University of Kent

Kent Academic Repository

Wang, Yichao, Arief, Budi and Hernandez-Castro, Julio C. (2024) *Analysis of Security Mechanisms of Dark Web Markets*. In: EICC '24: Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference. . pp. 120-127. ACM ISBN 979-8-4007-1651-5.

Downloaded from

https://kar.kent.ac.uk/105237/ The University of Kent's Academic Repository KAR

The version of record is available from

https://doi.org/10.1145/3655693.3655700

This document version

Publisher pdf

DOI for this version

Licence for this version

CC BY (Attribution)

Additional information

Versions of research works

Versions of Record

If this version is the version of record, it is the same as the published version available on the publisher's web site. Cite as the published version.

Author Accepted Manuscripts

If this document is identified as the Author Accepted Manuscript it is the version after peer review but before type setting, copy editing or publisher branding. Cite as Surname, Initial. (Year) 'Title of article'. To be published in ***Title of Journal*** , Volume and issue numbers [peer-reviewed accepted version]. Available at: DOI or URL (Accessed: date).

Enquiries

If you have questions about this document contact ResearchSupport@kent.ac.uk. Please include the URL of the record in KAR. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies).

Analysis of Security Mechanisms of Dark Web Markets

Yichao Wang
University of Kent
Canterbury, UK
yw300@kent.ac.uk

Budi Arief
University of Kent
Canterbury, UK
b.arief@kent.ac.uk

Julio Hernandez-Castro
Universidad Politécnica de Madrid
Madrid, Spain
jc.hernandez.castro@upm.es

ABSTRACT

As the name implies, the dark web market – also commonly known as the anonymous market – has put measures for protecting the privacy of its users as a key priority. With the rapid growth of the dark web market, competition between markets has become more intense. With this, malicious attacks between competitors – for instance, aimed at reducing the availability of competitors' services – have also become more common. These attacks not only affect the services' availability and accessibility, but they may also cause some personal and private information being leaked. As such, it is understandable that dark web markets may implement security mechanisms to protect themselves and their users. Although the literature has analysed and described dark web markets from multiple perspectives, there is still a gap in understanding the security mechanisms implemented by different dark web markets. Furthermore, data collection – which is often considered a common challenge in this research area – may be hindered by these security mechanisms. Therefore, the study presented in this paper aims to investigate the security mechanisms of various dark web markets systematically, in order to shed a better light on their operation. To achieve this aim, we performed data collection and experiments in twelve existing dark web markets, using them as information sources. Although data collection practices slightly vary for each market, the data was collected over a span of four months between May and August 2023. We found there are two main groups of security mechanisms used in dark web markets: web security and account security. Web security contains accessibility, waiting queue, anti-phishing, CAPTCHAs, secret phrase, warrant canary, bug bounty, rate limiting and a toolset. Account security contains username requirement, password & PIN requirement, mnemonic, multi-factor authentication (MFA) and account kill-switch. In conclusion, different types of security mechanisms used by the market may reflect the operator's business philosophy, which in turn may affect the way the market operates. The results of this study can help the academic and security research communities to understand the operation and evolution of the dark web markets better, which in turn can be used to combat crimes facilitated by these markets more effectively. Additionally, findings from this study may provide clues on how to improve the efficiency of data collection in this environment.

This work is licensed under a Creative Commons Attribution International 4.0 License.

EICC 2024, June 05–06, 2024, Xanthi, Greece
© 2024 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-1651-5/24/06
https://doi.org/10.1145/3655693.3655700

CCS CONCEPTS

• **Security and privacy** → **Social aspects of security and privacy**; *Web application security*.

KEYWORDS

dark web market, security mechanism, web security, account security, market operation

ACM Reference Format:
Yichao Wang, Budi Arief, and Julio Hernandez-Castro. 2024. Analysis of Security Mechanisms of Dark Web Markets. In *European Interdisciplinary Cybersecurity Conference (EICC 2024), June 05–06, 2024, Xanthi, Greece.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3655693.3655700

1 INTRODUCTION

Over the past decade, we have seen rapid growth in criminal activity on the dark web. As mentioned in the latest *Internet Organised Crime Threat Assessment (IOCTA) 2023* report, dark web markets have been identified as a venue often used for advertising and selling illicit services and products [9]. From the famous *Silk Road* dark web market to the recently shut down *Hydra Market* [19], from suspected of selling firearm to child abuse materials [6, 17, 22], the development of dark web markets is becoming more and more destructive to society over time. At the same time, how to mitigate the negative impact on society has become a serious challenge for scholars and law enforcement agencies. Recently, European law enforcement agencies conducted an operation codenamed *SpecTor*, which resulted in the closure and arrest of the suspected of operators of the *Monopoly Market*, a very successful and good-reputation dark web market at the time [8].

Nevertheless, the operation of the dark web market is not immutable. In a narrow sense, the dark web market usually refers to the marketplace on the Tor network. In recent years, due to the instability of the Tor[1] network [10], the mainstream market has begun to consider the possibility of operating on both Tor and I2P[2] networks to improve accessibility [13]. In addition, competitors' attacks on each other in the market threaten users security, which could result in loss to users.

Previous studies have mainly focused on social aspects, including analysis of products sold, emerging criminal patterns, criminal ecosystems, and key actors [7, 12, 13, 15, 16, 23]. However, the security mechanisms used by the dark web markets are not yet clear. In this paper, we aim to investigate the security mechanisms of different dark web markets. Furthermore, we understand the challenges of data collection in the dark web, and therefore, we expect to gain some valuable insights from this learning to improve the performance of existing crawlers.

[1]The Onion Router (Tor): https://www.torproject.org/
[2]Invisible Internet Project (I2P): https://geti2p.net/en/

Contributions. We obtained data and information on twelve mainstream dark web markets to document the security mechanisms implemented by those markets. We classified and described the security mechanisms used in the market, where web security includes accessibility, waiting queue, anti-phishing, CAPTCHAs, secret phrase, warrant canary, bug bounty, rate limiting, a distributed denial-of-service (DDoS) protection toolset, and account security includes username requirement, password & PIN requirement, mnemonic, multi-factor authentication (MFA), account kill-switch. We shared some insights into underlying trends, data collection and raised ethical considerations in this research area.

The rest of this paper is organised as follows. Section 2 introduces the work related to this paper in the field of dark web markets and cybercrime. We then describe and explain our research methods in Section 3. Section 4 is divided into two sub-sections to introduce and show the results in web security and account security aspects respectively. Section 5 summarises the key insights based on the findings we obtained, and discusses the implications of these findings along with ethical considerations. Finally, Section 6 concludes our paper and provides several ideas for future research.

2 RELATED WORK

Current literature on dark web markets has covered many aspects. Christin [5] collected and analysed data for eight months between late 2011 and 2012 for a longitudinal study in the most notorious dark web market – *Silk Road*. Van Wegberg et al. [21] analysed six years of longitudinal data from eight dark web markets. Both papers find out that the business model in the dark web is maturing. Wang et al. [23] compared the differences between Chinese and English dark web markets, which covers part of the security mechanisms but is very brief. During the COVID-19 pandemic, Bracci et al. [3] analysed COVID-19-related products over a period of approximately eleven months in 2020. The trends we see in dark web markets are very dynamic and ever-changing. Moreover, some literature also makes efforts to identify cross-platform players and key players, giving us a better understanding of the stakeholders (i.e. vendors, buyers and operators) in underground market and forums (not limited to dark web) [2, 13, 18]. However, there is currently no literature that clearly describes the security mechanisms implemented by dark web markets.

Data collection is also a challenge on the dark web [16, 25]. Labrador and Pastrana [16] evaluated multiple characteristics of selling products, vendors, and markets by implementing a custom crawler. Although we noticed that the authors described a flexible crawler capable of dealing with some anti-crawling techniques for this study, the time it takes for the crawler to crawl the entire market still depends on market constraints (in this case, a single market can take up to 61 hours), and this is often the reason why it is difficult for researchers to conduct large-scale longitudinal studies in dark web markets. Furthermore, Campobasso and Allodi [4] proposed a trainable, scalable crawler tool that makes it possible for researchers without computer backgrounds to use this tool for data collection in underground forums. In the experiments conducted by the authors, they overcame some restrictions (e.g., rate limiting, page loading time) by using different strategies when crawling different websites. But how these restrictions and strategies can be used for mainstream dark web markets remains unknown.

Turk et al. [20] studied and summarised the anti-crawling techniques in 26 underground forums, which cover both websites in the Tor network and the clear web. The paper also classifies these anti-crawling techniques and discusses some methods to mitigate these challenges. This study concluded that data collection in "adversarial" environments can be challenging. Even though there are some ways to mitigate, there are no easy solutions to avoid. It is recommended that the academic communities should actively share datasets. In fact, similar anti-crawling techniques are still unclear for dark web markets. Since dark web markets focus more on sales than forum-like discussions, we speculate that security mechanisms may be more stringent. Also, we introduce security mechanisms in terms of accounts.

Georgoulias et al. [11] comprehensively documents the features and functionality of existing dark web markets in 2021. The paper describes and summarises the operations of 41 markets and 35 independent vendor shops, and details the mechanisms for those markets' framework, which also include some security mechanisms, like CAPTCHAs during the registration process and the payment system mechanisms. In our work, we focus on security mechanisms using more recent and broad data points. The insights and experiences we share are more toward the data collection aspect.

Table 1: A summary of the selected dark web markets

Market Names	Type	Status
Abacus Market	Comprehensive	Live
Archetyp	Drugs-only	Live
ASAP Market	Comprehensive	Retired
Bohemia	Comprehensive	Live
Incognito	Drugs-only	Live
Kingdom Market	Comprehensive	Seized
Nemesis Market	Comprehensive	Live
Royal Market	Comprehensive	Closed
Tor2door Market	Comprehensive	Closed
Vice City Market	Comprehensive	Closed
Chinese Exchange Market	Comprehensive	Live
cabyc*	Comprehensive	Live

**cabyc* is the initials of Chang'an Nocturnal City in Chinese

3 METHODOLOGY

We selected twelve existing mainstream dark web markets when we started the research in May 2023. Over a span of four months (until August 2023), we collected data pertinent to these markets, paying close attention to any security mechanisms they have in place. Please note that there were some variations to the timing and quantity of the data collected from each market, due to some factors beyond our control (such as some markets were down for a period of time).

Table 1 provides a key summary of these twelve markets. These markets either sell drugs-only items, or they sell many categories of items (labelled as "Comprehensive"). In this table, we also state the market status at the time of writing this paper (December 2023).

Table 2: An overview of the selected dark web markets' web security mechanisms implementation (●= yes, ○= no, ◑= partial)

Markets	Accessibility TOR	Accessibility I2P	Waiting Queue	Anti-Phishing	CAPTCHAs	Secret Phrase	Canary	Bug Bounty
Abacus Market	●	○	●	●	text and image	◑	○	●
Archetyp	●	○	○	●	image	◑	○	●
ASAP Market	●	○	●	◑	interactive text	○	○	○
Bohemia	●	●	●	●	interactive text	○	●	●
Incognito	●	●	●	●	image	●	●	●
Kingdom Market	●	●	○	●	interactive text	●	○	◑
Nemesis Market	●	○	○	◑	image	○	●	○
Royal Market	●	○	○	◑	image	○	●	●
Tor2door Market	●	●	○	◑	text	○	●	◑
Vice City Market	●	○	●	○	color	○	○	●
Chinese Exchange Market	●	○	●	○	text	○	○	○
cabyc	●	○	○	○	Chinese, math, text	○	○	○

There are some markets marked as closed, or the reason for closure – which could be "retired" (where the market operators voluntarily closed down their market), or "seized" (where it is understood that the law enforcement agency took down the market). It should be noted that there are some uncertainties associated with this area of research. Also, we aim to reflect market conditions and characteristics at the time the research was conducted, which means the closure should not affect our results. Interestingly, we will discuss in the following sections whether security mechanisms have affected the operational life of the market. Those markets have been selected based on good representation and reputation in the dark web community (i.e. included and recommended by dark web forums and information websites).

We define and group the security mechanisms in those different markets into two main aspects: *web security* and *account security*.

In *web security*, we focus on the technical implementations and strategies that the market applies to their websites to protect users and themselves, such as CAPTCHAs, secret phrases, rate limiting, etc. In *account security*, we focus on the security mechanisms and policies that keep the account secure, such as username and password requirements, etc.

Information is gathered either while running a customised crawler or manually accessing the markets. Initially, we tried to use a crawler to obtain data for all mentioned markets. However, we encountered some difficulties, which also proves that some market security mechanisms are valid for operators. Therefore, we were able to note down those web security mechanisms we encountered and run some small experiments using the crawler. In terms of account security, most markets directly state such information (i.e. obtain information manually). Finally, we need manual access to the markets to obtain complete and comprehensive evidence and information. The crawler is implemented with Scrapy (https://scrapy.org/) and Selenium (https://www.selenium.dev/) using Python. While the crawler is helpful in certain scenarios, such as aiding in the comprehension of rate limiting, sometimes its utility can be limited during investigations, such as testing CAPTCHAs and introducing account security. In these cases, manual interaction is more effective and precise, allowing for a deeper understanding of the implementation of security mechanisms.

4 RESULTS

In this section, we describe and present our results. First, we describe the security mechanisms used by dark web markets in web security. We walk through the process of accessing a marketplace to explore security mechanisms, and cover an open source software commonly used by the dark web market. Following, we describe account security, which covers the username requirement, password & PIN requirement, mnemonic, MFA and account kill-switch.

4.1 Web Security

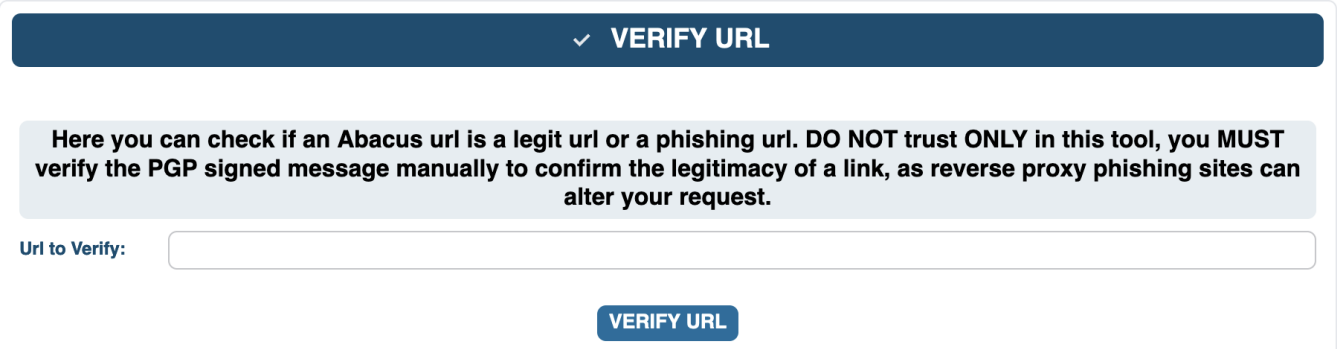
Table 2 presents an overview of whether selected dark web markets implement specific web security mechanisms. We describe the mechanisms and more separately in the following breakdown sections.

4.1.1 Accessibility. As background, accessing the dark web relies on the user needing to know the complete address of the server (or the server's mirror address). Market operators usually advertise on some "websites directories" sites, or users share them on general forums. As a registered or reputable user, users may also receive a private address, which is used to increase the accessibility of the market in the event that the main address suffers a DDoS. Most commonly, all markets support the Tor network, but we also found that some markets support the I2P network. One of the main reasons is that in 2023, the Tor network suffered from many performance issues [10], making it more difficult for users to access the market. Therefore, some markets decide to operate on both networks for redundancy. In addition, in the general environment, I2P seems to be faster than Tor in response time, which is also supported by literature [13]. We also noticed that three markets allow access to the product pages even if the user is not logged in or registered.

4.1.2 Waiting Queue. The first screen users usually see after entering a market will be queuing, which is mainly used to protect the website from DDoS attacks. The market first puts the user into a queue and then automatically redirects to the next screen after waiting for a period of time. We also found that this mechanism should also include load balancing function on the server side. We expect that most markets would implement this mechanism at the first point of entry to the site, but this is not the case. Only half of the

(a) Anti-phishing page on Bohemia

(b) Anti-phishing page on Archetyp



(c) Anti-phishing page on Abacus Market

Figure 1: Three anti-phishing pages on different markets with different designs

markets we selected apply this mechanism. Actually, CAPTCHAs could also have a protective effect on DDoS (which we describe in Section 4.1.4).

4.1.3 Anti-phishing. Depending on the market, users may see this screen before or after logging in. This is mainly due to the fact that the Tor network is flooded with fake mirror links used for phishing.

Figure 1a shows an example of an anti-phishing page. Users need to compare the URL in the browser's address bar and fill in the missing letters or numbers in the spaces.

Other markets have similar strategies. For example, Figure 1c shows that users can verify their address on the website by entering the complete URL address.

There are four markets marked as half-filled circles under the "anti-phishing" column of Table 2. This means that these four markets alert users to check and compare whether the URL being accessed is the same one showing on the page, but without any form of verification. For example, Figure 1b shows another way to remind the user in the background of the CAPTCHA to check that the starting and ending characters of the URL address should match. Admittedly, those measures do not completely prevent phishing from occurring. Once an attacker completely clones a website and replaces the engine behind this mechanism (i.e. the method of verification), completely unsuspecting users can still be easily deceived. This mechanism is more like a reminder to force users to check the URL. In case users notice the potential risk that the URL is inconsistent with the URL they usually visit. We also note that interestingly, in certain markets, this security mechanism is missing if users access the market via I2P network.

4.1.4 CAPTCHAs. As the most widely used security mechanism, CAPTCHA is ubiquitous on the dark web. Unlike *reCAPTCHA*-like software on the clear web, each dark web market can adopt its own style of CAPTCHAs.

Figure 2 shows examples of CAPTCHAs from six dark web markets. As shown in Table 2, in addition to the common static text input and image recognition, interactive text (i.e., the user needs to click/drag the correct answer instead of typing) and even colour and math-based questions appear in dark web markets as CAPTCHAs. Users not only need to solve a CAPTCHA when entering the website, but also sometimes they need to solve another one when logging in.

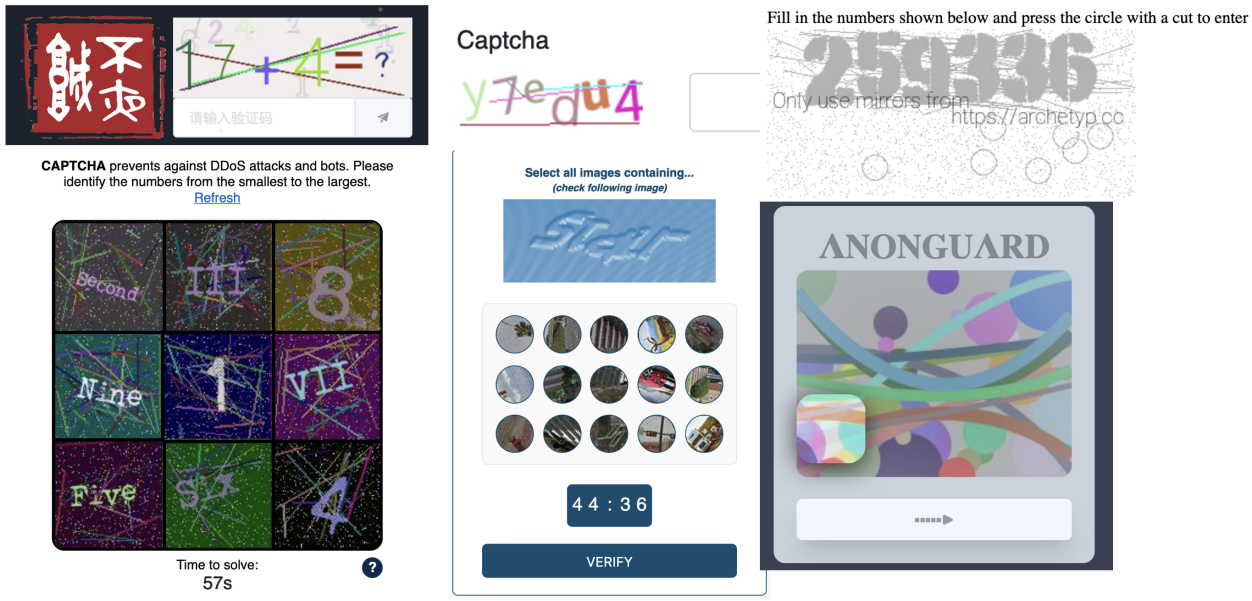


Figure 2: Examples of CAPTCHAs from six dark web markets.

Generally speaking, some CAPTCHAs are difficult to solve, and some even have time limits (i.e. users need to solve them correctly within a limited time).

4.1.5 Secret Phrase. This is actually another type of anti-phishing mechanism. Users can specify a secret phrase when registering. When the user logs in to the market, the secret will be displayed on the homepage. When the user realises that the secret phrase is displayed incorrectly (i.e. the user is on a fake website), the user has the opportunity to change the password and other information in the real market to prevent further losses.

In Table 2, there are two markets marked with half-filled circles. Their implementation of this mechanism may be unintentional, but they have the same effect. Users are asked to fill in their nickname when registering. However, users only need their username and password when logging in. Therefore, users have the same opportunity to check whether their nickname is showing correctly after logging in.

4.1.6 Warrant Canary. This is a more traditional security mechanism that states that the market is still controlled by specific operators. This statement (canary) is usually displayed on a page in the market and is signed with the operator's Pretty Good Privacy (PGP) signature. The statement has the date of the next update and proof of the date the current statement was signed (e.g., this could be the latest Bitcoin block hash). Users will be aware that operators may have lost control of the market if the canary is not updated within the mentioned date. We have noticed that some markets have canaries that are out of date, but operators usually update them after a few days.

4.1.7 Bug Bounty. While some may consider that bug bounty programs are not the core security mechanism, bug bounty programs do have an impact on market security by engaging users in discovering and exposing potential vulnerabilities for improvement. In Table 2, markets marked with full-filled circles refer that the market has a proper bug bounty program and clearly mention that certain rewards will be obtained after discovering some bugs. There are two markets marked with half-filled circles, meaning that the market mentions that a support ticket should be submitted to the market when a bug is discovered, but without further information. For markets marked with open circles, we believe users are still able to report directly to the market operator via in-site message or support ticket. However, these markets marked as open circles do not mention any guidance about what users should do if a bug is discovered.

4.1.8 Rate Limiting. This limitation may be affected by many factors in real-world data collection (e.g., the internet service provider, physical network interface, etc.). In practice, it is difficult for users to tell whether they are receiving rate limits from the market servers or they have other bottlenecks in the user's network. Here, we only discuss the potential use of security mechanisms on the dark web market side. A typical approach is to preset a threshold on the server side. Once the frequency or number of requests reaches this threshold within a period of time, the server will refuse to return the result page and perform additional security checks. Those additional security checks include additional CAPTCHAs (i.e. making the session expire) and killing the current Tor circuit (i.e. changing the Tor identity needed). In practice, some markets have very restrictive thresholds, making it very challenging to obtain data for the entire market.

4.1.9 EndGame DDoS Filter Toolset. EndGame (https://github.com/onionltd/EndGame) is an open-source and widely used front-end system for DDoS protection in the dark web. This toolset is used to easily deploy some of the security mechanisms we mentioned

Table 3: An overview of the selected dark web markets' account security mechanisms implementation (●= yes, ○= no)

Markets	Username	Password	PIN	MFA	Mnemonic	Kill-switch
Abacus Market	alphanumeric*	min. 1 chars	6 digits	●	●	○
Archetyp	alphanumeric	min. 4 chars	4 to 16 chars	●	○	○
ASAP Market	any	min. 6 chars	min. 4 chars	●	○	○
Bohemia	any	min. 7 chars‡	4 to 10 digits	●	●	○
Incognito	alphanumeric	min. 8 chars	system assigned	●	●	●
Kingdom Market	alphanumeric	min. 5 chars	6 digits	●	●	○
Nemesis Market	alphanumeric†	min. 5 chars	min. 4 chars	●	●	○
Royal Market	alphanumeric	min. 8 chars	4 to 6 digits	●	●	○
Tor2door Market	alphanumeric†	min. 8 chars	6 to 10 digits	●	●	○
Vice City Market	alphanumeric	min. 6 chars	4 to 12 chars	●	○	○
Chinese Exchange Market	system assigned	min. 8 chars‡	8 to 25 chars	○	●	○
cabyc	alphanumeric	min. 8 chars‡	8 to 24 chars	○	●	○

* lowercase only; † underscore and dash allowed; ‡ combination of uppercase, lowercase, number and/or special characters

above (e.g., two rate limiting methods based on Tor service circuit ID and cookies, customised randomly generated CAPTCHAs, time-based queue system, packet filtering, load-balancing etc.). Due to the nature of open source, market operators can easily customise functions without requiring a complex technical background, and the setup process is highly scripted. Compared with DDoS protection services on the clear web, EndGame can be deployed locally rather than hosted on a third party (like Cloudflare), which enforces the privacy requirements of market operators.

4.2 Account Security

In this subsection, we explore the security mechanisms applied to the account. As market operators, it is necessary to apply appropriate mechanisms to protect user accounts, which can help users avoid potential account loss, theft, scams, etc. Table 3 shows an overview of selected dark web markets' account security mechanisms implementation.

4.2.1 Username. The username is used as part of the login credentials. It is not only used to display the identity in the market, but also is part of the account security mechanism. Most markets support alphanumeric only, but there are exceptions, one market's username is assigned by the system, and two markets have almost no restriction (i.e. any character including special characters). The minimum length of usernames is one character, and four characters are the most common minimum requirement. The maximum length of usernames is sometimes set at 16 and 20 characters, but half of the markets in our study had no length limit (i.e. successful registrations with greater than 64 characters). Special characters are mostly not supported, but underscore and dash have been accepted in two markets.

4.2.2 Password & Personal Identification Number (PIN). Table 3 shows the minimum password requirements of the twelve selected dark web markets. In addition to minimum password length requirements, only three markets force users to set more complex passwords (i.e. a combination of uppercase, lowercase and numbers or/and special characters). Surprisingly, in two of the markets, there is an obvious maximum password length limit. This would not be recognised as a good strategy, with a market that has a maximum length limit of only 16 characters. In terms of PINs, all markets in our study have PINs used for payment-related activities. But those markets have various policies, some requested numbers only, while some can be set as complex as the password. One exception is that a market gives a secret word after user registration, but functions similarly to a PIN. In other markets, the PIN is set when the user registers.

4.2.3 Mnemonic & Multi-factor authentication (MFA). Due to the highly anonymous nature of the dark web market, the user registration process does not use any identifiable personal information, including the email address and phone number we commonly use on the clear web. Mnemonic and PGP keys are used for the same purposes in dark web markets. Mnemonics are given by the market when registered and are usually a set of English words or a long, meaningless string. Users need to save the mnemonic phrase in a safe place to use it to recover their account in certain situations. Nine of twelve markets have mnemonic for account recovery. MFA is mostly implemented through the PGP key. Users need to set up a PGP public key in the market first, and then the market will send verification information and encrypt it using the public key. Users can use the private key to obtain this verification information. MFA is often optional if browsing listings but mandatory for purchasing items. There is a market that uses the third method, which requires the users to enter the mnemonic phrase every time they login.

4.2.4 Account Kill-switch. This allows users to set a time limit in advance. When the account is inactive over the time set, the account will be automatically deleted by the market. Currently, this feature is a one-off, meaning the countdown will stop when the account is logged in again, and the user will need to set a new time limit. We only noticed this feature in one market (Incognito), but some markets support manual account deletion. However, we are not aware of any mechanism in the market to delete user accounts that have been inactive for a long time, although we believe this may exist but not be mentioned.

5 DISCUSSION

This section discusses the implications of these security mechanisms, especially with regard to market closure and the challenges these mechanisms pose to data collection. We also explain the ethical considerations that need to be taken into account in this line of research.

5.1 Implication of Security Mechanisms on Market Closure

Dark web markets have always been very dynamic and full of potentially unknowns features or quirks. We note that some markets are closed at the time of writing (December 2023). Wang et al. [24] mentioned that the closure of the dark web market has certain relationships with the security issues of the market. The authors noticed one of the underlying relationships is that markets are more likely to shut down when they are attacked.

When we look back at the security mechanisms mentioned in Table 1 and Table 2, we can see that the three markets with unknown reasons for closure (i.e. Royal Market, Tor2door Market and Vice City Market) might be due to relatively weak DDoS protection mechanisms (either the lack of waiting queue, or the use of weak CAPTCHAs, or both). This weakness would make them more prone to being disrupted by a third party. There could also be other security protection issues (or other factors) causing their demise.

Although our results may not be comprehensive, the security mechanisms implemented by the market reflect the market operator's business philosophy. That is to say, markets that want long-term stable operations will pay close attention to user experience and security. These factors will in turn attract users to trade in the market. We exclude impounded retirement and voluntary retirement because these two reasons for closure are often affected by more complex factors [14, 24].

5.2 Implication of Security Mechanisms on Data Collection

Data collection in dark web markets has always been a challenge in this field of research. Most mechanisms are not present after login to affect crawler access, with the exception of CAPTCHAs and rate limits. There are also other case-by-case solutions that work for certain market websites.

Regarding using automation (including machine learning) to solve CAPTCHAs on the dark web, Audran et al. [1] have verified that this is feasible with decent accuracy and performance. However, the authors focus on the clock CAPTCHAs and the variations. Apparently, there are many types and variants of CAPTCHAs used in the dark web market. There is a trade-off here, by the time we spend effort to crack a CAPTCHA, the market may no longer operate or change to the new CAPTCHAs.

Moreover, we argue that cracking (or knowing) rate limiting thresholds is more valuable, even if this requires some upfront experimentation. We can obtain complete data faster by using multiple accounts to run the crawler simultaneously. Nevertheless, very aggressive rate limiting settings can also affect access by real users (as humans, not crawlers). We wonder if we can design a crawler that can use an adaptive method to adjust the request rate dynamically instead of a set of predetermined values or a range of values.

There may actually be specific solutions for ad-hoc crawlers (rather than universal crawlers) of certain dark web markets. To our knowledge, most crawlers benefit from cookies obtained after manually solving CAPTCHAs, thereby simulating human visits to pages to obtain target data. During our research, we noticed that there is a market where the product listing data can be obtained by submitting a single request to the server API. Since the way this market obtains data on the front end of the web page is through the API, we are able to pass a larger parameter to the API to obtain all the data in JSON at once. Considering the file format characteristics of JSON, data transmission and formatting are very efficient and do not pass more stress onto the server. We also found that since JavaScript is generally not used in the dark web for security reasons (i.e. can be used to execute some malicious code), the structure of the web page is simpler than that on the clear web (i.e. there is less dynamically loaded content).

5.3 Ethical Considerations

Ethical considerations are very important for research in this area. All information obtained is considered inherently open and easily accessible to the public. Even though most dark web markets require registration, the process is open to the public. When registering, our usernames and other information are not linked to any individual or organisation. We also disclosed the names of these markets, because these names are well-known within the dark web community. We believe this will help academia and law enforcement agencies better understand the trends in mainstream dark web markets. However, we do not judge a market or its security mechanisms as good or bad.

When conducting security experiments (e.g., access restrictions and rate limiting), we carefully adjust parameters to ensure that our experiments do not affect the market's servers. We only visit the market from an observer's perspective and do not attempt any unnecessary actions out of this study. Our research ethics considerations were reviewed and approved by our university's research ethics committee (Ref: 057-04-2021).

In fact, there are many more aggressive security tests we could have done, such as the rate limiting and the OWASP Top Ten (https://owasp.org/www-project-top-ten). But for ethical reasons, we figured we did not want to be a potential attacker. On the other hand, some markets offer bug bounty programs that actually allow for a certain level of agreement to conduct some security testing on the market. Further dialogue and discussion should be necessary within the law enforcement agencies and academic communities to reduce barriers. This will also help both parties better understand the responsibilities and needs of both parties, and further promote understanding in the dark web field.

6 CONCLUSION

In conclusion, this paper presents the outcome of our investigation into how security mechanisms are implemented in mainstream dark web markets. In particular, we highlight that the twelve dark web markets we observed have different levels of security mechanisms to protect themselves and their users. At this stage, we believe that using manual labour in data collection on the dark web market is unavoidable.

Our results reveal that the security mechanisms implemented by mainstream dark web markets include web security and account security. Web security includes accessibility, waiting queue, anti-phishing, CAPTCHAs, secret phrase, warrant canary, bug bounty, rate limiting. Account security includes username requirement, password & PIN requirement, mnemonic, MFA, account kill-switch. We also discuss how security mechanisms being implemented by market operators (or not) may reflect the operators' business philosophy (for instance, whether they plan to stay long in the business). We also share some insights regarding data collection and the key challenges associated with it. Finally, we discuss ethical issues that need to be considered in this line of research.

For future work, it will be beneficial to expand the data sources, which will help the academic community gain a broader understanding of the security measures of the dark web markets and design crawlers for data collection in a more targeted manner. Moreover, a better and more detailed understanding of how rate limiting feature works may greatly improve the efficiency of crawlers and reduce manual labour. There is a promising sign that we can use software scripts to solve simple CAPTCHAs. However, it should be noted that market protections can vary to a large degree, and some dark web markets employ more complex CAPTCHAs. These are more difficult to solve, but it is envisaged that machine learning techniques can be used to solve them quite easily in the future. We are only able to cover the end-user side of security mechanisms, which may not be comprehensive. But we also raise ethical considerations for academics on how to properly and ethically improve research in this area.

ACKNOWLEDGMENTS

This work was partly supported by the funding received from the European Commission under the Horizon 2020 Programme (H2020) through the HEROES project (https://heroes-fct.eu/, Grant Agreement no. 101021801).

REFERENCES

[1] David Audran, Marcus Andersen, Mark Hansen, Mikkel Andersen, Thomas Frederiksen, Kasper Hansen, Dimitrios Georgoulias, and Emmanouil Vasilomanolakis. 2022. Tick Tock Break the Clock: Breaking CAPTCHAs on the Darkweb. In *Proceedings of the 19th International Conference on Security and Cryptography - SECRYPT*. INSTICC, SciTePress, Lisbon, Portugal, 357–365. https://www.scitepress.org/PublishedPapers/2022/112733/112733.pdf

[2] Rasika Bhalerao, Maxwell Aliapoulios, Ilia Shumailov, Sadia Afroz, and Damon McCoy. 2019. Mapping the Underground: Supervised Discovery of Cybercrime Supply Chains. In *2019 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, Pittsburgh, PA, USA, 1–16. https://doi.org/10.1109/eCrime47957.2019.9037582

[3] Alberto Bracci, Matthieu Nadini, Maxwell Aliapoulios, Damon McCoy, Ian Gray, Alexander Teytelboym, Angela Gallo, and Andrea Baronchelli. 2021. Dark Web Marketplaces and COVID-19: before the vaccine. *EPJ data science* 10, 1 (2021), 6. https://doi.org/10.1140/epjds/s13688-021-00259-w

[4] Michele Campobasso and Luca Allodi. 2022. THREAT/crawl: a Trainable, Highly-Reusable, and Extensible Automated Method and Tool to Crawl Criminal Underground Forums. In *2022 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, Boston, MA, USA, 1–13. https://doi.org/10.1109/eCrime57793.2022.10142081

[5] Nicolas Christin. 2013. Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace. In *Proceedings of the 22nd International Conference on World Wide Web* (Rio de Janeiro, Brazil) *(WWW '13)*. Association for Computing Machinery, New York, NY, USA, 213–224. https://doi.org/10.1145/2488388.2488408

[6] Christopher Copeland, Mikaela Wallin, and Thomas J Holt. 2020. Assessing the practices and products of Darkweb Firearm vendors. *Deviant Behavior* 41, 8 (2020), 949–968. https://doi.org/10.1080/01639625.2019.1596465

[7] Abeer ElBahrawy, Laura Alessandretti, Leonid Rusnac, Daniel Goldsmith, Alexander Teytelboym, and Andrea Baronchelli. 2020. Collective dynamics of dark web marketplaces. *Scientific reports* 10, 1 (2020), 1–8. https://doi.org/10.1038/s41598-020-74416-y

[8] Europol. 2023. 288 dark web vendors arrested in major marketplace seizure. https://www.europol.europa.eu/media-press/newsroom/news/288-dark-web-vendors-arrested-in-major-marketplace-seizure

[9] Europol. 2023. Internet Organised Crime Assessment (IOCTA) 2023. https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf

[10] Sergiu Gatlan. 2023. Tor and I2P Networks Hit by Wave of Ongoing DDoS Attacks. https://www.bleepingcomputer.com/news/security/tor-and-i2p-networks-hit-by-wave-of-ongoing-ddos-attacks/

[11] Dimitrios Georgoulias, Jens Myrup Pedersen, Morten Falch, and Emmanouil Vasilomanolakis. 2021. A qualitative mapping of Darkweb marketplaces. In *2021 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, Boston, MA, USA, 1–15. https://doi.org/10.1109/eCrime54498.2021.9738766

[12] Dimitrios Georgoulias, Jens Myrup Pedersen, Morten Falch, and Emmanouil Vasilomanolakis. 2023. Botnet Business Models, Takedown Attempts, and the Darkweb Market: A Survey. *ACM Comput. Surv.* 55, 11, Article 219 (Feb 2023), 39 pages. https://doi.org/10.1145/3575808

[13] Dimitrios Georgoulias, Ricardo Yaben, and Emmanouil Vasilomanolakis. 2023. Cheaper than You Thought? A Dive into the Darkweb Market of Cyber-Crime Products. In *Proceedings of the 18th International Conference on Availability, Reliability and Security* (Benevento, Italy) *(ARES '23)*. Association for Computing Machinery, New York, NY, USA, Article 106, 10 pages. https://doi.org/10.1145/3600160.3605012

[14] Alice Hutchings, Richard Clayton, and Ross Anderson. 2016. Taking down websites to prevent crime. In *2016 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, Toronto, ON, Canada, 1–10. https://doi.org/10.1109/ECRIME.2016.7487947

[15] Emmanouil Kermitsis, Dimitrios Kavallieros, Dimitrios Myttas, Euthimios Lissaris, and Georgios Giataganas. 2021. *Dark Web Markets*. Springer International Publishing, Cham, 85–118. https://doi.org/10.1007/978-3-030-55343-2_4

[16] Víctor Labrador and Sergio Pastrana. 2022. Examining the trends and operations of modern Dark-Web marketplaces. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, Genoa, Italy, 163–172. https://doi.org/10.1109/EuroSPW55150.2022.00022

[17] National Crime Agency. 2023. Child Sexual Abuse and Exploitation. https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/child-sexual-abuse-and-exploitation

[18] Sergio Pastrana, Alice Hutchings, Andrew Caines, and Paula Buttery. 2018. Characterizing Eve: Analysing Cybercrime Actors in a Large Underground Forum. In *Research in Attacks, Intrusions, and Defenses*. Springer International Publishing, Cham, 207–227. https://doi.org/10.1007/978-3-030-00470-5_10

[19] Joe Tidy. 2022. Hydra: How German police dismantled Russian darknet site. https://www.bbc.co.uk/news/technology-61002904

[20] Kieron Turk, Sergio Pastrana, and Ben Collier. 2020. A tight scrape: methodological approaches to cybercrime research data collection in adversarial environments. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, Genoa, Italy, 428–437. https://doi.org/10.1109/EuroSPW51379.2020.00064

[21] Rolf Van Wegberg, Samaneh Tajalizadehkhoob, Kyle Soska, Ugur Akyazi, Carlos Gañán, Bram Klievink, Nicolas Christin, and Michel Van Eeten. 2018. Plug and Prey? Measuring the Commoditization of Cybercrime via Online Anonymous Markets. In *Proceedings of the 27th USENIX Conference on Security Symposium* (Baltimore, MD, USA) *(SEC'18)*. USENIX Association, USA, 1009–1026. https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-van_wegberg.pdf

[22] Yichao Wang, Budi Arief, Virginia Nunes Leal Franqueira, Anna Grace Coates, and Caoilte Ó Ciardha. 2023. Investigating the Availability of Child Sexual Abuse Materials in Dark Web Markets: Evidence Gathered and Lessons Learned. In *Proceedings of the 2023 European Interdisciplinary Cybersecurity Conference* (Stavanger, Norway) *(EICC '23)*. Association for Computing Machinery, New York, NY, USA, 59–64. https://doi.org/10.1145/3590777.3590812

[23] Yichao Wang, Budi Arief, and Julio Hernandez-Castro. 2021. Toad in the Hole or Mapo Tofu? Comparative Analysis of English and Chinese Darknet Markets. In *2021 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, IEEE, Boston, MA, USA, 1–13. https://doi.org/10.1109/eCrime54498.2021.9738745

[24] Yichao Wang, Budi Arief, and Julio Hernandez-Castro. 2023. Dark Ending: What Happens when a Dark Web Market Closes down. In *Proceedings of the 9th International Conference on Information Systems Security and Privacy - ICISSP*. INSTICC, SciTePress, Lisbon, Portugal, 106–117. https://doi.org/10.5220/0011681600003405

[25] York Yannikos, Julian Heeger, and Martin Steinebach. 2022. Data Acquisition on a Large Darknet Marketplace. In *Proceedings of the 17th International Conference on Availability, Reliability and Security* (Vienna, Austria) *(ARES '22)*. ACM, New York, NY, USA, Article 53, 6 pages. https://doi.org/10.1145/3538969.3544472