Analyzing Cybercrime Services and Trust Dynamics on the Dark Web: A Case Study of DarkDock Marketplace

Hägvall, Joel
Valverde, Giancarlo

Department of Computer and Systems Sciences

Degree project 15 HE credits
Computer and Systems Sciences
Degree project at bachelor level
Spring Term 2024
Supervisor: Nicolas Harrand

Stockholm University

Table of Contents

Abstract

In an era where the web is widely used by different operators, cybercrime has become an evolving threat due to increased digitalization and the accessibility of the web, which has an anonymized side to it referred to as the “dark web”. Research shows that the dark web has enabled criminals to commit cybercrimes, e.g. exchanging illegal documents and distributing malware through marketplaces. However, there is insufficient research on types of cybercrimes prevalent on the dark web, and how sellers and buyers establish trust on these marketplaces.

This study has the goal to uncover the types of cybercrime services present on the dark web, particularly analyzing the marketplace DarkDock. This includes how the services and sellers are portrayed to establish trust between the seller and customer. Further, highlighting the services and tactics provides an understanding of the dark web ecosystem that strengthens criminal activity.

To explore the topic, the research goal is to answer the question:

- What different types of cybercrime services are offered on the marketplace ‘DarkDock’ on the dark web? How do these offers show an established trust with buyers on the marketplace ‘DarkDock’?

In order to respond to the question, a web scraper was developed to collect data from DarkDock. Together with a content analysis we aim to obtain both a qualitative and quantitative understanding of the collected data. By developing codes and themes for types of services and trust-establishing methods, they provide insights and knowledge for answering the research question.

Our findings suggest that crime-listings related to access crime are the most mentioned on DarkDock, followed by network crimes. Specifically courses, data and confidential information are being sold and advertised by sellers. This is done through emphasizing communication and assistance in the listings, including ensuring fast deliveries and satisfaction for customers.

The conclusions contribute to an understanding of what is being offered and how the dark web ecosystem works from a trust-building perspective. This provides knowledge for identifying potential upcoming cyber threats and mitigating them. Further research could include examining more marketplaces and what drives demand for certain services on the dark web, and focusing on offerings related to guides and informational courses.

Synopsis

Background

The web as we know it has an anonymized side to it, often referred to as the dark web. The dark web is accessed through specialized software and has been used in forming new marketplaces and forums containing malicious content. This content ranges from malware tools and services to confidential information being sold. An example of such a marketplace is DarkDock, which offers a variety of offers.

Problem

Past research has examined the dark web and its marketplaces, for both offerings and the seller's marketing tactics. The identified research gap is the lack of detailed and comprehensive descriptions of the offerings, as well as how sellers and buyers maintain mutual trust when it comes to cybercrimes.

Research Question

The study aimed to research various forms of cybercrime present on the dark web today. Therefore, our initial inquiry was, "*What different types of cybercrime services are offered on the marketplace 'DarkDock' on the dark web? How do these offers show an established trust with buyers on the marketplace 'DarkDock'?*". Our goal was to gain a comprehensive understanding of the trust elements associated with offers found on the dark web, and to identify what contributes to the sellers' credibility among their buyers.

Method

The research utilized specialized software to navigate the dark web. The marketplace was scraped using a custom developed scraper, along with screenshots of the site. Following the data collection, a content analysis was conducted to quantify occurrences of words and sentences, and identify patterns and themes in offerings.

Result

By using content analysis, we identified the frequencies of keywords related to types of cybercrimes found on the marketplace DarkDock together with developed themes. We also identified trust-ensuring methods found in listings related to the themes. The answers to our questions revealed that listings related to courses were the most mentioned, with sellers emphasizing different trust elements such as assistance, customer care and security.

Discussion

The discussion chapter highlighted the findings and compared them to related research, showing similarities and differences while connecting to the developed themes. Additional interpretations were mentioned along with suggestions on future research based on the project's topic.

Conclusion

The conclusion chapter reveals insight into dark web marketplaces and how its accessibility is suggested to facilitate cybercrime. Through analyzing listings and trust-building mechanisms used in listings, trends can be identified by law enforcement that can indicate potential threats to prevent attacks. Further research is suggested to monitor markets to develop cybersecurity measurements. Ultimately, the research mentions limitations in methodology and suggests investigating the prevalence of courses on marketplaces and adjustments of the developed web scraper.

Acknowledgement

We would like to thank our thesis supervisor Nicolas Yves Maurice Harrand, for providing us with his guidance and knowledge throughout this research process. Additionally, we thank Stockholm University for giving us the opportunity to pursue our Bachelor's Degree in Computer and Systems Science.

List of Figures

List of Tables

List of Abbreviations

Keywords:

Dark web, Tor, malware, social engineering, data leaks, DDoS attacks.

1. Introduction

On the deeper and darker parts of the web, known as the dark web, it is possible to purchase services related to cybercrime for as little as 10 USD. These services exist on marketplaces and are accessible to buyers with no prior coding or technical knowledge of the services (HP Wolf Security Blog, 2022).

DarkDock is one example of a dark web marketplace that unites trustworthy vendors to combat scams and deliver 'high-quality' services to vendors and buyers. DarkDock provides a platform for everyone, with the condition that the activities should not cause harm to others. DarkDock assures complete anonymity and security, forbidding any involvement with e.g. child pornography. Further, the transactions are monitored on the site (DarkDock, n.d).

The activity and content on the dark web includes services that are rented or offered by criminals, e.g malwares, remote access trojans, data leaks and distributed denial-of-service attacks (Manky, D, 2013). The platforms on the dark web are accessible by the use of anonymisation tools such as Tor and I2P, which makes the activity difficult to track (Sangher, K.S, 2023).

The services offered on the marketplaces facilitates criminal activity and affect organizations and businesses, according to research made by PwC. Around half of the businesses have been experiencing economic fraud in the last two years, and external perpetrators such as "hackers" account for around 31% of the types of "external perpetrators" organizations face (Ellerbeck, S, 2022). Moreover, organizations face economic losses after cybercrime incidents. IBM reports that in 2023, the average expense resulting from a data breach climbed to $4.45 million USD, reflecting a 15% rise from the last three years. This calculation was made by evaluating the financial impact of data breaches on 550 organizations in 17 different countries and sectors, including healthcare and finance (IBM, 2023). The financial losses are further aggravated by a 125% increase of cyber attacks in 2021 when compared to 2020, according to AAG IT.

The dark web marketplaces provide a platform for this rise in cybercrime. The purchasing of Services that affect both individuals and organizations have been circulating on the dark web's forums and marketplaces such as Silk Road, which lets users leave reviews of the services (Brinck, J et al. 2023).

1.1 Research Problem

The problem we will address in this research is the lack of understanding the way cybercrime is facilitated on dark web marketplaces, that relies on anonymity. To gain more insight into these activities, we will examine and categorize cybercrime offers that are present on the dark

web marketplace DarkDock in the form of listings, as well as analyzing trust-building mechanisms used on offers that enable these purchases.

1.2 Research Question

- What different types of cybercrime services are offered on the marketplace ‘DarkDock’ on the dark web?

The research question investigates the range of cybercrime offers available on DarkDock, seeking to categorize these offerings into different categories in the study, with the goal to illustrate what activities are performed in the marketplace.

- How do these offers show an established trust with buyers on the marketplace ‘DarkDock’?

In order to understand in more detail these listings of cybercrime, this sub-question will analyze the trust-establishing mechanisms used in listings by using developed codes and themes based on e.g descriptions and reviews, with the goal of understanding the reasons behind the purchases and what is presented when it comes to these offers.

1.3 Purpose

Our goal with the research is to investigate the different types of cybercrime services and trust-establishing methods to contribute to a deeper understanding of cybercrime and the vendors credibility.

1.4 Delimitations

This research is solely focused on the marketplace DarkDock and its offerings related to cybercrimes and our chosen set of categories. Other listings were not included in the process, since they were not following our definition of what is considered a cybercrime.

The developed scraper is limited to the specific marketplace as it includes code and classes that are based on the DarkDock marketplace. The developed scraper makes the scraping process more manageable as it is tailored to the purpose of our research, compared to other generic web scrapers.

2. Background

2.1 Dark Web

2.1.1 Layers of the Web

The web can be split into three layers: Surface Web, Deep Web and Dark Web. The surface web can be described as the web that is within reach by the use of web browsers, for example Microsoft Edge or Google Chrome (Jin, 2024. p. 331-346). The surface web is also referred to as the clear net, meaning all of the information is accessible to the user, and while it may seem like plenty of information it only accounts for a small portion of the web as a whole (Ho Woon Chung, 2018).

The deep web on the other hand is not indexed on the internet, and consists of content that is behind steps of authentication. A deep web website is accessed via browsers and some examples include Netflix and Google Drive (Prabha & Mittal, 2023).

2.1.2 Dark Web

This layer, which is unindexed, is referred to as the dark web, which is a general term and exists along the deep web. Dark web is a part of the deep web that is made up of domains with the ".onion" prefix (Dilipraj, 2014. p.121-140).

The dark web extends beyond merely using onion links, as it can be accessed through other ways than using Tor, each offering a similar experience. Alternatives to Tor that gives access to the dark web include the Invisible Internet Project (I2P), an encrypted peer-to-peer network that provides anonymity and privacy. Another example is I2P which uses cryptography, shields users' identities and activities (Geti2p, 2019). Another example using peer-to-peer technology is ZeroNet, which incorporates Bitcoin cryptography for authenticating users and utilizes the technology of BitTorrent to provide content in an efficient manner among users (Zeronet, 2019). Further, there is Hyphanet, previously known as Freenet, a peer-to-peer network providing anonymous communication and resisting censorship. This is made possible by using a decentralized data storage system (Hyphanet, n.d.).

The term "dark web" can be described as another part of the internet. Due to its anonymity and security when it comes to connection, it acts as a way of communication for journalists and activists. At the same time, it has enabled criminal activity through the use of marketplaces with sellers and customers trading weapons and social security numbers with each other (National Institute of Justice, 2020). Given information from Europol, compromised data is the two to third biggest category of the content available on the dark web (Bank of Scotland, nd).

2.1.3 TOR Browser and its function

Entering the dark web is possible by using specialized programs such as the TOR Browser, which uses the TOR network. TOR, which stands for The Onion Router, is a project created as a result of surveillance threats and as a response to tracking users on the internet. The goal is to protect privacy and anonymity by routing the traffic through several servers and make

sure it is encrypted at every step of routing (The Tor Project, nd). The layers could be viewed as layers of an onion, where the traffic routes through other computers in order to hide the original origin of the connection (Finklea, 2017).

When it comes to TOR and its network, it does not use the traditional traffic routing that shows if a user has entered a certain website or not. When browsing the web, a data packet is obtained from the visited website. Normally, the IP address is included within the data packet's header that is being sent, which makes it possible to trace. TOR has a different approach to this, which simply includes more servers along the routing to obscure the path and make it difficult for the outsider to scan the path's origin (Ozkaya & Islam, 2019). TOR uses a model of communication that relies on "onion routing", which relays data over the internet by routing it through nodes. As the model contains multiple nodes, each node has its own decryption, and does not know its predecessor. In this way anonymity is provided since the connection is encrypted multiple times, along with a masked IP-address (Britannica, n.d).

2.1.4 DarkDock

The marketplace DarkDock provides a broad range of services catered to various needs within the dark web. From digital products to drugs, hacking services, bank account information, and even weapons. DarkDock claims that the market is committed to user safety and has implemented features designed to enhance security and anonymity. These include escrow services, multisig transactions, data encryption, and compatibility with TOR for enhanced privacy.

To engage in the community on DarkDock, users are required to register an account, deposit funds, and explore the marketplace to discover their products and services. Accounts are not required in order to only view products. While DarkDock takes measures when it comes to safety, users are encouraged to create strong passwords, enabling two-factor authentication, and remain cautious when interacting with links (DarkDock, n.d.).

2.2 Cybercrime and Different Tools

Cybercrime encompasses a range of illegal activities where computers or computer networks are utilized as means, targets or platforms for crime. This also extends to conventional crimes that are executed or supported through the use of computers or networks. Cybercrimes can be categorized into access crime, data crime, network crime and other related crimes concerning cyberspace, and can have effects including disrupting critical operations of an infrastructure and potentially revealing confidential authority or organizational information (Das & NayK, 2013. pp. 142-153).

Some notable examples of tools and services that are typically found on the dark web are described below.

2.3 Access Crime

The first crime category is called "Access Crime", which gives the attacker unauthorized access to a system. This can include different types such as malware and social engineering (Das & NayK, 2013. pp. 142-153).

2.3.1 Malware

Starting with malware, also referred to as malicious software, refers to software that is developed with the purpose to disrupt, damage, or gain unauthorized access to computer systems. This category of software can manifest in various forms, such as viruses, worms, Trojan horses, and spyware (Brookshear, J: Glenn & Brylow, Dennis, 2020). Applications with malicious intentions can be spread via email links or attachments that the user might have clicked on, and can even be spread by installing what is thought to be an application of legitimate sort. This is often downloaded through a third party and not from the original source providing the application (Malwarebytes, n.d).

According to research done in 2022 by the cybersecurity company Venafi, malware offerings on the dark web have increased due to more activity on underground forums. Since 2022, offerings related to ransomware and phishing have been found on 475 pages on the underground forums. Findings are that ransomware and other malwares are sold as services by attackers, and the program which was executed in order to attack and shut down the Colonial Pipeline, was sold for around 1200 dollars on the dark web (BleepingComputer, n.d). The attack against the pipeline which ships refined oil to the East Coast in the US, resulted in a gasoline shortage due to operations being halted for five days in regards to the attacks. The consequences were increasing costs for gas and panic among gas consumers (Wood, Kimberley 2023).

The service to carry out various attacks is offered as a service and can be executed by beginners with little to no technical skills or knowledge (BleepingComputer, n.d). There are different cybercrime groups that have been formed, for example the cybercrime group LockBit, which has attacked businesses, encrypted their files and demanded payment in ransom in order for the victims to get their files back. The group has made over billions of dollars and caused damage to multiple businesses, by providing their "affiliates" the necessary tools for them to execute the attacks (National Crime Agency, 2024).

2.3.2 Social Engineering

Further example of an Access Crime is social engineering, which is a known method where attackers manipulate human interactions to gain access to or compromise an organization's data or systems. It is characterized by the attacker pretending to be a trustworthy individual, such as a new employee for example. By communication, they can collect enough data to breach an organization's network (Cybersecurity & Infrastructure Security Agency, 2021).

A method of social engineering is phishing, which is known as a method used by attackers to retrieve sensitive information. During a phishing attack, the attacker can impersonate

companies or organizations in order to lure the victim through, for example, an email (Brookshear, J: Glenn & Brylow, Dennis, 2020).

Another method of social engineering is MFA (Multi-Factor Authentication) fatigue attacks, which is combined with the malware called infostealer. An infostealer is a program set up to obtain victims' passwords and cookie data, and is available at a low cost for attackers. An MFA fatigue attack is when the attacker has the relevant information of a user, both username and password, and is trying to log in multiple times. Along with the login attempts, multiple MFA push notifications are sent to the user, and the user could grant it access just to stop the notifications from being sent. According to Microsoft, after investigation of the known LAPSUS$ group, it was found that MFA fatigue attacks were used in several of their operations. By paying employees to get access to MFA approvals, and searching on public company code publishings for credentials, they could get access (Accenture, 2022).

Previous research has found that social engineering is a part of the services offered on the dark web. By examining 8 popular dark web marketplaces, the developed category in the research referred to as "media" takes up to 10% of the dataset used. In the "media" category everything from tutorials of fraud, cracking, information stealing and guides are prevalent. The guides relevant to fraud are found to be written in regards to social engineering, and do not typically require technical expertise (Dimitrios, Georgoulias, 2023 et al). Moreover, Accenture's Cyber Threat Intelligence Team found that exposed credentials listings increased with 40% on dark web marketplaces from July to October 2022, with the average pricing of $10 per data log. It is concluded that MFA implementations have to be complemented with biometric features, and awareness of social engineering tactics have to be in the center of organizations, as the infostealers will continue to thrive on the marketplaces (Accenture, 2022).

2.4 Data Crime

Data Crime is described as the type of crime which involves intercepting or sniffing network traffic, modifying or tampering with data as well as stealing data. Stealing data involves obtaining confidential information of individuals or businesses such as credit card numbers or passwords (Das & NayK, 2013. pp. 142-153).

2.4.1 Data Leaks

An example of data crime is data leaks, which is also known as data breaches. Data leaks involve an unauthorized party gaining access to information that is protected and sensitive, and can affect both individuals and businesses (Kaspersky, n.d). Data breaches can occur in several ways, for example through stolen credentials or social engineering attacks, as well as attacks from inside safe environments. The main target is often corporations with plenty of data that can later be sold on forums in the underground space (Cloudflare, n.d).

According to Forbes, security researchers from Security Discovery and CyberNews found a data leak containing records of 26 billion entries with leaked passwords. The entries were found to be related to user accounts on platforms such as LinkedIn, Twitter and Dropbox and also organizations related to the government. Further, the researchers believe that the attackers

could use the information to commit phishing attacks, obtain unauthorized access and perform identity theft. Proposed mitigations are changing of passwords, double check emails for phishing attempts and implementing MFA (Multi-Factor Authentication) as a security layer on all platforms (Forbes, 2024).

In regards to earlier mentioned research on 8 different marketplaces, it was found that leaks of information related to databases and account credentials were on the dark web's marketplaces. These were categorized as "Fraud" and accounted for around 71% of the listings examined. Examples related to "hacked databases", "carding" and "miscellaneous accounts" are exposed voting procedures, bank card information and Netflix accounts respectively (Dimitrios, Georgoulias, 2023 et al).

2.5 Network Crime

The network crime category is related to someone tampering with a network, with the aim to interrupt the sending of data. (Das & NayK, 2013. pp. 142-153).

2.5.1 DDoS and network attacks

When it comes to network crime, services such as hiring attacks related to network fall into that category. One example of a network crime is a DDoS (Distributed Denial of Service) attack. It is often carried out by using a botnet, which involves many computers overwhelming a server with traffic, with the aim to make the server unreachable to its clients. The attacks can make businesses lose money, customers and even their reputation (Fortinet, n.d). DDoS attacks can not only be executed by the use of programs, but also be executed in terms of DDoS-for-hire, which are services marketed on the dark web and obtained through transactions with virtual currencies. A buyer purchases an attack service to run these services in order to bring an internet-connected target down (FBI, n.d).

One example of a DDoS attack at scale is the attack aimed at the code platform GitHub in 2018. Attackers sent around 1.3Tbps of data to the website, which resulted in the platform not being accessible for about 5-10 minutes. GitHub is used by many companies working on their source code (TechCrunch, 2018).

Given previously mentioned research where the researchers examined 8 different marketplaces, it was found that services regarding DDoS (Distributed Denial of Service) attacks, spam and email attacks related to phishing were sold on the darknet, with an average price median at 8.9 EUR (Dimitrios, Georgoulias, 2023 et al).

2.6 Related Research

2.6.1 Overview of Cybercrimes on the Dark Web

Past studies have examined the dark web and found that dark web marketplaces have been formed, selling all kinds of services and illegal products. Examples of such marketplaces are Hydra and DarkMarket, which have been seized by law enforcement due to its illegal distribution of various materials. Further, another type of shop called "dark web shops" have emerged which are typically run by individuals and smaller organizations. Since the marketplaces are emerging drastically and that Tor's indexing is burdensome when analyzing several markets by multiple links, one choice could be of preference, says the authors.

Further research is encouraged by the authors to be proceeded with, preferably focused on more specific smaller shops run by not only large teams (Oosthoek, K et al. 2023). By focusing on one specific marketplace, we aim to gain an understanding of how the marketplaces and sellers within them operate. The aim is to also understand what they sell in a more thorough and comprehensive process than analyzing multiple markets that could be prone to difficulties of non-working links.

Forums and marketplaces, such as the "dark web shops" on the dark web have been found to contain information related to different types of services or spreading of criminal goods for potential customers. One study focused on classifying services, and the findings and the showed offerings labeled as a "cybercrime" and "not a cybercrime" respectively. The total entries were estimated to be around 109 000 entries, with a majority labeled as "not a cybercrime" which accounted for around 99 000 of the entries. Around 6000 were marked with "cybercrime" while the remainder of 4000 entries were marked with "can't say". Cybercrime was categorized as services related to hacking, and data related to software and accounts. The "not cybercrime" category involved the selling of drugs, counterfeits and weapons.

The authors of the previously mentioned study highlights that there was a lack of information regarding every item analyzed, and that the depth would have turned into complex clusters. The dataset would need to be expanded to improve the model (Sangher, K.S. et al, 2023). This research gap highlights the need for investigation of cybercrime services apparent on the dark web, which the first research question will outline in terms of examining the different types of cybercrime services. By analyzing not only types of services, we aim to give explanations of what the services include.

When it comes to malware offered on the dark web, there have been mentions of malwares and the statistics related to it. One study, with the aim to comparing surface web and dark web trading activity, examined 8 different underground forums and found that 50% of the posts were related to selling malware, along with more malware-related activity and lower prices offered on the dark web compared to the surface web (Bermudez-Villalva, A: Stringhini, G, 2021). One example of a program circulating on the dark web is Remote Desktop access programs, which are sold within the price range from around 2000 and 4000 USD. They can give access to a company’s internal systems and is therefore a raising concern for companies. The author urges organizations to look at the dark web for gaining knowledge regarding new emerging threats. (Kaspersky, 2022).

Similar to the findings of Bermudez-Villalva et al (2021), they provided an overview of cybercrimes, but did not include descriptions regarding offerings and what the sellers actually

sell, which could be crucial information to have in order to understand the risk of what is being sold. Therefore, the first research question will cover descriptions of offerings to give an informed but also could bring a preventative perspective in terms of identifying new emerging threats and services.

2.6.2 Trust Factors on Dark Web Marketplaces

Research shows that products as well as hacking tools are marketed using forums on the dark web. Paracha, A.A et al (2023) examine the CrimeBB-dataset and use an AI-framework titled INSPECT in order to analyze the influential profiles on the dark web with numerical rankings. The findings are that the markets on the dark web gives sellers a way of communicating the product's features, the ability to showcase the product and to invite discussion among potential buyers. Since the markets are solely online and are reached using anonymized tools, both the buyer and seller have to maintain trust. One method that has been used to maintain trust is by using escrow services, which acts as a middleman in order to prevent risks. To further give the buyers a sense of trust, review systems are also used (ibid.).

By employing content analysis in our study, we aim to get a deeper understanding of trust when it comes to seller and buyer. This way, we can cover narratives and terminologies used within product discussion forums that would have not been evaluated through the use of only quantitative methods.

For customers navigating the dark web, trust is of high priority as they fear their purchases could get tracked. Further research has used observational methods on the dark web for around 50 marketplaces, with the findings that more than 50% have incorporated reviews to establish trust. Brinck, J et al (2023) exemplify the Silk Road Marketplace as the first marketplace to incorporate customer reviews on their website and the researchers have found that earlier reviews can influence customers behavior, and give sellers a reputation on the market that is valuable for their business and to maintain trust (ibid.). In addition, these factors are not only as relevant as other aspects, such as reviews or product feedback on these marketplaces, but they also constitute a central part of a marketplace. The feedback on the marketplaces have shown to have had an impact on the long-term presence of suppliers and tends to gradually remove less reliable ones, which can strengthen credibility of the marketplace. Additionally, early revenue generation has shown to be an indicator of the supplier’s future success on the platform, a factor that could outweigh the significance of reputation (Christin, N. & Cuevas, A, n.d).

Proceeding with the trust aspect, the market for stolen data can be characterized by what is called an "uninformative cost condition," which means that buyers may have difficulty distinguishing between credible and non-credible sellers based on price. This is because the sellers' marketing strategies can be difficult to interpret. This creates a challenge for buyers trying to navigate the market and identify which sellers actually offer valuable and genuine stolen data (Lee, J.R, 2023). This statement is shown with the findings that markets can be present on the dark web one day with a good engaging outlook and marketing presence, and gone the next day, which can be troublesome for further research of these markets. Due to the anonymity of the dark web and its reliance on privacy, users are believed to be honest and interact with other people. Suggestions for further research is that particular marketplaces ought to be studied (Brinck, J et al. 2023).

Therefore in order to fill the gap that concerns the lack of investigating specific marketplaces, our aim is to dive into the methods and characteristics of one specific market to establish trust. What does the negotiation process look like, pricing discussion, other shared norms or elements that need to be respected for a successful purchase?

3. Methodology

This chapter presents an overview of the research strategy, choice of methods and steps included in data collection and analysis, to ultimately address the ethical considerations of the study.

3.1 Research Strategy

3.1.1 Observational Study

When it comes to our research strategy, we use an observational study in order to answer our research question concerning the types of services offered and the trust elements found. An observational study is aimed towards observing phenomena which allows us to witness events when they occur (Johannesson, Paul & Perjons, Erik, 2014). There are two types of observational research, the first one is "participant observation" that aims to investigate lifestyles and beliefs of certain social groups. The other type is "systematic observation" that focuses on the study of interaction by using statistical analysis and aims to produce consistent data between observers (Denscombe, 2014), which suits our research question for the analysis part. Our aim is to research how participants act and behave in this natural setting.

The benefit with observational studies is that they are conducted by observing participants in their natural circumstances without imposing any changes or intervention (Gilmartin-Thomas, J.F., Liew, D., Hopper, I. 2018). They also enable the collection of relevant and detailed data on a subject that defies quantitative measurement. By observing, it is possible to qualitatively assess many elements of performance and formulate theories about its quality (ATLAS, ti, n.d).

On the other hand, observational studies can have inherent limitations such as the potential of bias and factors. Because there is no intervention the outcome can be influenced by facts that cannot be measured or controlled, which could compromise the validity of the study's result. It is also claimed that these studies lack the ability to prove causality and to get a lower standard of evidence compared to others studies, for example experimental studies (Hess, A.S., Abd-Elsayed, A. 2019).

3.1.2 Alternative Research Strategy

We considered other research strategies such as a survey study, but this strategy was less suitable for our research. Survey studies can provide valuable insights into different opinions and attitudes among many participants, but are more suitable for data that is straightforward. A survey is typically not used for understanding complex situations and settings, which in our research this method would have been limited in regards to its use and understanding. It would also have been more difficult to investigate actual behavior with the use of a survey (Johannesson, Paul & Perjons, Erik. 2014).

Further, the research method "interview" in a survey study was considered since it could bring valuable information and experiences from sellers and buyers, which can cover complex topics through e.g semi-structured interviews or unstructured interviews. On the other hand, interviews could be seen as an unethical way of gathering information since it involves illegal

activity on underground platforms. There could also be a risk of potential bias from the interviewer steering the conversation in a planned direction. Additionally this research strategy would have taken a lot more time to execute (Johannesson, Paul & Perjons, Erik. 2014).

Since our intention was to observe the data rather than interfering with it when it came to our research question, the research method “experiment” was left out. The main purpose of using an experiment is used for understanding the cause and effect between one dependent and independent variable and can involve a hypothesis (Johannesson, Paul & Perjons, Erik. 2014). Since this was not our intention, we proceeded with observing events as they occur naturally.

3.2 Research Method

3.2.1 Mixed Method Approach

Our choice of research method is the mixed method approach, which typically involves combining several research approaches. In our study, we will combine both quantitative and qualitative research methods to gain a more comprehensive understanding of the DarkDock marketplace.

The mixed method approach offers the advantage of data triangulation, where multiple data sources are used to cross-validate findings. The qualitative element allows us to analyze descriptions of types of services and products and their trust-building mechanisms, while the quantitative element provides us with measured data when it comes to the number of services. This combination leads to better accuracy and ensures that the data is of high quality, since the findings of one method can be compared to another method’s findings. Additionally, a mixed method approach and its use of multiple methods enables a broader perspective of what is being studied, which suits an environment like the dark web.

On the other hand, the potential drawbacks of the mixed method approach is that using several methods is time consuming, and the researchers need to possess the skills when it comes to what each method consists of. Another drawback is that one finding may not always have to give support to the other finding (Denscombe, 2014). Despite this, by using quantitative data such as number of listings, and qualitative data such as descriptions of services, the mixed method approach is the most suitable in our study.

The research method can be summarized in the following steps:

1. The first step was to install the Tor Browser, in order to navigate via links known as onion links (The Tor Project, n.d).

2. Once Tor Browser was installed, we opened it and searched for the search engine "Ahmia" (Ahmia, n.d) in order to navigate through onion links on the dark web. Upon finding the Ahmia search engine, we entered the keyword “marketplace” and explored various websites returned in the search results.

3. When we found a working marketplace website related to cybercrimes and the categories: Access, Data and Network Crime, we looked for both categories and

subcategories on the page. The categories we looked for on the site included: malware, carding, databases, leaks, services and network attacks.

4. The chosen site named “DarkDock” contained all sorts of categories, and we picked out the categories presented in the sidebar of the site that were relevant when it came to cybercrime and that related to the scope of our study. This is shown in Table 1.

Category	**Number of listings**
Tutorials	2223
Digital - Documents	447
Civil Softwares	393
Digital - Hacks	374
Digital - Cards and Cvv	329
Database	280
Digital - Accounts	276
Digital - False Documents	139
Forgery	138
Digital - Application software	119
Network Services	93
Digital - System Software	56
Digital - Drop Bank	50
Digital - Security	50
Digital - Utilities	29
Digital - Exploit kit	27
Digital Forensics	18
Intelligence	17
Confidential Info	13
Leaked Documents	12
Private Security	10
0day	7

Digital - Software Forensics Tools	2
Racketeering	2

Table 1: Categories and their respective quantities of listings, chosen for data collection and analysis.

5. When investigating the categories, we saved each URL of every category along with the home-page in the txt-file named “categoriesAndLinks.txt”, located in the project where we have made a web scraper. In order to gather all the information, we used our developed web scraper written in Python along with other scripts in the project.

6. The steps 1-9 were followed, as stated in the GitHub project[1], which is available for further explanations of the steps and contents of files.

7. Further in the content analysis, we randomly selected 200 listings from our dataset using a script in the project.

8. At last, a discussion is provided based on the findings from the analysis.

3.2.2 Alternative Research Method

Another research method that was in consideration was ethnography. This method includes researchers taking part in social interactions and cultures within a longer period of time in order to understand the situations fully. The focus for the researcher is on attaching themselves to the group, rather than detaching themselves from them.
Ethnography could be used in this case to understand and identify different interactions and patterns among sellers and buyers during a time period, identifying shared values among participants.

However, the use of ethnography is time consuming since the researcher has to be fully present within the group. Additionally, the participation in these environments could be a risk for the researchers integrity, since it would involve selling and promoting illegal services. Another drawback of the method is that the websites on the dark web can change addresses in a short time span, therefore conducting an ethnographic research is more challenging as it demands that the researcher devotes time and is reliant on that the website is accessible (Denscombe, 2014).

Ultimately, the mixed method approach allows us to investigate a dark web marketplace without participating in it for a long time period. The use of a scraper allows us to collect information of both numerical and textual data without having to rely on the website’s availability.

[1] GitHub (2024) tor-onion-site-scraper. [GitHub repository] Available at: https://github.com/joelhagvall/tor-onion-site-scraper

3.3 Data Collection Method

3.3.1 Observational Studies

The data obtained from the observation are images, text and descriptions of what we see. This form of data is referred to as qualitative data (Johannesson, Paul et al, 2014).

3.3.2 Web Scraping

To retrieve information from the specific site we are to observe, we have developed a web scraper with the use of ChatGPT, a large language model from OpenAI, (OpenAI, ChatGPT 2024) for code suggestions, structure and improvement of the code and debugging. A web scraper involves using tools in order to retrieve data from a website, by collecting the website's fundamental HTML-code. A scraper can then extract the HTML-code into a CSV-file or a table for a categorized data collection (Fortinet, n.d). Examples of prompts used on ChatGPT during the development phase were: “How do we connect to a TOR-website through Python?”, “Can you make our script not appear as a bot?” and “Can you improve our code and make it more efficient?”. The usage of this tool is reflected in the discussion section.

The scraping project named “tor-onion-site-scraper” is available on GitHub and can be used to recreate this process, following the “README” file and setup guidelines. To retrieve the relevant information for our study, we have used several scraping scripts using Python, along with the packages and libraries: requests, urllib.parse, os, csv, bs4, pandas and matplotlib. In order for the scripts to work, the user has to install Tor on the machine. In summary, the project consists of scripts with the features to save HTML files, save CSV files and plot occurrences of keywords [2].

3.4 Data Analysis Method

3.4.1 Content Analysis

For the data analysis method, a content analysis will be applied to the data. Given our research questions that examine the type of cybercrime services offered, and the methods sellers use to establish trust with customers, the choice of content analysis as the data analysis method is suitable.

Content analysis is a method that quantifies the text’s content and has an advantage when it comes to reproducibility, given that the method is based on developing codes that are retrieved from information as it is stated, not as implied by the author. It also shows strength when it comes to revealing ways of communication from the text analyzed, which is interesting in this study. At the same time it is important to note that the analysis is at its best when analyzing less comprehensive information (Denscombe, 2014).

In our case, we can first quantify the number of listings of the marketplace, and other data related to numbers such as number of listings related to certain categories. Moreover, it is

[2] GitHub (2024) tor-onion-site-scraper. [GitHub repository] Available at: https://github.com/joelhagvall/tor-onion-site-scraper

convenient to use content analysis for the second research question as well, by developing themes of extracted text to find factors related to establishing trust.

The advantage of the quantitative element in content analysis is that data of large quantities can be analyzed, and the measurement can be validated by other researchers as well. Also, it is possible to visualize the quantified data with the help of charts, which helps in organizing the data obtained. It is also important to ensure that the data is of high quality and valid, otherwise it can be considered as weak data. Moreover, since the produced data can result in a data overload where the researchers can get overwhelmed by the different variables (Denscombe, 2014), we have limited the categories and keywords to only a few.

To conduct the content analysis, our initial steps are:

1. Selecting data from the listings, found in each CSV file, first “merged_data.csv” and then “random_listings.csv”.

2. Further, the text is to be separated into units which can include words or sentences. The units in the first CSV file for the first research question are the title and description of each listing, which includes words and sentences. The units in the second CSV file for the second research question are the description, refund tab and comments of each listing, also containing words and sentences.

3. Then, categories are to be produced that are relevant to the collected data and suitable for analysis. For the first table the first column is related to categories of offers along with their subcategories, keywords and frequencies. The second table’s categories are related to trust themes, keywords and frequencies.

4. Given the categories, units such as keywords or sentences have to be produced. We produced related keywords for every category in Table 2, and themes in Table 3. For the second research question, we duplicated the CSV-file and created “trustListings.csv” where we added columns that contained extracted relevant elements and the developed themes side-by-side with the actual data.

5. Given developed categories and codes, the keywords have to be counted of their frequency in the data.

6. At last, an analysis is to be made based on the code’s frequency and their possible connection to other codes present in the data collection.

The coding scheme below will act as a framework for conducting the content analysis for the first research question.

Offer Category	Subcategory	Keywords	Frequency

Table 2: Coding scheme for content analysis, with offer category, subcategory, keywords and its frequencies.

To answer the second research question, a qualitative analysis of each listing is applied using a coding scheme. The trust themes are developed by selecting text that is found in each listing, as shown in Table 3.

Trust Theme	Keywords	Frequency

Table 3: Coding scheme for qualitative analysis, with trust theme, keywords and frequency.

3.5 Ethical Considerations

The data for this study was collected from the previously mentioned link, which allows anyone to replicate the study provided the site remains accessible and is not seized. Our research was conducted in accordance with ethical standards and within legal boundaries, as is required for studies of this nature (Denscombe, 2014).

We also want to highlight the importance of ethical considerations in this process. The study was conducted only for research purposes. We declare that no purchases, activities or downloads of illegal content or any material from the Dark Web were involved. No harm was caused to market users or customers, and no names or personal information (for example phone number, e-mails) will be shown in this study. Furthermore, we do not want to encourage any criminal activity.

Regarding the data analysis phase, we ensured the integrity of our approach. The data analysis was not manipulated or conducted in a biased manner (Denscombe, 2014). We also did not do any sort of plagiarism of the work of other researchers.

4. Results

This chapter starts by presenting the marketplace and the themes developed for the content analysis, aiming to answer the research question. Starting with the first question, it focuses on the types of services offered by categorizing the offers found. The second question identifies trust-related factors which sellers use on the marketplace. Examples of listings are ultimately shown to highlight the themes identified.

4.1 Overview of Listings (RQ1)

In order to get the full picture of each listing's information and to see how it relates to each theme, we have narrowed the categories down that are found on DarkDock and defined by them, to better align with our research question. These categories are related to the offers and the examples mentioned earlier which fall under the offer categories: Access Crime, Data Crime and Network Crime. For the category "Digital", found in the sidebar of the marketplace, we have selected a fixed number of subcategories, since all subcategories found on the marketplace did not fall under our definitions. Upon selecting the relevant categories for our study and collecting every listing of every category and adding them together to a final dataset, we have applied a content analysis.

The analysis is based on the overall offer category indicating which type of service or product it is regarding. The main reason to search for every product under the categories is to find products that potentially have not been labeled with a subcategory on the site. Our developed offer categories are displayed in Table 4 below and are based on around 5000 listings found in "merged_data.csv" located in the project folder.

Offer Category	Subcategory	Keywords	Frequency	Total
Access Crime	Malware	Malware, trojan, ransomware, RAT, keylogger, spyware, worm	1896	8560
	Phishing	Phishing, social engineering, fraud	770	
	Hacking	Hacking, exploit, vulnerability, penetration	612	
	Course	Tutorial, guide, ebook	5282	
Data Crime	Leaks	Leak, data leak, breach, dump	306	7269
	Database	Database, SQL injection, MySQL, Oracle	383	
	Credit Card	Credit card, CVV, carding, carder, BIN	2799	
	Account	Account, login, username, email, credential, password, hash, cracking, brute force	3781	
Network Crime	DDoS	DDoS, botnet, stresser, booter	159	248
	Interception	interception, man in the middle, mitm, eavesdropping, dns spoofing, spoofing, cache poisoning, http session hijacking	35	
	Other	attacks, wi-fi cracking, rogue access points, firewall	54	

Table 4: Offer categories and their related subcategories, as well as keywords and their frequencies in the data set

The above listed subcategories are examples of services related to their subcategories. The offer categories are described as:

1. **Access Crime**: The category refers to activities related to unauthorized access when it comes to for example applications or systems. The subcategories include programs to give unauthorized access such as malware, guides and tools to obtain personal information which is known as phishing, services with the aim to give unauthorized access which is referred to as hacking, and courses.

2. **Data Crime**: This category is focused on offerings surrounding theft of data and the unauthorized access of it. Relevant subcategories are leaks, database, credit card and account, which all contain information of personal nature, whether it is credit card details or identity numbers of any kind.

3. **Network Crime**: The category refers to activities related to exploiting or targeting computer networks. It includes the subcategories such as DDoS, interception and network attacks. Programs such as DDoS use computers to perform targeted attacks to websites, and interception services hijack the communication between parts in order to obtain information.

Overall, the highest number of mentions of titles and descriptions of every chosen listing is connected to “Access Crime” with 8560 mentions, followed by “Data Crime” with 7269 mentions and “Network Crime” with 248 mentions. A deeper dive into the offer categories are analyzed further below.

4.1.1 Access Crime

Starting with the first offer category “Access Crime”, the most mentioned type of subcategory for the service found is “Course”, including tutorials and guides on how to commit frauds and making profit off of it. This is shown in Figure 1 below.

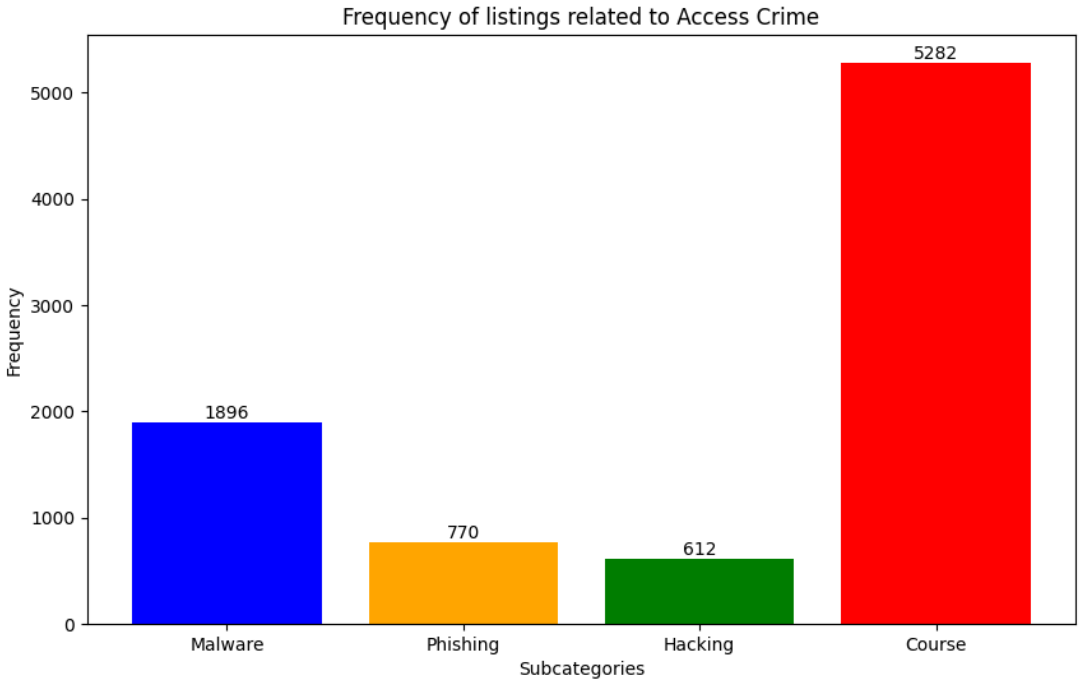

Figure 1. Frequency of listings related to Access Crime.

The frequency when it comes to listings related to access crime and the keywords related to the subcategory “Course” was found to be of 5282 mentions in the dataset and is the highest number compared to the other subcategories. Next is “Malware” with its keywords, which resulted in 1896 total mentions, along with “Phishing” which occurred 770 times and “Hacking” where the mentions were 612 times.

One example of an access crime is exemplified below in Figure 2. The offering shows a tutorial for fraud methods and a guide for especially beginners starting out with the methods. Examples of methods include carding and banking. It shows customer reviews and refund policies, together with delivery method and quantity, mimicking a typical e-commerce website.

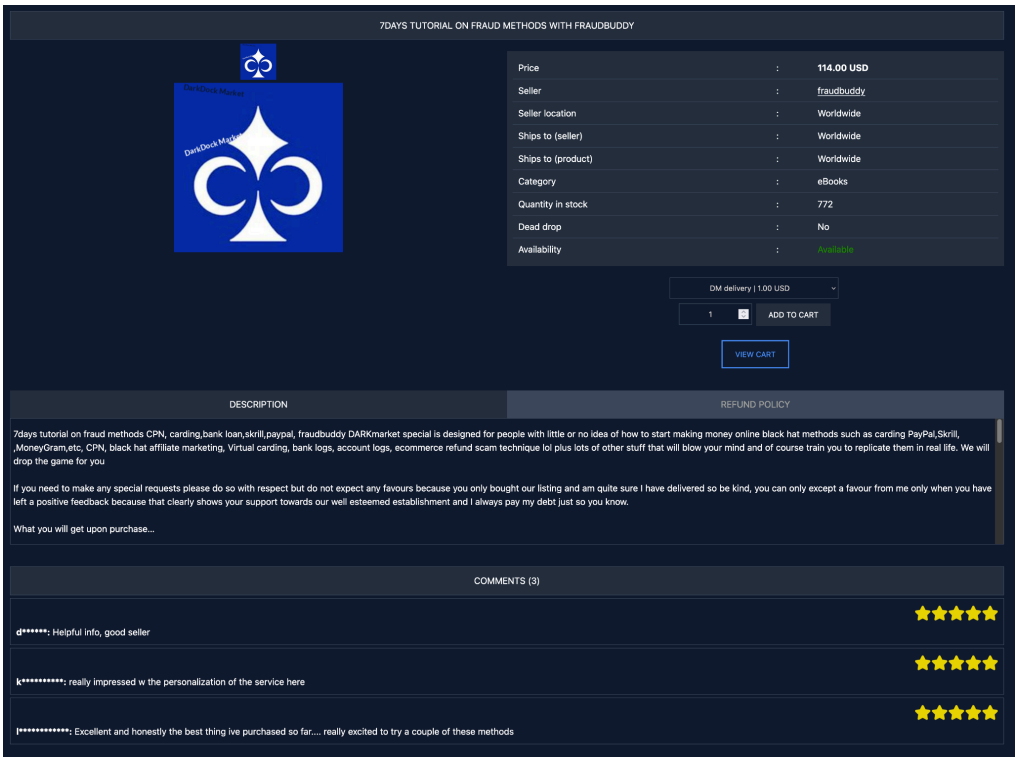

Figure 2. Listing related to subcategory "Course", with the title "7DAYS TUTORIAL ON FRAUD METHODS WITH FRAUDBUDDY".

4.1.2 Data Crime

Moving on to the second offer category "Data Crime", the most mentioned subcategory is "Account" and data related to accounts that concerns selling personal information. This is visualized in Figure 3 below.

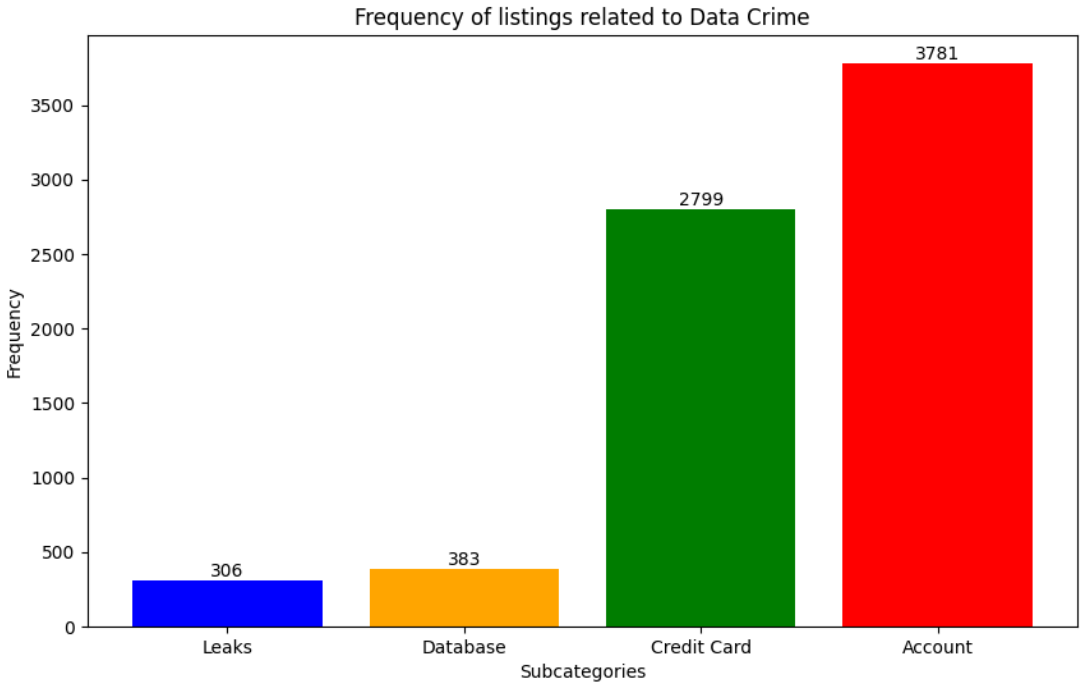

Figure 3. Frequency of listings related to Data Crime.

When it comes to the offer listings related to data crime and their keywords, the most occurred keywords identified were found in the "Account" subcategory with 3781 mentions. Further, the "Credit Card" subcategory and their keywords were found 2799 times, along with "Database" at 383 mentions and "Leaks" with 306 mentionings. "Database" and "Leaks" remain much lower compared to "Credit Card" and "Account" in mentionings.

An example of an offer related to data crime is shown in Figure 4. The offering provides a description of access to accounts registered for the crypto-website Binance, showcasing customer reviews and quantity in stock.

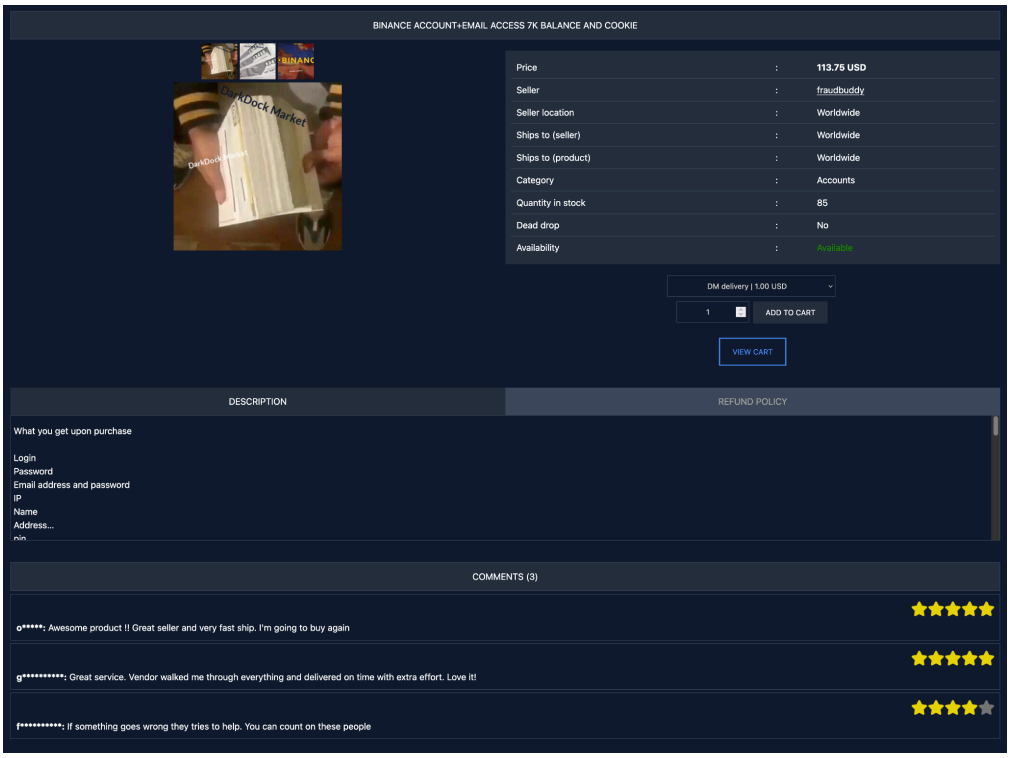

Figure 4. Listing related to subcategory "Account", with the title "BINANCE ACCOUNT+EMAIL ACCESS 7K BALANCE AND COOKIE".

4.1.3 Network Crime

At last, the last offer category "Network Crime" consists of "DDoS" as the most prevalent subcategory, and the marketplace offers kits of services making network attacks easily accessible for buyers. The findings are illustrated in Figure 5.

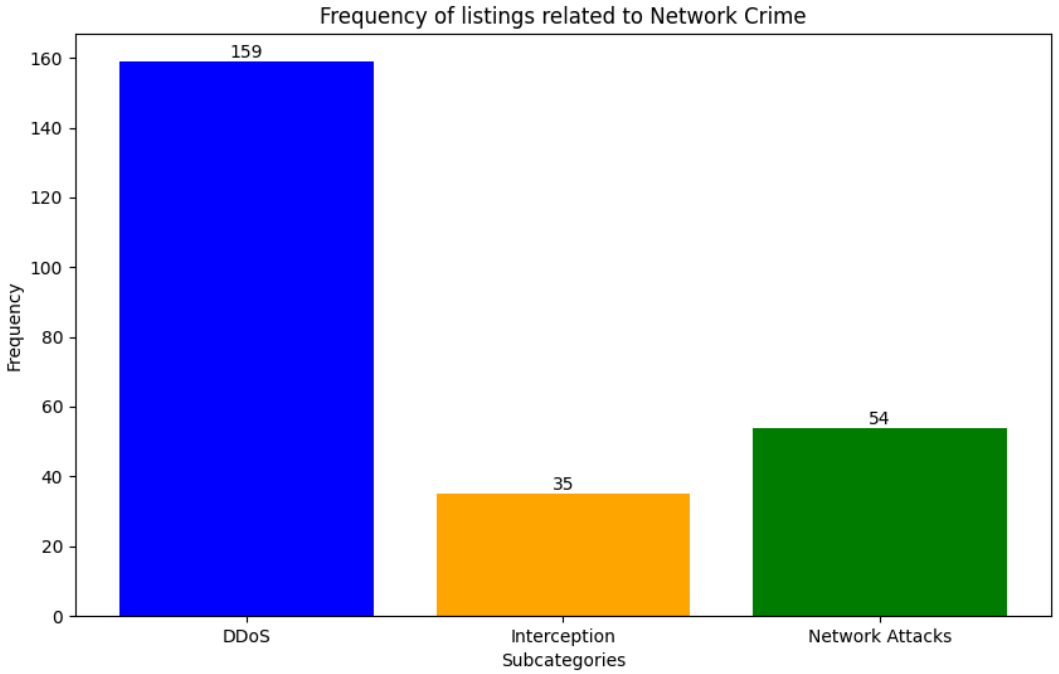

Figure 5. Frequency of listings related to Network Crime.

For listings related to network crime, the chart reveals that the keywords related to “DDoS” were the highest found with 159 mentions, followed by “Network Attacks” with 54 mentionings and “Interception” with 35 times where their keywords were mentioned.

An illustrated example of a DDoS-listing is shown in Figure 6. The offer provides a description of the tools provided to perform an attack including refund policies, together with customer reviews and inventory.

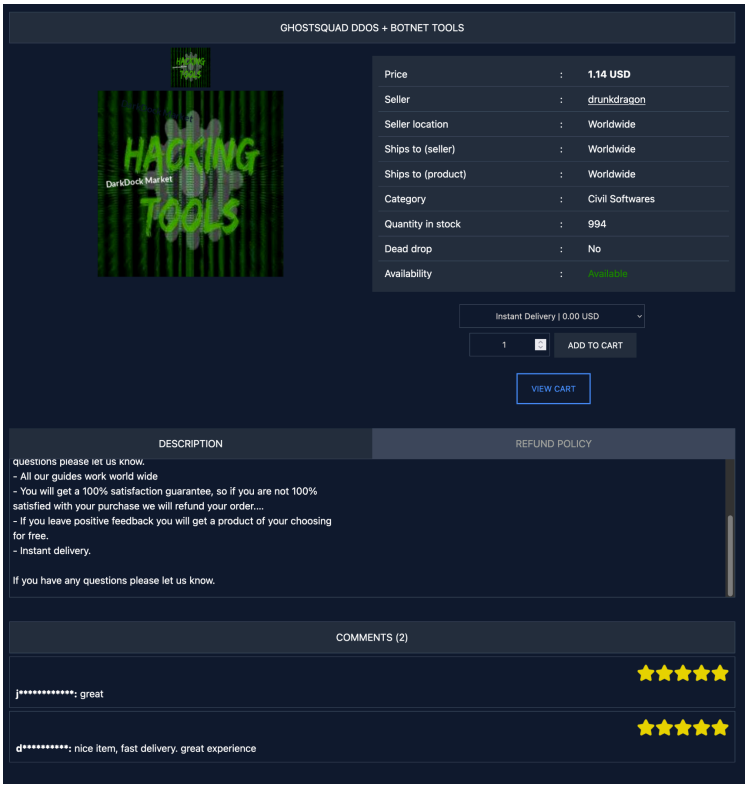

Figure 6. Example of listing related to subcategory "DDoS", with the title "GHOSTSQUAD DDOS + BOTNET TOOLS".

Ultimately, the data shows that courses are the most mentioned offer on the site based on our narrowed selection that consists of offers related to access, data and network crime. The high frequency in mentions of courses could potentially be explained by their ease of reproduction as a service, as well as accounts and DDoS attacks. One identified trend among the categories is that distributed information or content is found on the marketplace at a higher rate than for example software or services are. With this in mind, we further aim to answer what these differences are based upon in the second research question. What are the factors that make these listings successful when it comes to establishing trust between the seller and the buyer?

4.2 Trust Methods (RQ2)

This section presents the trust-related elements found based on 200 random listings on DarkDock by utilizing content analysis. This was achieved by first extracting information from the listings with the scraper, randomly selecting 200 listings and then developing five trust related-themes based on the information shown in each listing. The themes are developed as follows: **Customer Care and Reviews**, **Product and Service Quality**, **Security**, **Value and Assurance**, and **Ethics and Compliance**.

Our developed themes consist of keywords that are based on information of each listing found in the description, refund policy tab and under reviews. We first explain the themes together with the codes, to ultimately go through their frequencies. Identifying these elements could

potentially give an insight into how sellers use different techniques to sell their products and to establish trust towards their customers. Finally, we showcase some examples to exemplify the elements found.

4.2.1 Trust Themes

The five total trust themes and their respective codes are described below, ultimately showing an example of a listing connected to the themes and codes. Worth emphasizing is that the codes are based on information found on each listing that consist of claims and views stated by each seller.

1. **Customer Care and Reviews:**

Starting with the first theme, it highlights how sellers communicate with their customers specifying methods of communication. Customer care is an element in a marketplace where sellers show assistance and guidance towards customers, and this is shown in reviews where the buyers answer to this guidance and give their feedback. The developed codes are:

Assistance - Sellers show that they are open for questions or considerations that might arise from customers.
Appreciation from buyer - A buyer of the product has posted a positive review regarding the service and/or seller.
Friendly - Seller has a friendly tone in the description offering the service.
Criticism - The listing has received critique and negative feedback based on review of the listing.
Appreciation from seller - The seller shows appreciation towards their customers in the description.

2. **Product and Service Quality:**

Further to the second theme, “Product and Service Quality” covers how sellers market their products and services, by giving explanations and motivations in the description showcasing the offers. Product and Service Quality are important aspects in marketplaces since sellers' purpose is to sell products to customers and to make them satisfied, by ensuring inclusive descriptions and clarifications on delivery. Developed codes are as follows:

Delivery - Promotes fast deliveries and “instant delivery” towards customers for their services.
Quality - Description where the quality of the product or service is underscored from the seller.
Extensive Description - Text that includes detailed information of the product or service, including specifications and questions and answers.
Claims - Means that the seller is highlighting the product’s features, benefits, or performance to make it appear attractive.
Transparency - Description where the seller provides clear and accurate information about the product.
Authenticity - Promotes that the product being advertised is genuine and represents the product's true nature and quality.
Reliability - Highlights an assurance of performance and reliability from the seller.
Efficiency - Means that the seller promotes a handling of transactions, communication, and ensures a good experience for the buyer, according to them.

3. Security:

The third theme “Security” relates to protecting customer’s data, both when it comes to privacy for the individual and security on the site. Security and privacy are crucial factors for buyers to ensure that their personal data and transactions remain secure, and therefore is crucial to establish trust.

Security - This means that the seller ensures protection of the buyer’s personal and financial information.
Anonymity - Means that the buyer’s identity remains hidden, allowing them to purchase without revealing personal information.
Disclaimer - Means a statement that limits the seller’s accountability and clarifies conditions or limitations related to the product or service.

4. Value and Assurance:

The fourth theme “Value and Assurance” is focusing on what is included and marketed in the service that is offered to the customer. This could be guarantees, return policies and assurances regarding the service. All these factors impact a customer’s decision to make a purchase and to reduce risks.

Satisfaction Guarantee - This means an offer for refund or replacement if the sellers are not satisfied with their purchase, showing the seller’s commitment to customer satisfaction.
Rewards - This refers to incentives or benefits offered to buyers for making purchases, such as discounts or even free products.
Refund - Possibility to return the purchase, providing reassurance to the customer.
Value - Refers to the perceived benefits or the worth of a product or service.
Problem Guarantee - In case of a problem with the product or service, it will be refunded to the customer.
Guarantee - Ensures that buyers will receive certain benefits or assurances, such as product quality or performance.
Tutorials - Refers to educational or instructional content provided by the sellers to buyers how to use the products effectively.
Customization - Highlights the customer’s ability to customize their orders according to the description.
Credibility - Sellers portray themselves as a reliable and trustworthy seller, encouraging customers to make a purchase.
Assurance - Sellers assure customers they will receive the product or service and that any errors or wrongdoings will be acted upon.

5. Ethics and Compliance:

The last theme “Ethics and Compliance” highlights accountability and integrity when it comes to the selling of the service. This highlights the legal aspects and ethical standards in the offerings, which are important factors to establish trust. Developed codes are:

Responsibility - Code that indicates if a seller takes responsibility for the selling, ensuring meeting expectations of customers.

Ethical Considerations - Shows if the seller recognizes ethical implications with the service being sold.

To exemplify the developed themes, an example of the themes and codes is shown below. This listing shown in Figure 7, which sells a “Paypal receipt generator”, is chosen from our csv-file “trustListings.csv” of random listings, based on the amount of codes we have developed.

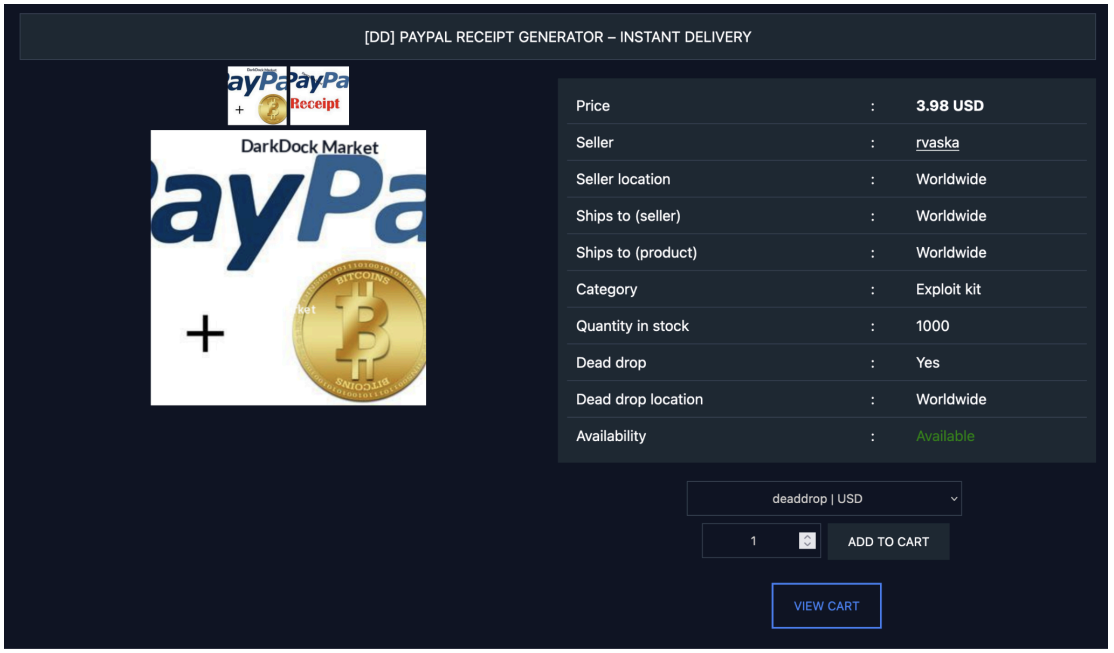

Figure 7. Example of listing related to the trust themes.

The codes and relevant sentence extracted from the description of the listing, shown in Figure 8, are stated as follows:

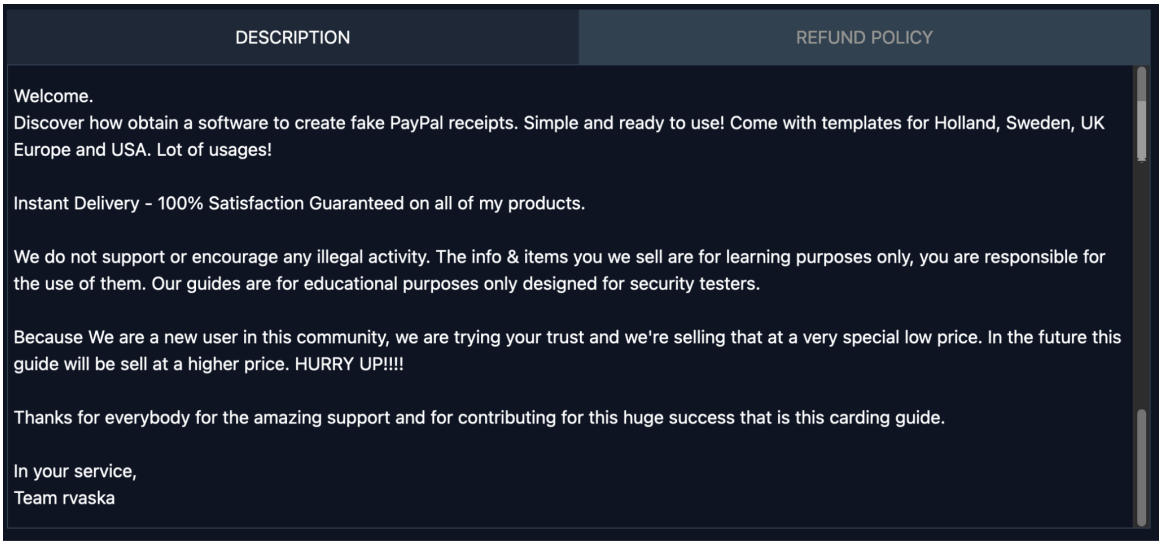

Figure 8. Listing’s description related to the trust themes.

Appreciation from seller (Theme 1: Customer Care and Reviews)*: "Thanks for everybody for the amazing support and for contributing for this huge success that is this carding guide."*

Delivery (Theme 2: Product and Service Quality)*:* "*Instant Delivery*"

Disclaimer (Theme 3: Security)*:* "*We do not support or encourage any illegal activity. The info & items you we sell are for learning purposes only, you are responsible for the use of them. Our guides are for educational purposes only designed for security testers.*"

Customization (Theme 4: Value and Assurance)*:* "*Come with templates for Holland, Sweden, UK, Europe and USA. Lot of usages!*"

Satisfaction Guarantee (Theme 4: Value and Assurance)*:* "*100% Satisfaction Guaranteed on all of my products.*"

Ethical Considerations (Theme 5: Ethics and Compliance)*: "We do not support or encourage any illegal activity"*

These sentences exemplify some of the codes found in each theme.

4.2.2 Frequency of Trust Themes

Having the codes and themes developed and exemplified above, we can now count the code occurrences and group them into the themes and then analyze the chart. The first plotting shows the total frequency for grouped codes for a certain trust-element. The second plotting shows the frequency for each code individually within the specific theme. This is shown in Figure 9 below.

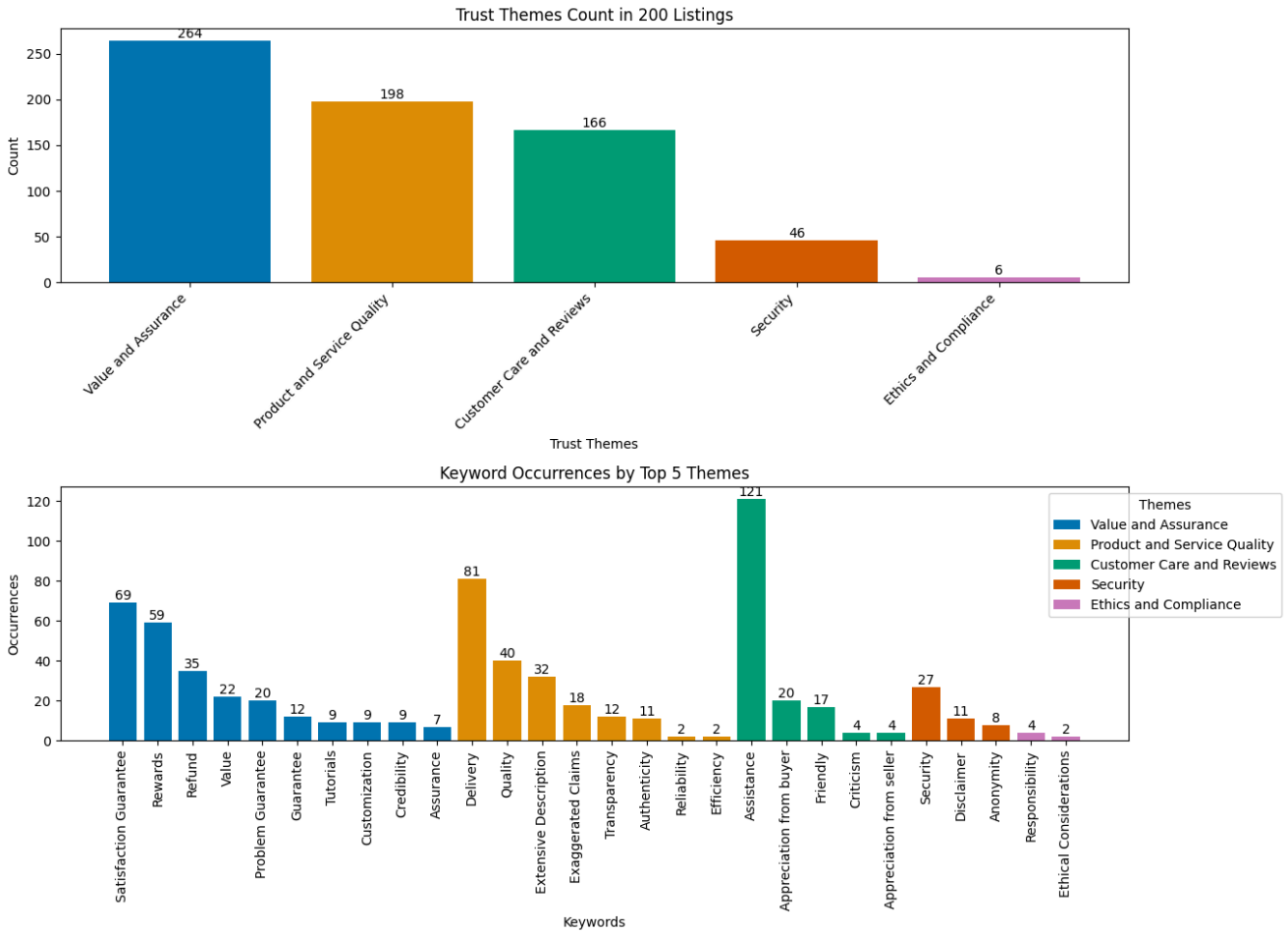

Figure 9. Frequency of Trust Themes.

Based on the chart, the following results have been conducted:

- **Value and Assurance:** The first theme focusing on listings emphasizing value of the product and assurance of the service for the customer is the most frequently mentioned of the developed themes, with “Satisfaction Guarantee” as the most frequently mentioned code. This suggests that offering guarantees for customers could be highly prioritized by the sellers as a trust-building mechanism. “Rewards”, which means offering incentives when buying the services is the second largest keyword occurrence in the trust theme. This proposes a customer centered approach when selling services and to build trust. In contrast, “Assurance” is the least frequently mentioned code in this theme and suggests that assuring a service could decrease the level of trust and customer confidence in contrast to the high frequency of offering guarantees and rewards.

- **Product and Service Quality:** The second most frequently mentioned theme surrounds the product and service offered along with its quality, which suggests that maintaining and upholding satisfaction from customers could potentially be of importance. The most mentioned code “Delivery” could propose that sellers promote their delivery time, which could build trust with customers. The code “Quality” is mentioned half the times as the previous code, suggesting that mentioning quality of

the service is something sellers could possibly do to ensure trust. In contrast, the least frequent codes “Reliability” and “Efficiency” are mentioned twice respectively, proposing that communicating how reliable a vendor is or how efficient they are, could indicate that it lacks in building trust with customers.

- **Customer Care and Reviews:** The third theme is centered towards customer feedback and care from sellers. The code “Assistance” shows a strong majority of the codes with 121 occurrences, suggesting that sellers prioritize assistance to customers to potentially establish trust and maintain communication. In comparison, the codes “Criticism” and “Appreciation from seller” are mentioned 4 times respectively and do not show as much of a significance in frequency as “Assistance” does.

- **Security:** Moving on to the fourth theme concerning security for customers as a trust-building mechanism, it shows a low amount of occurrences compared to the other trust themes. The most mentioned code “Security” could indicate that secure statements by sellers are used more than codes such as “Disclaimer” and “Anonymity”.

- **Ethics and Compliance:** Ultimately, the last and sixth theme involves sellers addressing ethical considerations, which focuses on the importance of taking responsibility in the marketplace. The theme in total is at 6 occurrences, with “Responsibility” being the highest mentioned code, along with “Ethical Considerations” counted to the lowest mentioned. This could suggest that addressing responsibility when it comes to the sellers is done more often than acknowledging the ethics involved with selling the service. The trust theme is not found in many of the listings, which could indicate that the elements surrounding ethics and compliance are on a low level and not prioritized by sellers to build trust with its clients.

Ultimately, given the results, both the themes and codes all share similarities and differences after analyzing the graph.

Similarities:
Starting with the first similarity, even though the theme “Value and Assurance” is the most frequently mentioned theme, the themes “Product and Service Quality” and “Customer Care and Reviews” all share a majority of the total frequency count. This could possibly indicate a potential explanation of the themes as trust mechanisms, as they occur the most. Providing assurance, product and service quality while enabling good customer care could be trust-themes to establish trust with customers.

Further, all 5 themes have one thing in common - they all have one code that is showing a majority of occurrences, though the 4 first themes all have one code that stands out compared to other codes in each theme. It is of importance to note that this gap shows a bigger frequency for assistance in comparison with other codes, but at the same time the theme consists of less codes developed in comparison to other themes. With more codes, the result could have been much higher and affect the overall results.

Differences:
Moving on to analyzing the differences between the themes, “Security” and “Ethics and Compliance” are showing a significant decrease in frequency for sellers expressing information regarding customers' security and ethical concerns. These two themes are nowhere near the 3 first themes, which could indicate that customers and sellers prioritize other trust-building elements than security. Further, after analyzing the codes in each theme, “Value and Assurance” and “Product and Service Quality” along with its codes are more evenly spread in comparison to the theme “Customer Care and Reviews”. In this theme, the code “Assistance” accounts for a majority of the codes and for the developed codes overall.

These findings show that assisting customers could potentially be considered to be the most vital trust-building element for sellers based on our analyzed data. Other highly mentioned elements emerged from the similarities and differences are found to be delivery, satisfaction guarantee and security. These codes are the most found in the listings analyzed, and could be relevant for sellers to take into consideration in order to establish trust with their customers on the marketplace. To exemplify how the sellers use different language and techniques, the earlier exemplified listings (Figure 2, 4, 6) consist of information related to the developed themes. In the listings, we can conclude that the sellers offer instant delivery and highlight customers' satisfaction by offering a guarantee, as well as assisting them if questions arise. Incentives are also offered in case of a positive review. The satisfaction from customers is shown by the reviews appreciating the product and experience.

5. Discussion

In this chapter we discuss the results and analysis in order to answer the research question and fill the stated research gap. At first we address what types of cybercrimes are found given frequency of listings and themes emerging from the listings, to later discuss what methods these offers have in order to establish trust given our developed themes. The findings are compared to existing research, highlighting the differences and similarities found when it comes to the developed themes and research.

5.1 Overview of Cybercrime Offers and their Trust Indicators on DarkDock

5.1.1 Types of Cybercrimes

Given the data on the offer categories, we can conclude that the offer category Access Crime is in higher popularity of the listings selected, followed by Data Crime and Network Crime.

Out of all offer categories, it is suggested that listings related to unauthorized access and spreading of courses were the most mentioned on the marketplace. The “Access Crime” category advocated for 8560 mentionings which was a majority of all other offers analyzed, with subcategory “Courses” being mentioned 5282 times. This can be contrasted to the findings by Bermudez-Villalva and Stringhini’s research (2021) where they did not find any offerings related to courses. Instead they found 50% of the listings in eight forums to be related to selling malware. In our case, malware is the second most mentioned subcategory in the offer category “Access Crime”. Even though the authors examined eight forums instead of one single marketplace, this shows that malware is still offered in high frequency. The high frequency could potentially be motivated by the assumption that courses are easier to reproduce than malware. Courses could also be more beneficial and attractive to customers since committing fraud might not always be an easy path, and direction could be needed to perform the crime in a “successful” way without being caught.

Further, listings related to selling account information were the most popular when it came to the second most popular offer category “Data Crime”. The prevalence of “Data Crime” was at 7269 mentions in total, with subcategory “Account” accounting for 3781 mentionings. This finding differs from previous research where Sangher, et al (2023) found accounts to be in their less prevalent category named “Cybercrime”. On the other hand, a different methodology was used based on bigger datasets than ours, which could have an effect on the overall results. Accounts and credit cards being more prevalent in the data could be explained by confidential information, giving access to financial assets or other forms of additional value simply by knowing the user credentials.

Additionally, listings related to subcategory “DDoS” were the most popular when it came to the least popular offer category “Network Crime”. “DDoS” had 159 mentions, along with “Network Attacks” with 54 mentionings and “Interception” with 35 mentions. The total frequency of “Network Crime” was estimated at 248 mentionings. This total, compared to the

other offer categories, is indicating a lower frequency for services connected to network crime but still being the most popular within this category. One possible reason for this could be the low prices for these services. Previous research examined eight different marketplaces and found that services for DDoS attacks, spam and email attacks related to phishing were sold on the dark web at an average price median at 8.9 EUR (Dimitrios, Georgoulias, 2023 et al). In comparison with our study, the price for our selected listing example was 1,14 USD, which is significantly lower than their average median price. Despite the comparison being based on median values from different offerings, this indicates that the prices are low and accessible. This affordability could potentially allow more customers to purchase services that can disrupt networks.

Overall, the types of cybercrime offers found on DarkDock are related to activities selling access crimes including courses, data crimes involving account information and network crimes such as DDoS tools. These services are suggested to be appealing and more available, given courses. Also of high value, especially with account information, and ultimately accessible, given affordable DDoS tools.

5.1.2 Trust Establishing Methods

Based on the content analysis from our selected listings, we can reason that the trust-building methods of offers are: the highly prioritized assistance with customers, ensuring delivery time and offering guarantees of satisfaction. Other aspects such as, offering rewards and promoting the service's quality in the description could also be significant when it comes to building trust with buyers on the marketplace.

The most occurring theme named "**Value and Assurance**" highlights its suggested role in ensuring trust. Methods such as refunds, satisfaction guarantees, and customizations could enhance trustworthiness. The findings suggest that dark web markets provide sellers with a platform to communicate product features, showcase their products, and engage with potential buyers (Paracha, A.A, 2023). However, these measures alone do not ensure trust. Each offer is unique, and merely stating these assurances in a product description does not guarantee their fulfillment, especially in the context of dark web marketplaces where both the seller and customer are anonymous.

Regarding the theme "**Product and Service Quality**," providing detailed explanations and motivations in product descriptions could build trust. Transparency through extensive descriptions and delivery information aims to create more appealing deals, supported by reviews, which have been shown to impact the long-term presence of suppliers (Christin, N. & Cuevas, A., n.d). However, the effectiveness of these measures varies with the type of product. For example, delivering a copied or illegally obtained tutorial or guide is simpler than developing malware that works for every customer in regards to customisation. This makes it challenging to measure and standardize quality. Ultimately, as with "Value and Assurance," product and service quality descriptions do not guarantee actual performance or satisfaction.

Further, the third theme "**Customer Care and Reviews**" shows that a few reviews are available for a couple of the listings analyzed. The amount of reviews for the listings selected is small, although the site offers customers the functionality to create reviews for every listing. In comparison, Brinck, J et al (2023) found that more than 50% of the 50 marketplaces analyzed have incorporated reviews. This puts DarkDock as one of the marketplaces having reviews visible among its customers to potentially maintain trust and uphold the reputation of sellers. On the other hand, comments and reviews can potentially be faked and generated by bots. As proposed by Brinck, J et al (2023) and Paracha, A.A et al (2023), comments and reviews are found to give sellers a sense of credibility and to raise trust among customers, even influence their behaviors. One noteworthy concern is the fake comments that appear on clear web sites like Amazon, do in fact appear on the dark web. This problematizes the idea of reviews being considered the important trust factor.

The fourth theme "**Security**" indicates that the leading code "security" is the most occurring out of all codes within the theme. The "security" code contains quotes from the listings related to mentions of "escrow" services, which Paracha, A.A et al (2023) explains is a middleman to prevent risks and to give customers a sense of trust (ibid). Navigating the dark web when it comes to trust is challenging and it is important to note that the dark web offers less ways of ensuring security for customers, as it lacks integration with for example reputable payment providers and "secure e-commerce" badges that are shown in clearnet marketplaces. The escrow service in this case could be considered a "payment provider" that could be trusted, especially since Brinck, J et al (2023) explains that users are considered to be honest and interact with other people on the dark web due to its nature of privacy. At the same time, escrow services on sites like DarkDock have a limitation of details regarding the payment process and the organizations behind them. This makes escrow services a trust factor with some concerns.

Concluding, the developed themes provide an overview of how an emphasis on our codes "assistance", "quality", "customer care" and "security" is suggested in order to establish trust between sellers and customers. These codes and themes, ranging from e.g offering guidance and help towards customers, providing extensive descriptions and using escrow services, could contribute to an understanding of services and trust-establishing methods on dark web marketplaces. However, trust on the marketplace is a challenge given limited information on payment processes, authenticity of products and potential fake reviews.

6. Conclusion

The final chapter covers a brief summary of our results and findings, while answering the research question. We also address the limitations of the study and how the findings can contribute to future research.

In summary, our study puts dark web marketplaces in the spotlight along with “Courses” in the category “Access Crime” as the most mentioned offer found. For the category “Data Crime” was “Account” the most popular one; and for the category “Network Crime” was “DDoS” the most in frequency. The offerings portrayed by the sellers to establish trust with customers included offering assistance, informing on delivery time and ensuring satisfaction guarantees.

6.1 Consequences

These findings have broader implications for society as a whole with its easy accessibility, as the site provides criminals with easy access to committing cybercrimes. This underscores the importance of law enforcement monitoring listings to prevent cybercrimes, as well as investigating dark web marketplaces further.

By monitoring the listings and the use of certain trust-building language and methods. Law enforcement can recognize trends related to offerings and the seller’s and buyer’s objectives on the marketplace. For example, trends in offering of courses or DDoS network tools could potentially indicate threats that should be acted upon.

This monitoring helps predict and also prevent attacks since these can be carried out by inexperienced actors acquiring advanced tools, e.g finding a security vulnerability before an attack has occurred. It is important to understand the vulnerabilities found and to develop mitigations in forms of updates and patches to prevent attacks.

This knowledge provides security specialists to develop practices and resilient security measures for the protection of e.g sensitive data, information and systems. By understanding these dynamics of dark web marketplaces and enhancing awareness, involved users can better prepare for possible threats and to contribute to a safer digital environment.

6.2 Limitations

Future improvements to methodology could include that the code related to the scraping could be enhanced to finding duplicates and keeping one of them in the dataset, since the same listing can be found on multiple categories. This could affect the results. Further UI-improvements such as an automated script could be made for the project since it consists of several files that requires following a procedure step-by-step.

Additionally, investigating all listings given all categories apparent on the site could be beneficial in order to not lose any important data, given that the listings are categorized after being collected. Some listings on the site could be unlabeled of a category that may have not been included in this study due to our choosing of specific categories apparent on the site, and we can not guarantee that they have categorized their listings correctly.

6.3 Usage of AI-tools

During this process, we have used AI-tools for writing and debugging code and improving written text. It is important to note that by using AI-tools for writing and improving code, errors and mistakes can be made that could make the code less efficient and accurate when it comes to extracting data. Therefore, further development and analysis of the scraper is advised for studies built upon the project. Additionally, using AI-tools for writing text and correcting language could also come with errors, and may be used as a tool.

Furthermore, we have used AI-tools for grammatical purposes, such as suggesting synonyms, formulations of sentences and brainstorming new ideas and perspectives. While the use of AI-tools might be helpful, the information generated should not be entirely reliant on. This information should be carefully considered combined with critical thinking, as AI could generate inaccurate suggestions.

6.4 Future Research

For future research, investigating more marketplaces in depth is considerable since there is a lack of analysis on more specific dark web marketplaces. The findings of the rise of courses offered was rather unexpected, as malware is often described to be the most offered among earlier studies. These findings could raise interesting questions for future research such as: What makes courses so prevalent on the dark web marketplaces? and; What type of courses sell on dark web marketplaces?

7. References

Accenture (2022), Popularity spikes for info stealer malware on the dark web. Available at: https://www.accenture.com/us-en/blogs/security/information-stealer-malware-on-dark-web [2024-03].

Ahmia (n.d) Available at: https://ahmia.fi/ [2024-02].

ATLAS.ti. (n.d.). What is observational research? Available at: https://atlasti.com/guides/qualitative-research-guide-part-1/observational-research [Accessed 2024-04].

Bank of Scotland (n.d.). Dark web threats – and what to do about them. Available at: https://business.bankofscotland.co.uk/business-resource-centre/insights-and-ideas/dark-web-threats.html [2024-03].

Bermudez-Villalva, A. and Stringhini, G. (2021) 'The shady economy: Understanding the difference in trading activity from underground forums in different layers of the web', *2021 APWG Symposium on Electronic Crime Research (eCrime), Electronic Crime Research (eCrime), 2021 APWG Symposium on,* pp. 1–10. doi:10.1109/eCrime54498.2021.9738751. [2024 -03].

BleepingComputer. (n.d.). The dark web is getting darker - Ransomware thrives on illegal markets. [online] Available at: https://www.bleepingcomputer.com/news/security/the-dark-web-is-getting-darker-ransomware-thrives-on-illegal-markets/. [2024-03].

Brinck, J., Nodeland, B. and Belshaw, S. (2023) 'The "Yelp-Ification" of the dark web: An exploration of the use of consumer feedback in dark web markets', *Journal of Contemporary Criminal Justice*, 39(2), pp. 185–200. Available at: https://research-ebsco-com.ezp.sub.su.se/linkprocessor/plink?id=d64f24a2-1d46-3de8-a527-2666f43335d9 [2024-04].

Brookshear, J. Glenn & Brylow, Dennis (2020). Computer science: an overview. 13th edition. NY, NY: Pearson, pp.242 [2024-02].

Cloudflare, What is a data breach? https://www.cloudflare.com/learning/security/what-is-a-data-breach/ [2024-02].

Cuevas, A. and Christin, N. (n.d.). Does online anonymous market vendor reputation matter? [online] Available at: https://www.usenix.org/system/files/sec24summer-prepub-871-cuevas.pdf [2024-05].

Cybersecurity & Infrastructure Security Agency (2021). Avoiding social engineering and phishing attacks | CISA. [online] Cybersecurity and Infrastructure Security Agency CISA. Available at: https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks [2024-02]

DarkDock. (n.d.). Available at: http:///oirolrkrppy6sei6x6bvkkdolc4cjqzqfhxisfzu6exqblahwrrvktyd.onion/faq [2024-03].

Das, S. and Nayak, T. (2013). Impact of cyber crime: issues and challenges. *International Journal of Engineering Sciences & Emerging Technologies*, 6(2), pp.142–153. Available at: https://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf. [2024-02]

Denscombe, Martyn (2014). The good research guide: for small-scale social research projects. 5th ed. Maidenhead, England: McGraw-Hill/Open University Press [2024-02]

Dimitrios Georgoulias, Ricardo Yaben, & Emmanouil Vasilomanolakis. (2023). Cheaper than you thought? A dive into the darkweb market of cyber-crime products. *ARES*, 1–10. https://doi-org.ezp.sub.su.se/10.1145/3600160.3605012 [2024-02]

Dilipraj, E., 2014. Terror in the deep and dark web. *Air Power Journal*, 9(3), pp.121-140. [2024-02]

Ellerbeck, S. (2022). Nearly half of organizations are being hit by economic crime, with cybercrime the gravest threat. What can they do about it? World Economic Forum. Available at: https://www.weforum.org/agenda/2022/07/fraud-cybercrime-financial-business/. [2024-02]

Federal Bureau of Investigation (n.d), The FBI and international law enforcement partners intensify efforts to combat illegal DDoS attacks https://www.fbi.gov/contact-us/field-offices/anchorage/fbi-intensify-efforts-to-combat-illegal-ddos-attacks [2024-03]

Finklea, K. (2017) Dark web. *Congressional research service*, Washington DC, 10 March 2017, 1-19. https://fas.org/sgp/crs/misc/R44101.pdf [2024-03]

Forbes (2024), Warning as 26 billion records leak: Dropbox, LinkedIn, Twitter Named. https://www.forbes.com/sites/daveywinder/2024/01/23/massive-26-billion-record-leak-dropbox-linkedin-twitterx-all-named/ [2024-03]

Fortinet (n.d). What is DDOS attack? https://www.fortinet.com/resources/cyberglossary/ddos-attack [2024-03]

Fortinet. What is web scraping? How do scrapers work? https://www.fortinet.com/uk/resources/cyberglossary/web-scraping [2024-03]

Geti2p.net. (2019). Intro - I2P. Available at: https://geti2p.net/en/about/intro. [2024-03]

Gilmartin-Thomas, J.F., Liew, D. and Hopper, I. (2018). Observational studies and their utility for practice. *Australian Prescriber,* 41(3), pp.82–85. doi:https://doi.org/10.18773/austprescr.2018.017. [2024-04]

GitHub. (2024) tor-onion-site-scraper. [GitHub repository] Available at: https://github.com/joelhagvall/tor-onion-site-scraper [2024-04]

Griffiths, C. (2023). The latest 2022 cyber crime statistics (updated December 2022) | AAG IT Support. aag-it.com. Available at: https://aag-it.com/the-latest-cyber-crime-statistics/. [2024-04]

Hess, A.S. and Abd-Elsayed, A. (2019). Observational studies: uses and limitations. Pain, pp.123–125. doi:https://doi.org/10.1007/978-3-319-99124-5_31. [2024-04]

Ho Woon Chung et al. (2018) 'Malware trends on "Darknet" crypto-markets: Research review', *SSRN Electronic Journal*. Available at: https://research-ebsco-com.ezp.sub.su.se/linkprocessor/plink?id=65b84543-5fc4-3b5b-b783-ded4e4a99cfe [2024-02]

Hyphanet (n.d) Available at: https://www.hyphanet.org/ [2024-04].

IBM, Cost of a Data Breach Report 2023 https://www.ibm.com/reports/data-breach
Jin, P. et al. (2024) 'Forensic investigation of the dark web on the Tor network: pathway toward the surface web', *International Journal of Information Security*, 23(1), pp. 331–346. doi:10.1007/s10207-023-00745-4. [2024-03]

Johannesson, Paul & Perjons, Erik (2014). An introduction to design science. Cham: Springer International Publishing, pp.59 [2024-03]

Kaspersky, How data breaches happen & how to prevent data leaks https://www.kaspersky.com/resource-center/definitions/data-breach [2024-03]

Kaspersky (2022). Cybercriminals sell access to companies via the dark web from $2000. [online] Available at: https://www.kaspersky.com/about/press-releases/2022_cybercriminals-sell-access-to-companies-via-the-dark-web-from-2000. [2024-03]

Karo-Karo, G.F.M., Harumnanda, M.S.A. and Lim, C. (2023) 'Investigating multiple malware as a service (MaaS): analysis and prevention techniques', *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs), Cryptography, Informatics, and Cybersecurity (ICoCICs), 2023 IEEE International Conference on*, pp. 270–274. doi:10.1109/ICoCICs58778.2023.10277515. [2024-03]

Lee, J.R. (2023). Understanding markers of trust within the online stolen data market: An examination of vendors' signaling behaviors relative to product price point. *Criminology & public policy*,22(4), pp.665–693. doi:https://doi.org/10.1111/1745-9133.12651. [2024-03]

Malwarebytes, What is malware? https://www.malwarebytes.com/malware [2024-02]

Manky, D. (2013) 'Cybercrime as a service: a very modern business', *Computer Fraud & Security*, 2013(6), pp. 9–13. doi:10.1016/S1361-3723(13)70053-8. [2024-03]

National Crime Agency (2024), International investigation disrupts the world's most harmful cyber crime group.
https://nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group [2024-03]

National Institute of Justice, Taking on the dark web: law enforcement experts ID investigative needs https://nij.ojp.gov/topics/articles/taking-dark-web-law-enforcement-experts-id-investigative-needs [2024-03]

Oosthoek, K., Van Staalduinen, M. and Smaragdakis, G. (2023) 'Quantifying dark web shops' illicit revenue', *IEEE Access*, Access, IEEE, 11, pp. 4794–4808. doi:10.1109/ACCESS.2023.3235409. [2024-03]

OpenAI (2024). ChatGPT. https://chatgpt.com/ [2024-03]

Ozkaya, E & Islam, MDR 2019, Inside the dark web. *CRC Press*, Boca Raton, FL. https://doi.org/10.1201/9780367260453 [2024-03]

Paracha, A.A., Arshad, J. and Khan, M.M. (2023) 'S.U.S. You're SUS!—Identifying influencer hackers on dark web social networks', *Computers & Electrical Engineering*, 107, p. N.PAG. doi:10.1016/j.compeleceng.2023.108627. [2024-04]

Prabha, C. and Mittal, A. (2023) 'Dark Web: A Review on the deeper side of the Web', *2022 OPJU International Technology Conference on Emerging Technologies for Sustainable Development (OTCON), Emerging Technologies for Sustainable Development (OTCON), 2022 OPJU International Technology Conference on*, pp. 1–6. doi:10.1109/OTCON56053.2023.10113989 . [2024-04]

Sangher, K.S. et al. (2023) 'Towards safe cyber practices: Developing a proactive cyber-threat intelligence system for dark web forum content by identifying cybercrimes', *Information (Switzerland)*, 14(6). doi:10.3390/info14060349. [2024-04]

TechCrunch (2018), The world's largest DDoS attack took GitHub offline for fewer than 10 minutes. https://techcrunch.com/2018/03/02/the-worlds-largest-ddos-attack-took-github-offline-for-less-than-tens-minutes/ [2024-03]

The Evolution of Cybercrime: Why the dark web is supercharging the threat landscape and how to fight back (2022), An HP Wolf Security Report. Available at: https://threatresearch.ext.hp.com/evolution-of-cybercrime-report/ [2024-03]

The Tor Project (nd). The Tor Project | Privacy & freedom online. [online] Torproject.org. Available at: https://www.torproject.org/about/history. [2024-02]

www.britannica.com. (n.d.). Tor | Browser, Dark Web, & Function | Britannica. Available at: https://www.britannica.com/technology/Tor-encryption-network. [2024-02]

Wood, Kimberley (2023). The georgetown environmental law review, cybersecurity policy responses to the colonial pipeline ransomware attack. Available at: https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack/ [2024-03]

Zeronet.io. (2019). ZeroNet: Decentralized websites using Bitcoin crypto and the BitTorrent network. [online] Available at: https://zeronet.io/. [2024-04]