to any language." This again has the potential to increase revenues for a potential buyer opening up victims on a global scale.

Product #91 is representative of the type of narrative that interlinks customization and financial gain, and so is worth capturing the key elements of the description here:

> This Ransomware is editable and you can change your own amount and bitcoin address…You will have the option to change the encryption extension of the ransomware; meaning you can have all encrypted files to end in any extension…So lets say the document encrypted was Gizmo_Prototype_design.docx you can encrypt it to become Gizmo.Prototype.design.example@example.com. Victim will have no choice but to contact you via email for payment. This gives you to increase payment charge based on victims urgency. With this ransomware you will also have the option to have it USB auto installable with time frame meaning, you can install it on a portable USB and it will automatically boot and start encrypting files after a given time frame of 2 hours or 2 days ..depending on your preference…

4.2.4 Assurances & Guarantees

Assurances and guarantees were found across approximately 50% of the dataset and with 86 mentions in total. Both categories served to ease the mind of the purchaser, back the quality of the product and ultimately to promote the selling of a product. In several examples, product descriptions give assurances about the efficacy of the product, for example noting that a product has “over 90% success guaranteed”. In other examples, sellers seek to give assurances through distinguishing themselves by offering support to anyone that has issues. This is seen through items such as, “We deliver full support” or “feel free to message me, I am here to help you anyway ;)”. This is especially contrasted with some product descriptions that explicitly state that a purchaser should have some technological experience as no further support can be offered.

One of the items that stood out is that some sellers recognize that given the nature of the products being sold, some buyers may be hesitant and fear that they themselves might become the victim of a cyber-attack. Some product descriptions sought to give assurances that the purchaser would be protected and would not become a victim themselves. This was seen with product #47, “I am providing clean code (written in Python) to be sure I am not scamming you to stole your data, and a well detailed guide to know how you can use it like a Professional.” Product #12 “All my items are tested and working 100%. If you have any problem, contact me and I will try to answer in 24hr.”

Guarantees function in a stronger way than assurances, and often either promise a money back guarantee or some other type of compensation if the product does not function to expectations. A typical example is with a statement like “100% satisfaction or money back guarantee”, or with product #54, “IMPORTANT! -100% Guarantee! if the method/software is not working anymore, you can choose 5 items from my shop!”

4.2.5 Legality and Feedback Solicitation

The two final codes that emerged from the dataset were those of legality and feedback solicitation. These were respectively the least significant codes with legality being present in 29.5% of the product description and feedback solicitation in 26%. These two codes stand out because they are less about the purchaser and more about the vendor. In both instances the focus of the narrative veers from the script of asking the purchaser to imagine victims, financial gain, the ease of use of a product or even the quality of a product. Instead, they function to protect and promote the seller. Legality appears slightly more frequently than feedback solicitation, and functions to distance the vendor from any nefarious style of activity that the product may be used for. As such this could be seen as a "get out of jail" card or form of plausible deniability for a seller. Product #29 is particularly interesting in this regard as after explaining that large amounts of money can be made from the product through the targeting of business and hospitals, it also states, that the product is "For educational Purpose Only" and that, "I'm not responsible of what you will do". In addition to this, the description goes on to warn that the purchaser must read the instructions first, "WARNING DO NOT OPEN THE FILE WITHOUT READING THE TUTORIAL FIRST!!! YOU CAN INFECT YOURSELF, I WILL NOT BE RESPONSIBLE". Product #48 has a similar line of argument in that after extolling the product as the ultimate tool for blackmail goes on to say, "Please only use this material and or software for research purposes. Using it for any illegal activity is not tolerated". Product #44 markets itself as particularly effective in targeting Android devices, but also includes a disclaimer that "ALL MATERIAL, SOFTWARE, TUTORIALS ARE STRICTLY FOR: ACADEMIC, RESEARCH, EDUCATIONAL and TRAINING ONLY – WE DO NOT CONDONE ILLEGAL ACTIVITIES". In almost all examples illegality is juxtaposed with a claim to legality.

With regard to feedback solicitation, this serves the explicit purpose of improving the reviews of a given product. It is clear that some vendors believe that positive reviews of a product could lead to an increase in sales. As such, purchasers are encouraged via “freebies” to give positive reviews of a product. This type of scenario is seen in product #55 with, “request your free bonus after positive feedback”, or in product #75, “If you leave positive feedback, you will get a product of your choosing for free.”

5. DISCUSSION

This study provides an examination of the rapidly expanding Ransomware-as-a-Service (RaaS) market through the systematic analysis of 105 ransomware advertisements across 26 darknet marketplaces, representing 49 vendors. A thematic analysis revealed six central themes: victimization, customization, financial motivators, assurances and guarantees, legality, and feedback solicitation. These findings offer critical insights into the commodification of ransomware, which has become increasingly accessible to a wide array of actors, including those with limited technical expertise. The identification of these themes highlights the strategic mechanisms employed by RaaS vendors to appeal to both novice and seasoned cybercriminals, underscoring the professionalization and broadening reach of ransomware within the illicit digital economy. This analysis is pivotal in understanding the commercial dynamics that underpin the proliferation of ransomware and the operational structures that support its widespread adoption in cybercrime.

The emergence of RaaS reflects a broader transformation within the cybercrime ecosystem, characterized by the increasing commodification of malicious tools and services. Rather than being the exclusive domain of technically advanced actors, ransomware is now accessible to a far wider range of individuals, facilitated by the ease with which cybercriminal

services are packaged and sold. This shift parallels the growing prevalence of "cybercrime-as-a-service" (CaaS), wherein sophisticated attack capabilities are made available to users regardless of their skill level (Shulman, 2010). Previous research highlights the role of CaaS in democratizing cyber-attacks, enabling individuals with varying levels of technical proficiency to carry out complex operations (Sood & Enbody, 2013; Holt & Lampke, 2010). These developments align with the findings of Meland et al. (2020), who underscore how the reduction in technical barriers has expanded the pool of potential attackers and intensified the global spread of ransomware. This commodification, central to our study, reveals not only the professionalization of ransomware markets but also the increasing sophistication of their operations.

Our analysis further exposes how victimization lies at the heart of RaaS marketing, with approximately 70% of advertisements emphasizing the potential harm inflicted on targets. This focus on victimization highlights how cybercriminals frame their actions as primarily driven by financial gain, with victims seen as instruments to achieve monetary rewards rather than as individuals or organizations targeted for ideological or personal reasons. This aligns with broader trends in cybercrime, where the depersonalization of attacks has become more pronounced, as financial incentives supersede other motives (Holt & Bossler, 2015). Ransomware advertisements frequently emphasized the damage that could be inflicted on victims, underscoring the potential for profit by exploiting vulnerabilities in individuals, businesses, and critical infrastructure (Palo Alto Networks & Unit 42, 2023b). This shift in the nature of ransomware, from ideologically motivated attacks to financially driven victimization, is reflective of the growing commercialization of cybercrime (Kshetri, 2016).

Money Motivator emerged as another dominant theme, present in 47% of the product descriptions. The frequent co-occurrence of financial gain with victimization underscores how central monetary rewards are to the ransomware market. As seen in prior research, the commercialization of cybercrime has fostered an entrepreneurial mindset among cybercriminals, where ransomware is marketed as a lucrative investment opportunity (Holt, Smirnova, & Chua, 2016). This framing of ransomware as a tool for financial independence reflects broader trends in illicit economies, where criminal activities are increasingly viewed through a business lens (Décary-Hétu & Aldridge, 2015). Vendors often employ competitive pricing strategies, such as limited-time discounts and price increases, which mirror legitimate e-commerce tactics and contribute to the professionalization of the RaaS market (Martin, 2014). Understanding the financial incentives driving both buyers and sellers in this ecosystem is critical for developing interventions that disrupt the economic drivers of ransomware attacks.

The customization theme, identified in 41% of the dataset, underscores the flexibility of RaaS products and their appeal to a global market. Customization allows attackers to modify ransomware to suit specific targets, increasing the potential financial reward. This finding aligns with literature on the increasing sophistication of cybercriminal tools, which are becoming more adaptable to diverse targets (Ablon et al., 2014). Customization also facilitates the global spread of ransomware, as attackers can tailor their attacks to different industries, geographic regions, or languages, further expanding their reach and profitability (Yar & Steinmetz, 2023). This trend reflects a broader shift in cybercrime, where attackers are incentivized to refine their methods to exploit specific vulnerabilities more effectively, thus maximizing their earnings (Agrafiotis et al., 2018).

The Assurances & Guarantees theme, found in 50% of the dataset, highlights how vendors seek to establish trust in their products by offering guarantees of success and customer support. This is consistent with findings from other illicit markets, where trust and reputation are key to facilitating transactions (Holt & Lampke, 2010). Guarantees of product efficacy, such as money-back offers or success rates over 90%, help alleviate concerns that buyers may have regarding the reliability of the product. By offering these assurances, vendors can reduce the perceived risks associated with purchasing ransomware, particularly for less-experienced cybercriminals (Holt et al., 2016). This not only enhances the credibility of the vendors but also stabilizes the market by making it appear more professional and less risky to potential buyers.

Finally, Legality and Feedback Solicitation were the least prominent themes, present in 29.5% and 26% of the dataset, respectively. Disclaimers such as "for educational purposes only" allow vendors to distance themselves from the illicit use of their products, providing them with a form of plausible deniability (Décary-Hétu & Aldridge, 2015). These disclaimers highlight the tension between the inherently illegal nature of ransomware and the need for vendors to maintain a façade of legitimacy. Similarly, feedback solicitation operates to enhance the vendor's reputation, with positive reviews functioning as social proof that can drive further sales (Martin, 2014). In this way, reputation management becomes a critical component of the RaaS market, mirroring practices in legitimate business environments.

Theoretical Implications

This study's findings provide important contributions to the theoretical discourse on cybercrime by situating the RaaS market within established frameworks, such as Routine Activity Theory (RAT) and the theory of cybercrime ecosystems. Routine Activity Theory, which posits that crime occurs when a motivated offender, a suitable target, and the absence of

capable guardians converge (Cohen & Felson, 1979), is highly applicable in explaining the proliferation of ransomware. RaaS significantly reduces the technical barriers to cybercrime, thereby increasing the pool of motivated offenders. This accessibility, combined with the relative anonymity of the darknet and cryptocurrency transactions, creates a criminogenic environment where capable guardianship is limited, leading to more opportunities for crime (Holt & Bossler, 2015). Our findings reinforce RAT by showing how the commodification of ransomware transforms previously complex cyberattacks into routine transactions that can be easily executed by a broad range of actors, including those with minimal technical expertise.

Additionally, our findings advance the understanding of cybercrime ecosystems, as described by Décary-Hétu & Leppänen (2013), by highlighting the professionalization of cybercrime markets. In line with the ecosystem perspective, RaaS vendors are akin to service providers in legitimate economies, operating within a broader illicit marketplace that includes feedback systems, customer support, and reputation management. This professionalization introduces new dimensions to existing theories of organized crime and illicit markets, as it underscores the convergence between traditional business practices and cybercriminal activities. The rise of customizable and market-driven ransomware products suggests a need to integrate theories of digital entrepreneurship and illicit economies into our understanding of modern cybercrime (Martin, 2014). These insights push the boundaries of existing cybercrime theories by demonstrating that the operational structures of RaaS parallel those of legitimate industries, thereby necessitating a more complex theoretical framework that accommodates the intersection of criminality and commerce.

Policy Implications

From a policy perspective, our study underscores the urgent need for cybersecurity strategies that go beyond technical defenses to address the economic underpinnings of the RaaS market. Disrupting the financial mechanisms that facilitate ransomware payments could be a particularly effective approach, as it targets the core incentive driving these attacks. This includes targeting cryptocurrencies, anonymous payment systems, and other transaction methods favored by cybercriminals (Holt et al., 2016). Policies aimed at regulating these financial networks could reduce the profitability of ransomware, making it a less attractive venture for would-be attackers.

The global nature of RaaS products also necessitates enhanced international cooperation in tracking, prosecuting, and preventing these attacks. Given the borderless nature of cybercrime, aligning legal frameworks across countries would allow for more effective enforcement and cooperation. Additionally, the customization features we identified suggest that defenses must evolve to be more dynamic and adaptive, rather than static or reactive. Cybersecurity policies should prioritize the development of proactive, context-specific measures that can adapt to the continually evolving ransomware landscape (Agrafiotis et al., 2018).

Finally, the presence of assurances and guarantees in RaaS marketing highlights the importance of trust and reputation in these illicit markets. Law enforcement agencies could exploit this reliance on trust by infiltrating or creating counterfeit vendors, which could destabilize the relationships between sellers and buyers. Such interventions could disrupt the operational flow of these markets and undermine the trust that is essential to their functioning. Overall, our findings call for a multi-pronged approach that includes financial regulation,

international cooperation, and innovative enforcement tactics aimed at dismantling the economic structures that sustain ransomware attacks.

Limitations

While this study provides valuable insights into the RaaS market, several limitations should be acknowledged. First, our dataset of 105 ransomware advertisements from 26 darknet marketplaces, representing 49 vendors, may not capture the full diversity of ransomware products and vendors on the darknet. The volatile nature of the darknet, where marketplaces frequently disappear or relocate, further complicates a comprehensive representation of the RaaS ecosystem. As a result, some markets or vendors may have been missed during data collection.

Second, the exclusive focus on English-language markets may limit the global generalizability of our findings, excluding significant non-English speaking vendors from markets like Russia or China, known to play major roles in cybercrime (Holt et al., 2016). This focus potentially overlooks key dynamics in these other markets.

Third, relying on public TOR advertisements presents limitations, as the analysis was based on self-reported vendor information, which may be exaggerated or misleading. Vendors may overstate product efficacy, minimize risks, or provide inaccurate information to attract less-experienced buyers. We were unable to verify the authenticity of these claims as the study did not involve purchasing or testing the products.

Finally, our use of qualitative thematic analysis may introduce some subjectivity in interpreting vendor narratives. While we took steps to ensure reliability, such as employing multiple coders, the analysis remains influenced by researcher perspectives. Future research could benefit from quantitative methods, such as network analysis, to offer a more systematic understanding of vendor relationships and market structures.

Conclusion and Future Research

This study offers a critical examination of the RaaS market, highlighting the increasing commodification and accessibility of ransomware within the global cybercrime ecosystem. By analyzing the strategies employed by vendors to market their products, this research underscores the professionalization of cybercriminal activities and their growing impact on the digital economy. These findings point to the need for more comprehensive interventions that address the economic and operational drivers of ransomware proliferation.

Future research should expand the scope by investigating non-English speaking markets and employing advanced quantitative methods to explore vendor networks and market structures more deeply. Additionally, evaluating the effectiveness of policy and law enforcement measures in disrupting RaaS markets will be key to shaping effective global cybersecurity strategies. As ransomware continues to evolve, a cross-disciplinary approach will be critical in mitigating its growing threat.

6. REFERENCES

Ablon, L., Libicki, M. C., & Golay, A. A. (2014). Markets for cybercrime tools and stolen data: Hackers' bazaar. Rand Corporation.

Adams-Collman, J. (2018). Ransomware and cyber security: the king that did not wannacry. *Primary Dental Journal*, 7(1), 44-47.

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity, 4(1), tyy006.

Baker, K. (January, 2023). Ransomware as a service (RAAS) explained how it works & examples. Crowdstrike. Retrieved from https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/.

Beerman, J., Berent, D., Falter, Z., & Bhunia, S. (2023, May). A review of colonial pipeline ransomware attack. In *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)* (pp. 8-15). IEEE.

Burgess, M. (June, 2022). Conti's attack against Costa Rica sparks a new ransomware era. *Wired*. Retrieved from https://www.wired.com/story/costa-rica-ransomware-conti/

Chainalysis (February, 2024). The 2024 Crypto Crime Report. Retrieved from https://www.chainalysis.com/wp-content/uploads/2024/06/the-2024-crypto-crime-report-release.pdf

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588-608.

Datta, P. M., & Acton, T. (2024). Ransomware and Costa Rica's national emergency: A defense framework and teaching case. *Journal of Information Technology Teaching Cases*, 14(1), 56-67.

Décary-Hétu, D., & Aldridge, J. (2015). Sifting through the net: Monitoring of online offenders by researchers. *European Review of Organised Crime*, *2*(2), 122-141.

Décary-Hétu, D., & Leppänen, A. (2016). Criminals and signals: An assessment of criminal performance in the carding underworld. *Security Journal*, *29*, 442-460.

Department of Justice (DOJ) (January, 2023). U.S. Department of Justice disrupts Hive ransomware variant. DOJ Office of Public Affairs. Retrieved from https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant.

Federal Bureau of Investigation Internet Criminal Complaint Center (2022). *Federal Bureau of Investigation Internet Crime Report 2022*. Retrieved from chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

Fruhlinger, J. (2020, February 12). The OPM hack explained: Bad security practices meet China's Captain America. CSO. https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

Gallegos-Segovia, P. L., Bravo-Torres, J. F., Larios-Rosillo, V. M., Vintimilla-Tapia, P. E., Yuquilima-Albarado, I. F., & Jara-Saltos, J. D. (2017, October). Social engineering as an attack vector for ransomware. In *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)* (pp. 1-6). IEEE.

Ghayoomi, H., Laskey, K., Miller-Hooks, E., Hooks, C., & Tariverdi, M. (2021). Assessing resilience of hospitals to cyberattack. *Digital Health*, *7*.

Gunn, J. (June, 2024). The democratization of cyberattacks: How billions of unskilled would-be hackers can now attack your organization. *The Hacker News*. Retrieved from https://thehackernews.com/expert-insights/2024/06/the-democratization-of-cyberattacks-how.html#:~:text=Phishing%20and%20ransomware%20attacks%20were,access%20to%20launch%20an%20attack.

Hobbs, A. (2021). *The colonial pipeline hack: Exposing vulnerabilities in us cybersecurity*. SAGE Publications: SAGE Business Cases Originals.

Holt, T., & Bossler, A. (2015). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge.

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: products and market forces. *Criminal Justice Studies*, *23*(1), 33-50.

Holt, T. J., Griffith, M., Turner, N., Greene-Colozzi, E., Chermak, S., & Freilich, J. D. (2023). Assessing nation-state-sponsored cyberattacks using aspects of Situational Crime Prevention. *Criminology & Public Policy*, *22*(4), 825-848.

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). Exploring and estimating the revenues and profits of participants in stolen data markets. *Deviant Behavior*, *37*(4), 353-367.

Howell, C. J., Fisher, T., Muniz, C. N., Maimon, D., & Rotzinger, Y. (2023). A depiction and classification of the stolen data market ecosystem and comprising darknet markets: a multidisciplinary approach. *Journal of Contemporary Criminal Justice*, *39*(2), 298-317.

IBM Security (2024). Cost of a data breach report 2024. Retrieved from https://www.ibm.com/reports/data-breach.

Kamphausen, G., & Werse, B. (2019). Digital figurations in the online trade of illicit drugs: A qualitative content analysis of darknet forums. *International Journal of Drug Policy*, *73*, 281-287.

Kshetri, N. (2016). Big data's role in expanding access to financial services in China. *International journal of information management*, *36*(3), 297-308.

Laferrière, D., & Décary-Hétu, D. (2023). Examining the uncharted dark web: Trust signaling on single vendor shops. *Deviant Behavior*, *44*(1), 37-56.

Madhira, N., Pelletier, J. M., Johnson, D., & Mishra, S. (2024). Code red: A nuclear nightmare-navigating ransomware response at an Eastern European power plant. *Journal of Information Technology Teaching Cases*, *14*(1), 108-118.

Martin, J. (2014). *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs*. Springer.

Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. *Computers & Security, 92*, 101762.

Möller, D. P. (2023). Ransomware attacks and scenarios: Cost factors and loss of reputation. In *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices* (pp. 273-303). Cham: Springer Nature Switzerland.

Moore, D., & Rid, T. (2016). Cryptopolitik and the Darknet. Survival, 58(1), 7-38.

Palo Alto Network & Unit 42 (2021). Ransomware threat assessments: A companion to the 2021 Unit 42 ransomware threat report. Retrieved from https://unit42.paloaltonetworks.com/ransomware-threat-assessments/7/.

Palo Alto Network & Unit 42 (2023a). Ransomware and Extortion Report. Retrieved from https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2023-unit42-ransomware-extortion-report.pdf.

Palo Alto Networks & Unit 42. (2023b). 2022 Ransomware threat report. Retrieved from https://unit42.paloaltonetworks.com/ransomware-threat-report-2022/

Ransomware Act (2022). Reporting Attacks from Nations Selected for Oversight and Monitoring Web Attacks and Ransomware from Enemies Act or the RANSOMWARE Act. Retrieved from https://congress.gov/bill/117th-congress/house-bill/4551#:~:text=Passed%20House%20(07%2F27%2F2022),-Reporting%20Attacks%20from&text=This%20bill%20requires%20the%20Federal,individuals%2C%20companies%2C%20and%20governments.

Shulman, H. (2010). The cybersecurity dilemma: Hacking, trust and fear between nations. International Security, 41(1), 94-139.

Sood, A. K., & Enbody, R. J. (2013). Crimeware-as-a-service—A survey of commoditized crimeware in the underground market. International Journal of Critical Infrastructure Protection, 6(1), 28-39.

Soska, K., & Christin, N. (2015). Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. In *24th USENIX security symposium (USENIX security 15)* (pp. 33-48). Symposium, Berkeley, CA, USA, 2015.

Tor Project (August, 2024). The Onion Router. Retrieved from https://www.torproject.org/

Turner, A. B., McCombie, S., & Uhlmann, A. J. (2019). A target-centric intelligence approach to WannaCry 2.0. *Journal of Money Laundering Control*, 22(4), 646–665.

White House (May, 2021). Executive order on improving the nation's cybersecurity. *The White House: Presidential Actions*. Retrieved from https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

White House (November, 2023). International counter ransomware initiative 2023 joint statement. *The White House: Statements and Releases*. Retrieved from https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement/.

Yar, M., & Steinmetz, K. F. (2023). Cybercrime and society. Sage.