International Journal of Information Security manuscript No.
(will be inserted by the editor)

Secure in the Dark? An In-Depth Analysis of Dark Web Markets Security

Yichao Wang · Budi Arief · Julio Hernandez-Castro

Received: date / Accepted: date

Abstract As the name implies, dark web markets – also commonly known as anonymous markets – have put in place measures for protecting the privacy of its users, both sellers and buyers, as this is a key priority that can attract users worldwide. With the rapid growth of dark web markets, competition among them has become more intense. In this environment, malicious attacks targeting competitors – for instance, aimed at reducing the availability of rivals' services – have also become more common. These attacks not only affect other services' availability and accessibility, but they may also lead to personal and private information being leaked. As such, it is understandable that dark web markets may want to implement strong security mechanisms to protect themselves and their users from both law enforcement and other operators. This is particularly true as good security can be a matter of survival but also help to gain a competitive edge over rivals. Although the literature has analysed and described dark web markets from multiple perspectives, there is still a gap in the understanding of the different security mechanisms they deploy. Furthermore, data collection – which is often considered a challenge in this research area – may be hindered by these very security mechanisms. Therefore, and in order to cover this gap, the study presented in this paper aims to investigate in depth the security mechanisms of various dark web markets. This will hopefully help to shed a brighter light on their operation. To achieve this, we performed data collection and experiments in twelve dark web markets. Although data collection practices may need to vary slightly for each market, all the data was collected over the span of four months, between May and August 2023. We found there are three main groups of security mechanisms in dark web markets: (i) those aimed towards increasing web security, (ii) those mostly aimed at improving account security, and (iii) those related to financial security. In addition, it is interesting to note that different types of security mechanisms on a given market may reflect the operator's business philosophy, technical knowledge and security posture, which in turn could have a big impact on the longevity, profitability and overall success of a particular market. The results of this study can help the academic and security research communities to understand the operation and evolution of dark web markets, hopefully to combat the crimes facilitated by these dark web markets more effectively. Additionally, findings in this study may provide some clues on how to improve the efficiency of data collection in this particularly hostile environment.

Keywords Dark Web Market · Security Mechanism · Web Security · Account Security · Financial Security · Market Operation

Y. Wang
University of Kent, Canterbury, UK
E-mail: yw300@kent.ac.uk

B. Arief
University of Kent, Canterbury, UK
E-mail: b.arief@kent.ac.uk

J. Hernandez-Castro
Universidad Politécnica de Madrid, Madrid, Spain
E-mail: jc.hernandez.castro@upm.es

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 [16]. From the famous *Silk Road* to the recently shut down *Hydra Market* [28], many have been suspected of selling from firearms to child sexual abuse materials [11,33,26]. It is arguable that the rising numbers and popularity of dark web markets, despite presenting some advantages in countries where freedom is at stake, can globally be seen as becoming, over time, more and more destructive to society. At the same time, they are increasingly becoming a serious challenge for both 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 operators of the *Monopoly Market*, a very successful, esteemed and renown market at the time [15].

Nevertheless, the operation of dark markets is far from immutable. In a narrow sense, the term "dark web markets" meant a marketplace on the Tor network. In recent years, however, and mostly due to the instability of Tor[1] network [17], mainstream markets have begun to consider the possibility of operating on both Tor and I2P[2] networks to improve their accessibility [20]. This situation is, in addition, accentuated by the increased frequency of competitors' attacks against each other.

Previous studies have mainly focused on social aspects, including analysis of products sold, emerging criminal patterns, criminal ecosystems, and key actors [20,19,34,24,23,14]. However, the security mechanisms used by the dark web markets have not been addressed in enough depth. In this paper, we aim to investigate the security elements of different dark web markets. Furthermore, we understand the challenges of data collection on the dark web, and therefore, we expect to gain some valuable insights from the data collection process in this work in order to help improving the efficacy of current crawlers.

Contributions. This paper's key contributions are:

- We obtained data from twelve mainstream dark web markets, to document and study the security mechanisms they implemented.
- We classified and described the security mechanisms used in the markets, where *web security* includes accessibility, waiting queues, anti-phishing, CAPTCHAs, secret phrases, warrant canaries, bug bounties, rate limiting, and distributed denial-of-service (DDoS) protection; *account security* includes areas such as username, password and PIN requirements, mnemonics, multi-factor authentication (MFA), account kill-switch, etc.; and *financial security* covers strategies such as the choice of (crypto)currency being used, specific transaction concepts such as the use of multi-signature, escrow and finalise early, as well as the handling of complaints and general user support.
- We share some insights into underlying trends, data collection and also raise some ethical considerations that may be relevant in this research area.

The rest of this paper is organised as follows. Section 2 introduces the work related to this work in the field of dark web markets and cybercrime. Section 3 describes and explains our research methodology, including the design and architecture of our custom crawler. Section 4 presents the key results of our research, namely our findings on the main three types of security mechanisms encountered on the dark web markets: web security, account security and financial security. 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

As rapidly developing business, dark web markets are undergoing changes all the time. The current literature on them has covered well various important features, providing valuable insights for the understanding of how dark web markets operate. For instance, Christin [9] collected and analysed data for eight months (between late 2011 and 2012) for a longitudinal study in the most notorious dark web market at the time – *Silk Road*. Van Wegberg et al. [32] analysed no less than six years of longitudinal data from eight dark web markets. Both works find out that the business models of these markets is maturing. Wang et al. [34] compared Chinese and Occidental dark web markets, covering briefly some aspects of the security mechanisms they employ. During the heights of the COVID-19 pandemic, in 2020, Bracci et al. [6] analysed COVID-19-related products over a period of approximately eleven months.

The trends observed 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) [27,4,20]. However, there is currently no literature that comprehensively describes the security mechanisms implemented by dark web markets.

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

Table 1: A summary of the selected dark web markets (as of 31 August 2024)

Market Names	Type	First Seen	Last Seen	Status
Abacus Market	Comprehensive	2021-09	(still active)	Live
Archetyp	Drugs-only	2020-05	(still active)	Live
ASAP Market	Comprehensive	2020-03	2023-07	Retired
Bohemia	Comprehensive	2021-05	2024-01	Closed/Seised
Incognito	Drugs-only	2020-10	2024-03	Closed/Seised
Kingdom Market	Comprehensive	2021-05	2023-12	Seised
Nemesis Market	Comprehensive	2021-05	2024-03	Seised
Royal Market	Comprehensive	2021-03	2023-08	Closed
Tor2door Market	Comprehensive	2020-07	2023-09	Closed
Vice City Market	Comprehensive	2020-08	2023-07	Closed
Chinese Exchange Market	Comprehensive	2018-03	(still active)	Live
cabyc*	Comprehensive	2022-02	(still active)	Live

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

Data collection on the dark web is also a big challenge [37,24]. Bergman and Popov [3] systematically reviewed 34 published research articles that contained web crawlers on the dark web. They also developed a new dark web crawler based on the knowledge in the literature, able to achieve automatic web content classification through a novel toolset. Although the results show that the crawler they developed is usable, some human inputs are still required to ensure the reliability of the data collection process. In another study, Labrador et al. [24] 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). This is often the reason why it is challenging to conduct large-scale longitudinal studies in dark web markets. Furthermore, Campobasso and Allodi [8] proposed a trainable, scalable crawler tool that makes it possible for researchers without computer backgrounds to use their 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. It is both interesting and extra challenging that they also noticed a new and complex anti-crawling measure in the study, consisting on the dynamic obfuscation within HTML attributes (like IDs or the name of tags/classes). However, how these ideas and strategies can be deployed for mainstream dark web markets remains unclear.

Turk et al. [30] studied and summarised the anti-crawling techniques used in 26 underground forums, covering both websites in the Tor network and the clear web. The paper also classified these anti-crawling techniques and discussed some methods to mitigate these challenges. This study concluded that data collection in "adversarial" environments can be particularly challenging. Even though there are some ways to mitigate their effect, there are no easy solutions to avoid it completely. It is recommended that the academic communities should actively share datasets. In fact, similar anti-crawling techniques are still unseen in dark web markets. Since dark markets focus more on sales than forum-like discussions, we speculate that security mechanisms may be more stringent. In relation to this, we feel there is a real need to investigate these security mechanisms further, particularly regarding the protection of user accounts.

Georgoulias et al. [18] comprehensively documented the features and functionality of existing dark web markets in 2021. Their paper described and summarised the operations of 41 markets and 35 independent vendor shops, and detailed the mechanisms for those markets' framework, which also include some security mechanisms, like CAPTCHAs during the registration and payment process. In our current work, we focus on security mechanisms using more recent and broad data points. The insights and experiences we share are mostly regarding data collection.

Finally, Yoon et al. [38], as well as Güldenring and Roth [21] investigated the important problem of phishing domains/websites on the dark web. They showed various strategies designed by onion service operators to protect their users from phishing attacks. They also proposed "recognisers" capable of detecting phishing to fill the existing research gap. There are some parallels between these papers and the work we are presenting in the current paper here, but there are also several differences. For instance, our focus extends beyond security mechanisms specifically designed to prevent phishing attacks (though some are indeed effective against such attacks). We also cover mechanisms related to DDoS

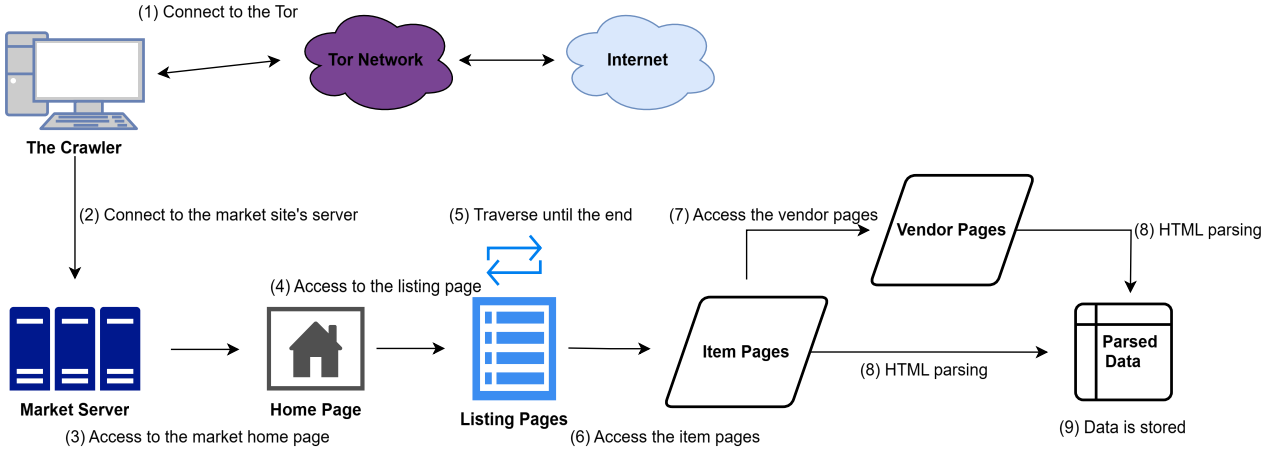


Fig. 1: The architecture and the logic of our crawler

attacks, account, web and financial security, together with some other related topics.

3 Methodology

We selected twelve existing mainstream dark web markets when we started our research in May 2023. Market selection was based on observations of the *Dread* forum (a dark web forum), searches on the clear web using keywords such as "dark web market", and manual verification of markets that were active at the time. 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 markets being down for short periods of time, etc.).

Table 1 provides a key summary of these twelve markets which either sell drugs-only items, or sell many different categories of items (labelled as "Comprehensive"). In this table, we also state the date they were first and last seen online, and the market status at the time of writing this paper (August 2024). There are some markets marked as closed, with the reason for closure – which could be "retired" (where the market operators voluntarily closed down their market), or "seised" (where it is understood that some law enforcement agencies 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 likely affected the operational longevity of the market. Those markets have been selected based on good representation and reputation on 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 three main aspects: *web security*, *account security* and *financial 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. In *financial security*, we describe the mechanisms associated with transactions, such as the accepted currencies, the type of transaction, etc.

Information is gathered either while running a customised crawler or manually accessing the markets. The next subsection provides an overview of the customised crawler we implemented for conducting this research. While the crawler is helpful in certain scenarios, such as aiding in the understanding of rate limiting, sometimes its utility can be limited during investigations, such as when testing CAPTCHAs and account security. In these cases, manual interaction is generally more effective and precise, allowing for a deeper understanding of the implementation quirks of security mechanisms.

3.1 Implementation of A Customised Crawler

Initially, we tried to use an existing crawler to obtain (sales-related) data for all markets. However, we encountered some difficulties, which also shows the dynamic nature of most market security mechanisms.

Table 2: An overview of the selected dark web markets' web security mechanisms (●= 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	○	○	○

While dealing with these issues, we were able to jot down the security mechanisms we encountered and run some small experiments against them using the crawler.

The crawler is implemented with Scrapy[3] and Selenium[4] using Python. The Scrapy framework implements the crawling, downloading, and parsing functions, while Selenium can be integrated into Scrapy, providing an interface for login, CAPTCHA solving, and other processes that require human interaction. This solution ensures that Selenium performance limitations do not significantly slow down the actual crawling speed. Figure 1 depicts the architecture and the logic of our crawler. There are nine steps that our crawler needs to perform before obtaining the data:

1. The crawler is hosted in a virtual machine container (i.e. the host). In this step, we need to establish a Tor connection from the host. Privoxy[5] is used to relay between Tor connections and Scrapy, because they support different proxy network protocols.
2. Selenium can be integrated into Scrapy. Then, Selenium is used to initialise and establish a connection to the market server.
3. Human interaction is required here to solve the CAPTCHAs, to log in to an account, etc. After that, Selenium passes the web session back to Scrapy to automate the subsequent steps.
4. Depending on the structure of different websites, the market usually has its own peculiar taste and logic in arranging and displaying the products on sale. The crawler will look for the entry to the listing page on the home page. The URL of the listing page can also be defined in the crawler, in advance.
5. This step sorts the products appropriately on the listing page, and then traverses through all of the listing pages of all items on the website.
6. This depends on the market, but most of the information that we care about (such as price, sales volume, feedback, and product description) should be included on the item page.
7. The crawler will then find the vendor information page on the item page and access it via Scrapy.
8. This step parses our target data (depending on the purpose of the study) in the HTML code using methods such as XPath.
9. Finally, the data is saved in the host computer for later analysis.

Thanks to the flexibility provided by Scrapy, the crawler can be easily modified. For example, in our study, we can access all the links on the homepage (based on HTML) in Step 4, and then further confirm whether those pages contain any valuable information. Scrapy can also handle repeatedly visited URLs well and supports customised filters. When downloading data, we can use the middleware function of Scrapy to determine whether the response code of the website is valid (i.e. between Step 7 and 8). When the website returns a non-valid response, the crawler can call the Selenium component for manual interaction and inspection. Moreover, to the best of our knowledge, the class names used in steps 5-8 are static in terms of path or ID in the HTML code, thus indicating that the sites do not apply crawler obfuscation traps. This process also prevents crawlers from getting stuck in program deadlocks (infinite loops) [12].

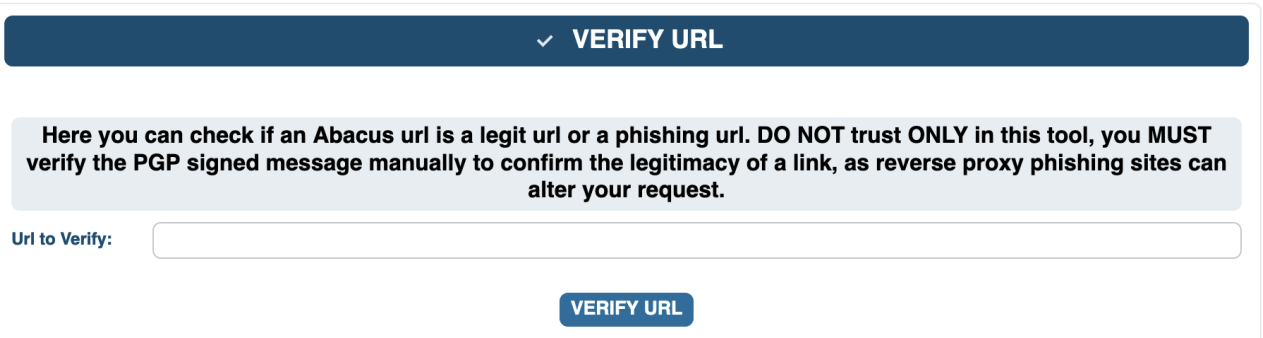
4 Results

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

[3] `https://scrapy.org/`
[4] `https://www.selenium.dev/`
[5] `https://www.privoxy.org/`

(a) Anti-phishing page on *Bohemia*

(b) Anti-phishing page on *Archetyp*



(c) Anti-phishing page on *Abacus Market*

Fig. 2: Three anti-phishing pages on different markets

commonly used by the dark markets. Following this, we describe account security, which covers the username, password & PIN requirements, mnemonics, MFA and account kill-switch. Finally, we describe the details of their implementation of financial security, including the supported currencies, transaction types, as well as the handling of complaints and general user support.

4.1 Web Security

Table 2 presents an overview of whether selected dark web markets implement specific web security mechanisms. We describe each mechanism in the following sections.

4.1.1 Accessibility

Accessing the dark web requires the users to know the address of the server (or its mirror). To help promote their markets, market operators usually advertise the address of their servers on the "website directories" pages. Users also typically share them on general forums. In the case of a registered or reputable user, you may also receive a private address, which is used to increase the availability of the market in the event that the main address suffers a successful DDoS attack. In general, all markets support the Tor network, but we also found that some additionally support the I2P network. One of the main reasons for this is that from late 2022 to early 2023, the Tor network suffered from many performance issues [17,29], making it significantly harder for users to access these markets. Therefore, some decided to operate on both networks for redundancy. In addition, we noticed that most of the time, I2P seems to be faster than Tor when it comes to response times. This observation is in agreement with what Georgoulias et al. reported in their paper [20]. They measured the response times in *AlphaBay*, and highlighted that the average response time for I2P was 5.6 seconds, which is faster than the 9.1 seconds for Tor. In [13], other researchers have shown that although I2P generally features better latency results than Tor, the latter seems to offer, in general, better

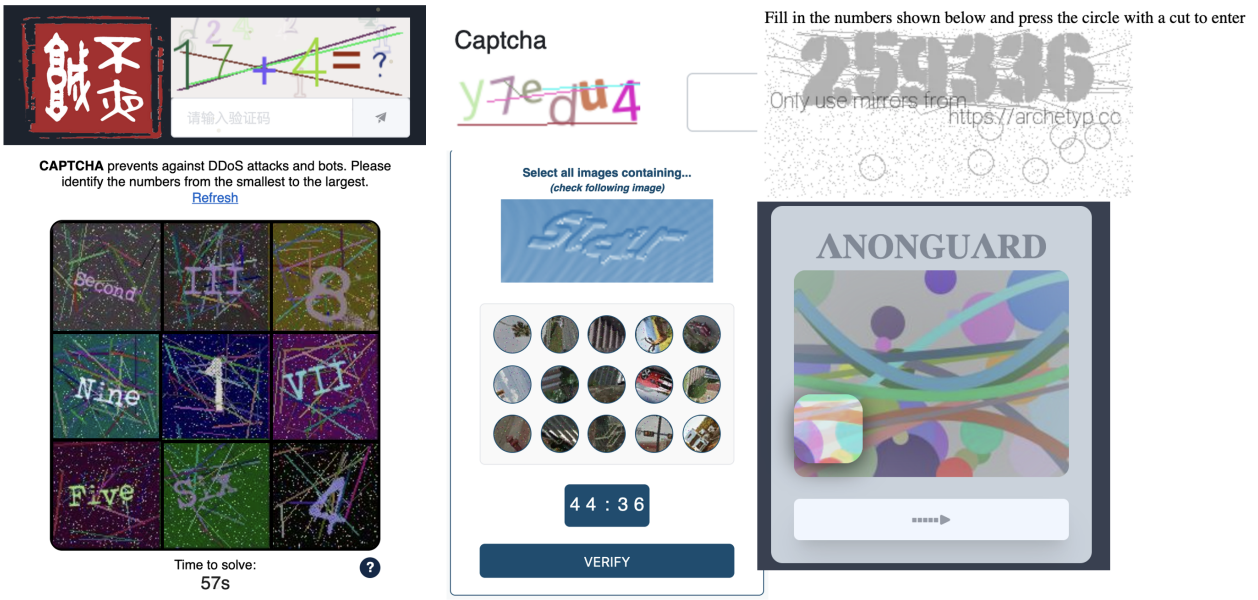


Fig. 3: Examples of CAPTCHAs from six dark web markets.

throughput and download times than I2P. For example, Tor got to an average speed of 51 kB/s while I2P only got to approximately 13 kB/s. This research was published more than a decade ago (2011) and can easily no longer hold true, which would be in agreement with what we observed during our work. In addition, and regarding congestions, Tor uses circuit switching, whereas I2P uses packet switching. Hence, Tor has often to cope with high congestion rates [10] leading to high latency. Whereas in I2P, the packet switching leads to some implicit load balancing and helps to avoid congestion and service interruptions. This is specifically important for large file transfers and therefore I2P is more suitable for such purposes. We also noticed that three markets (*ASAP Market*, *Nemesis Market*, *Chinese Exchange Market*) allow access to 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 some sort of load balancing feature 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 surprisingly not the case. Only half of the markets we selected apply this security mechanism. Actually, CAPTCHAs could also have a somewhat 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 2a 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 2c 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 2b 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. We

also note that, interestingly, in certain markets, this security mechanism is missing if users access the market via the I2P network.

4.1.4 CAPTCHAs

As the most widely used security mechanism in this sector, CAPTCHAs are ubiquitous on the dark web. The lack of access (due to their illegal operations) to a somewhat standardised solution such as *reCAPTCHA* forces each dark market to develop their own implementations, an approach that is strongly considered as dangerous in the computer security circles. This naturally implies that all of the CAPTCHAs deployed in dark markets are, without exceptions, flawed and trivial to break automatically, specially after the recent developments in AI capabilities in text and image recognition and classification.

Figure 3 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. These are all old and now trivial approaches that the CAPTCHA community has abandoned years ago. The most popular modern approach is based around adversarial examples that fool AI systems. Users not only need to solve a CAPTCHA when entering the website, but also sometimes they need to solve another one when logging in.

Generally speaking, some CAPTCHAs seem to be difficult to solve, and some even have strict time limits (i.e. the users need to solve them correctly within a limited time). However, if we bring in the latest knowledge on CAPTCHA generation and breaking from the security community, these CAPTCHAs are all trivial to break. It seems that CAPTCHA designers for dark web markets, fortunately (and unsurprisingly) do not follow recent academic literature in the topic, and it absolutely shows in their designs.

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 a core security mechanism, bug bounty programs do usually have an impact on market security, by engaging users in discovering and reporting potential vulnerabilities for improvement. In Table 2, markets marked with full-filled circles are those that have a proper bug bounty program and clearly mention that certain rewards will be obtained after discovering 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 on rewards. That is not the way to run a bug bounty program. For markets marked with open circles, we believe users are still able to report directly to the market operator via in-site messages or support tickets. For example, one of the markets we observed has an optional subject in their ticket system – bug bounty, which further categorises the priorities into low, medium, and high. However, markets with open circles do not mention any guidance about what users should do if a bug is discovered.

In one of the markets, we observed a very detailed list of potential rewards available to the bug reporter. The market operators have graded the importance of different bugs, including info, low, medium, high, and

Table 3: An overview of the selected dark web markets' account security mechanisms (●= 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

critical. These tiered rewards range from $5 to more than $5,000. In terms of scope, this program covers various types of vulnerabilities, such as UI issues, server-side disclosure, sensitive data disclosure, authentication bypass, command execution, etc.

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 suffering from rate limits by the market servers or if there are 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 given period of time, the server will refuse to return the result page and perform additional security checks. Those additional security checks may 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. For example, in *Bohemia*, our crawler operates at an average of ten requests per minute without the need for manual intervention for a long time. If we doubled up the speed (or even faster), we might be able to collect data more quickly in bursts, but if we continued for several minutes, we would trigger the anti-crawling mechanisms and this would interrupt our data collection. As such, we have to make a compromise in this situation. The slower method would lead to a lengthy data collection time – e.g., taking more than four hours just to retrieve the listing pages data, without the item details yet – but it would allow our crawler to operate autonomously without requiring our intervention.

4.1.9 EndGame DDoS Filter Toolset

EndGame[6] is an open-source and widely used front-end system for DDoS protection on the dark web. This toolset is used to easily deploy some of the security mechanisms we mentioned 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 an advanced 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 fits well with 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 provides 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.

[6] `https://github.com/onionltd/EndGame`

Table 4: An overview of the selected dark web markets' financial security (●= yes, ○= no)

Markets	Currency Allowed			Transaction		
	BTC	XMR	Others	Multisig	Escrow	FE
Abacus Market	●	●	○	●	●	●
Archetyp	○	●	○	○	●	●
ASAP Market	●	●	○	○	●	●
Bohemia	●	●	○	●	●	●
Incognito	●	●	○	○	●	●
Kingdom Market	●	●	●	○	●	●
Nemesis Market	●	●	○	○	●	●
Royal Market	●	●	○	○	●	●
Tor2door Market	●	●	○	●	●	●
Vice City Market	●	●	○	●	●	●
Chinese Exchange Market	●	○	○	○	●	○
cabyc	●	○	●	○	●	○

FE: finalise early

Most markets support alphanumeric only, but there are exceptions, one market's username is automatically 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, but four characters is the most common minimum requirement. The maximum length of usernames is sometimes set at 16 or 20 characters, but half of the markets in our study had no length limit (i.e. we achieved successful registration with more than 64 characters). Special characters are mostly not supported, but underscore and dash are accepted in two markets.

4.2.2 Password & Personal Identification Number (PIN)

Table 3 shows the minimum password requirements of the twelve studied 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 is not a good strategy, with a market having a maximum length limit of only 16 characters. In terms of PINs, all markets in our study have PINs for payment-related activities. But they employ quite different policies. Some requested numbers only, while some can be set to be 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, similar to the seed phrase one would employ to generate a Bitcoin wallet. Users need to save the mnemonic phrase in a safe place to use it to recover their account in certain situations. Nine out of twelve markets have mnemonics 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 that public key. Users can use the private key to obtain this verification information. MFA is often optional when browsing listings but mandatory for purchasing items. *Incognito* also requires users to enter their mnemonic phrase each time they log in, in addition to using PGP as MFA.

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 reported or well-known.

4.3 Financial Security

In this subsection, we explore information about financial security related to doing transactions while using the market. Financial security is essential for both users and vendors, as it could attract and maintain their loyalty by offering more selections. Table 4 presents an overview of allowed currencies and transaction types in our observed markets.

4.3.1 Currency

Not surprisingly, Bitcoin (BTC) remains the dominant currency in the markets we observed, despite its poor anonymity properties and easy traceability. On the other hand, Monero (XMR) has become a popular choice due to it being significantly more anonymity-focused than Bitcoin [2,5]. In practice, Monero is considered the best choice by the dark web community. With Bitcoin, buyers and vendors are advised to use *mixers* to avoid tracking and enhance their anonymity [18,36]. There are many markets that offer a variety of options (i.e. two or more currencies) to provide flexibility for users and vendors. The market usually has a real-time exchange rate for currency conversion, even though most item prices are shown in US dollars. That means the buyer will pay the corresponding cryptocurrency according to the exchange rate. Additionally, Litecoin (LTC) and Tether (USTD) are also available in some markets, but in a very small percentage. Litecoin has the same anonymity features as Bitcoin, so next to zero, and using USDT in this context is clearly a mistake because USDT is controlled and tracked by a private institution. DAI, with its decentralised features would be a much better option than USDT, but both pale in comparison with Monero.

4.3.2 Transaction

In this study, we examine and describe three different transaction functions: *Multisig*, *Escrow*, and *Finalise early*. The market offers various transaction functions for vendors to select, allowing them to pick one (or more) that best fits their operations. Buyers can then select from the transaction functions supported by the vendors during trading.

Multisig, also known as multi-signature, refers to a transaction only made after being agreed upon by two or more parties. This method is quite attractive within the dark web community because of the extra security it provides, especially when it comes to avoiding market exit scams. Thanks to this, even if the market is closed, transactions can still be completed (as long as the buyer and vendors have another communication channel, which is usually a public dark web forum) if the items have been shipped. At the same time, when using this mechanism, the transaction funds do not need to go through the market's wallet address.

Escrow is the most basic transaction model, that is, the market acts as a somewhat trusted "third party" between buyers and vendors. Typically, buyers will need to deposit funds into the market's wallet first, which then will be reflected on the market's interface. After purchasing an item, the funds will still be held in the market wallet. When the buyer confirms that the item has been delivered, the market operator will release the funds to the vendor. At this time, the funds are still (possibly) in the market address, and the vendors need to withdraw them to their private address. Escrow seems to solve the trust issue between buyers and vendors relatively well, but introduces extra security risks due to the needed trust on the market operators, which frequently exit scam.

Finalise early refers to the common possibility that, once the buyer places an order, the funds could reach the vendor's wallet directly, even before the items have arrived. This process shortens the escrow time. On the other hand, this increases the risk of fraud to buyers by vendors. Therefore, the market usually only allows vendors with a certain reputation (or that pay a certain deposit to the market in advance) to enable this function. This mechanism is, in general, more beneficial to vendors than to buyers, because it ensures a faster turnover of funds and mitigates the impact of market exit scams.

4.4 Support and Complaints

At the core of dark web markets, a user support system capable of dealing effectively and efficiently with complaints is quite necessary. Every market has this mechanism where it acts as a middleman to resolve any disputes between buyers and vendors. The whole process is integrated with the market and is done on a case-by-case basis. In theory, data on dark web markets, including private messages related to support and complaints (as well as transaction details, customer information, etc.), is encrypted using one or more encryption algorithms. This is to protect their users and themselves from potential criminal evidence. But few markets have made any statement about this. Therefore, while this is implemented as a functional security mechanism, its technical security remains highly unclear.

5 Discussion

We see that, unsurprisingly, the actual implementation of security mechanisms is actually very relevant to almost every aspect of market operations. This is reasonable, as some users go to dark web markets with the intent of hiding their true identities, in order to conduct potential illegal activities without legal consequences. Market operators also know the importance of security mechanisms, and often build their infrastructure with security at its core.

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 describe the deployment of market-associated forums. Finally, we explain some ethical considerations that need to be taken into account in this line of research.

5.1 Interaction of Security Mechanisms on Market Closure

Dark web markets have always been very dynamic and full of potentially unknown features or quirks. We noted that three markets (i.e. *Royal Market*, *Tor2door Market* and *Vice City Market*) were closed at the time of writing the first draft (December 2023) of this work. Following on, when we were revising and extending this paper (August 2024), we noted two more markets (*Bohemia* and *Incognito*) were closed down. Wang et al. [35] mentioned that the closure of a dark web market has some correlation with the security issues of the market. The authors noticed that one reason why this correlation might exist is that markets are more prone to shut down definitely when under attack. Also, it is reasonable to expect that markets offering very poor levels of security can become low-hanging fruit for competitors and law enforcement.

For the first three markets with unknown reasons for closure (i.e. *Royal Market*, *Tor2door Market* and *Vice City Market*), a review of the security mechanisms listed in Table 2 suggests that relatively weak DDoS protection (either the lack of a waiting queue, or the use of weak CAPTCHAs, or both) could have been a contributing factor. This weakness would make them more prone to being disrupted by a third party. This would often result in the loss of data and trust, which in turn might encourage users to switch to competitor markets.

On the other hand, the implementation of security mechanisms reflects the operator's business philosophy, even though this may change at any time. In the *Bohemia* market, there was betrayal and division within the operations team. However, not long after (August 2024), the dark web community believed that law enforcement agencies arrested the administrator(s) based on a news report [7,25]. In the *Incognito* market, even more shocking to the dark web community, the market operators turned to extorting and blackmailing both users and vendors, claiming they had the on-site transaction details, shipment information, private messages, etc. The operators threatened to disclose them to authorities. Nevertheless, according to information from law enforcement agencies [31], the founder of the market was arrested a few months later.

From the perspective of dark web users and vendors, there are almost no security mechanisms to prevent or mitigate such events because the operators are the ones who implement those mechanisms. The rich security mechanisms implemented actually attract users and vendors to join. However, driven by the huge potential profits, the market almost always has its way and closes at a specific and maximally profitable time.

While our results may not be exhaustive, we believe the security mechanisms implemented by the market interact somehow with potential market closures. 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 [22,35].

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 its variations. There are many other types and variants of CAPTCHAs used on the dark web market, but we agree with their conclusions based in our experience and the data we collected. There is a trade-off here, after the time we spend in an effort to crack a given CAPTCHA, the market may no longer operate or change to new CAPTCHAs. This is why we need a general CAPTCHA solver based on AI, but we strongly believe the state of the art is very close to achieve this.

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 threads to run the crawler simultaneously. Nevertheless, very aggressive rate limiting settings can also affect access by real customers. 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.

In addition, and somewhat surprisingly, in our experience the use of I2P makes data collection easier. Tor's network performance can cause the market server to take significantly longer to respond than over the I2P network. When considering data collection, the crawler's downloader will require additional time to wait for the data to be downloaded locally [20]. Moreover, certain markets implement security mechanisms slightly differently on the Tor network than on I2P. For example, the *Bohemia* market on the I2P network does not use anti-phishing mechanisms although they do on the Tor network.

There may also 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 a simple API, we are able to pass larger parameters to this said 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 put more stress onto the server.

We also found that since JavaScript is generally not used on the dark web for security reasons (e.g., JavaScript can be used to execute some malicious code), the structure of the web page is simpler than those on the clear web (i.e. there is less dynamically loaded content).

5.3 Market-Associated Forums

Forums associated with dark web markets, though often overlooked, provide crucial platforms for users to report scams and receive important updates, boosting transparency and trust. They also boost market security through open communication, user feedback, and effective problem-solving.

Most markets have associated forums on *Dread* or in their own servers. Those *Dread*-based forums are usually moderated by market operators and often jointly moderated by *Dread* administrators. The purpose is to have a relatively open platform for exchanging information, which includes release announcements, promotions, feedback, complaints, etc. Since such *Dread*-based forums are not part of a specific market, feedback and complaints, for example, are more independent, or their purpose is to be a communication infrastructure with other users in the same market. A common example of this is when a user is treated unfairly by a vendor, the user could take to the forums to tell what happened to them and use it as a warning to other users. Additionally, when the market website goes down for various reasons, the market operators are able to issue announcements and solutions timely. Another example is when a market operator disappears (e.g., due to a scam exit or arrest), *Dread* administrators often come together with other users to discuss the matter, verify possible truths, and mitigate losses.

The other type of forum is internal to the market and is therefore owned and moderated by the market operators. Some markets also have *Telegram* group chats, which are moderated by the market administrators, even though it is no longer considered a traditional dark web scope.

5.4 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.

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 the University of Kent'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[7]. 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 the other party, and further promote understanding of the dark web area.

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 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 though we would not be surprised if soon enough this can be automated.

Our results reveal that the security mechanisms implemented by mainstream dark web markets include web security, account security and financial 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/seed phrases, MFA, account kill-switch. Financial security includes the choice of (crypto)currency being used, specific transaction functions such as multi-signature, escrow and finalise early, as well as support and complaints handling. We also discuss how security mechanisms being implemented (or not) by market operators may reflect the operators' business philosophy (for instance, whether they plan to stay long in the business). We share some insights regarding data collection and the key challenges associated with it. We also describe the deployment of market-related forums and the roles they play. Finally, we discuss some 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 markets and design crawlers for data collection in a more targeted manner. Moreover, a better and more detailed understanding of how rate limiting works may greatly improve the efficiency of crawlers and reduce manual labour. There are promising signs that we will soon be able to use a collection of scripts that can universally solve the kind of CAPTCHAs encountered in dark markets, which will be a very useful breakthrough. It is envisaged that machine learning techniques can be used to solve them quite easily in the near 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.

[7] https://owasp.org/www-project-top-ten

Conflict/Competing Interest

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). In particular, Y.W. received travel funding to present the original paper at the 2024 European Interdisciplinary Cybersecurity Conference (EICC '24). B.A. and Y.W. are colleagues of one of the Special Issue Editors (S.L.), while J.H-C. is a former colleague of S.L. Additionally, B.A. collaborated with one of the other Special Issue Editors (M.S.) as Programme Committee Co-Chairs of a conference in 2023.

References

1. Audran, D., Andersen, M., Hansen, M., Andersen, M., Frederiksen, T., Hansen, K., Georgoulias, D., Vasilomanolakis, E.: Tick tock break the clock: Breaking captchas on the darkweb. In: Proceedings of the 19th International Conference on Security and Cryptography - SECRYPT, pp. 357–365. INSTICC, SciTePress, Lisbon, Portugal (2022). URL https://www.scitepress.org/PublishedPapers/2022/112733/112733.pdf
2. Ben Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M.: Zerocash: Decentralized anonymous payments from bitcoin. In: 2014 IEEE Symposium on Security and Privacy, pp. 459–474 (2014). URL https://doi.org/10.1109/SP.2014.36
3. Bergman, J., Popov, O.B.: Exploring dark web crawlers: a systematic literature review of dark web crawlers and their implementation. IEEE Access **11**, 35,914–35,933 (2023). URL https://doi.org/10.1109/ACCESS.2023.3255165
4. Bhalerao, R., Aliapoulios, M., Shumailov, I., Afroz, S., McCoy, D.: Mapping the underground: Supervised discovery of cybercrime supply chains. In: 2019 APWG Symposium on Electronic Crime Research (eCrime), pp. 1–16. IEEE, Pittsburgh, PA, USA (2019). URL https://doi.org/10.1109/eCrime47957.2019.9037582
5. Biryukov, A., Khovratovich, D., Pustogarov, I.: Deanonymisation of clients in bitcoin p2p network. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, CCS '14, pp. 15—-29. Association for Computing Machinery, New York, NY, USA (2014). URL https://doi.org/10.1145/2660267.2660379

6. Bracci, A., Nadini, M., Aliapoulios, M., McCoy, D., Gray, I., Teytelboym, A., Gallo, A., Baronchelli, A.: Dark web marketplaces and covid-19: before the vaccine. EPJ data science **10**(1), 6 (2021). URL https://doi.org/10.1140/epjds/s13688-021-00259-w
7. Burnhill, E.: Man charged with money laundering of cryptocurrencies (2024). URL https://www.rte.ie/news/ireland/2024/0808/1463995-cryptocurrencies/
8. Campobasso, M., Allodi, L.: 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), pp. 1–13. IEEE, Boston, MA, USA (2022). URL https://doi.org/10.1109/eCrime57793.2022.10142081
9. Christin, N.: Traveling the silk road: A measurement analysis of a large anonymous online marketplace. In: Proceedings of the 22nd International Conference on World Wide Web, WWW '13, pp. 213–224. Association for Computing Machinery, New York, NY, USA (2013). URL https://doi.org/10.1145/2488388.2488408
10. Conrad, B., Shirazi, F.: A survey on tor and i2p. In: Ninth International Conference on Internet Monitoring and Protection (ICIMP2014), pp. 22–28 (2014). URL http://i2p2.de/_static/pdf/icimp_2014_1_40_30015.pdf
11. Copeland, C., Wallin, M., Holt, T.J.: Assessing the practices and products of darkweb firearm vendors. Deviant Behavior **41**(8), 949–968 (2020). URL https://doi.org/10.1080/01639625.2019.1596465
12. David, B., Delong, M., Filiol, E.: Detection of crawler traps: formalization and implementation—defeating protection on internet and on the tor network. Journal of Computer Virology and Hacking Techniques **17**(3), 185–198 (2021). URL https://doi.org/10.1007/s11416-021-00380-4
13. Ehlert, M.: I2p usability vs. tor usability a bandwidth and latency comparison. In: Seminar Report, Humboldt University of Berlin, pp. 129–134 (2011). URL https://www.freehaven.net/anonbib/cache/ehlert2011:usability-comparison-i2p-tor.pdf
14. ElBahrawy, A., Alessandretti, L., Rusnac, L., Goldsmith, D., Teytelboym, A., Baronchelli, A.: Collective dynamics of dark web marketplaces. Scientific reports **10**(1), 1–8 (2020). URL https://doi.org/10.1038/s41598-020-74416-y
15. Europol: 288 dark web vendors arrested in major marketplace seizure (2023). URL https://www.europol.europa.eu/media-press/newsroom/news/288-dark-web-vendors-arrested-in-major-marketplace-seizure
16. Europol: Internet organised crime assessment (iocta) 2023 (2023). URL https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf
17. Gatlan, S.: Tor and i2p networks hit by wave of ongoing ddos attacks (2023). URL https://www.bleepingcomputer.com/news/security/tor-and-i2p-networks-hit-by-wave-of-ongoing-ddos-attacks/
18. Georgoulias, D., Pedersen, J.M., Falch, M., Vasilomanolakis, E.: A qualitative mapping of darkweb marketplaces. In: 2021 APWG Symposium on Electronic Crime Research (eCrime), pp. 1–15. IEEE, Boston, MA, USA (2021). URL https://doi.org/10.1109/eCrime54498.2021.9738766
19. Georgoulias, D., Pedersen, J.M., Falch, M., Vasilomanolakis, E.: Botnet business models, takedown attempts, and the darkweb market: A survey. ACM Comput. Surv. **55**(11) (2023). URL https://doi.org/10.1145/3575808
20. Georgoulias, D., Yaben, R., Vasilomanolakis, E.: 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, ARES '23. Association for Computing Machinery, New York, NY, USA (2023). URL https://doi.org/10.1145/3600160.3605012
21. Güldenring, B., Roth, V.: Protecting onion service users against phishing. arXiv preprint arXiv:2408.07787 (2024). URL https://doi.org/10.48550/arXiv.2408.07787
22. Hutchings, A., Clayton, R., Anderson, R.: Taking down websites to prevent crime. In: 2016 APWG Symposium on Electronic Crime Research (eCrime), pp. 1–10. IEEE, Toronto, ON, Canada (2016). URL https://doi.org/10.1109/ECRIME.2016.7487947
23. Kermitsis, E., Kavallieros, D., Myttas, D., Lissaris, E., Giataganas, G.: Dark Web Markets, pp. 85–118. Springer International Publishing, Cham (2021). URL https://doi.org/10.1007/978-3-030-55343-2_4
24. Labrador, V., Pastrana, S.: Examining the trends and operations of modern dark-web marketplaces. In: 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 163–172. IEEE, Genoa, Italy (2022). URL https://doi.org/10.1109/EuroSPW55150.2022.00022
25. Moore, A.: Man charged over €6.5m cryptocurrency seizure in dublin (2024). URL https://www.bbc.co.uk/news/articles/cql3vx15e2wo
26. National Crime Agency: Child sexual abuse and exploitation (2023). URL https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/child-sexual-abuse-and-exploitation
27. Pastrana, S., Hutchings, A., Caines, A., Buttery, P.: Characterizing eve: Analysing cybercrime actors in a large underground forum. In: Research in Attacks, Intrusions, and Defenses, pp. 207–227. Springer International Publishing, Cham (2018). URL https://doi.org/10.1007/978-3-030-00470-5_10
28. Tidy, J.: Hydra: How german police dismantled russian darknet site (2022). URL https://www.bbc.co.uk/news/technology-61002904
29. Tor Project: Network ddos (2023). URL https://status.torproject.org/issues/2022-06-09-network-ddos/
30. Turk, K., Pastrana, S., Collier, B.: 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), pp. 428–437. IEEE, Genoa, Italy (2020). URL https://doi.org/10.1109/EuroSPW51379.2020.00064
31. U.S. Attorney's Office: "incognito market"' owner arrested for operating one of the largest illegal narcotics marketplaces on the internet (2024). URL https://www.justice.gov/usao-sdny/pr/incognito-market-owner-arrested-operating-one-largest-illegal-narcotics-marketplaces
32. Van Wegberg, R., Tajalizadehkhoob, S., Soska, K., Akyazi, U., Gañán, C., Klievink, B., Christin, N., Van Eeten, M.: Plug and prey? measuring the commoditization of cybercrime via online anonymous markets. In: Proceedings of the 27th USENIX Conference on Security Symposium, SEC'18, pp. 1009–1026. USENIX Association, USA (2018). URL https://www.usenix.org/syste

m/files/conference/usenixsecurity18/sec18-van_weg berg.pdf
33. Wang, Y., Arief, B., Franqueira, V.N.L., Coates, A.G., Ó Ciardha, C.: 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, EICC '23, pp. 59–64. Association for Computing Machinery, New York, NY, USA (2023). URL https://doi.org/10.1145/3590777.3590812
34. Wang, Y., Arief, B., Hernandez-Castro, J.: Toad in the Hole or Mapo Tofu? Comparative Analysis of English and Chinese Darknet Markets. In: 2021 APWG Symposium on Electronic Crime Research (eCrime), pp. 1–13. IEEE, IEEE, Boston, MA, USA (2021). URL https://doi.org/10.1109/eCrime54498.2021.9738745
35. Wang, Y., Arief, B., Hernandez-Castro, J.: 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, pp. 106–117. INSTICC, SciTePress, Lisbon, Portugal (2023). URL https://doi.org/10.5220/0011681600003405
36. Wu, L., Hu, Y., Zhou, Y., Wang, H., Luo, X., Wang, Z., Zhang, F., Ren, K.: Towards understanding and demystifying bitcoin mixing services. In: Proceedings of the Web Conference 2021, WWW '21, p. 33–44. Association for Computing Machinery, New York, NY, USA (2021). URL https://doi.org/10.1145/3442381.3449880
37. Yannikos, Y., Heeger, J., Steinebach, M.: Data acquisition on a large darknet marketplace. In: Proceedings of the 17th International Conference on Availability, Reliability and Security, ARES '22. ACM, New York, NY, USA (2022). URL https://doi.org/10.1145/3538969.3544472
38. Yoon, C., Kim, K., Kim, Y., Shin, S., Son, S.: Doppelgängers on the dark web: A large-scale assessment on phishing hidden web services. In: The World Wide Web Conference, WWW '19, p. 2225–2235. Association for Computing Machinery, New York, NY, USA (2019). URL https://doi.org/10.1145/3308558.3313551