Dark Ending: What Happens when a Dark Web Market Closes down

Yichao Wang[a], Budi Arief[b] and Julio Hernandez-Castro[c]
Institute of Cyber Security for Society (iCSS) & School of Computing, University of Kent, U.K.

Keywords: Cybercrime, Dark Web, Anonymous Online Markets, Data Collection, Rug Pull, Exit Scam, Closing-down, Take-down.

Abstract: As the economic hubs of (potentially) illegal transactions, dark web markets are fraught with uncertainty, including their ending. The ending of a dark web market can bring disruption to the stakeholders involved, especially vendors and buyers. Most importantly, there is a growing concern that such an ending can cause financial repercussions or even fraud victimisation. At the moment, there is scant published work about how, why or when dark web markets would end. We aim to fill this gap to help the academic and security research communities to reflect on what would typically happen to dark web markets in their final days. We used crawling and data scraping techniques to gather relevant weekly data from six dark web markets over a span of several months, right up to their closure. We then analysed the data to find common characteristics and predictive features leading to the closure of these markets. We found three main reasons for the ending of dark web markets: (i) exit scam, (ii) voluntary closure, or (iii) taken down by Law Enforcement Agencies (LEAs). We also gained further insights by analysing our data more closely. For instance, markets are most likely to be closed down when they are most visible, when they are under attack or when they are growing rapidly to their peak. In particular, more mature markets (i.e. markets that have been in operation for a long period of time) are more likely to disappear when their economic patterns start to change (for example, there might be a rapid growth or a sudden – or even gradual, but noticeable – economic decline). When a market was closed down, vendors and buyers would typically move on quickly to other alternative markets – which might grow rapidly as a result – and in turn, those alternative markets' risk of being closed down would become higher. Whether a market is still accepting new vendors (or not) appears to be a valuable indicator for predicting the market's next move. These insights can be useful in anticipating potential market closure, so that sufficient warning can be provided to avoid people being victimised.

1 INTRODUCTION

Dark web markets are one of the main economic hubs of illegal online activity. Similar to the legitimate online markets, as time goes by, some dark web markets flourish, some wither, new ones are opened and some close down. However, unlike legitimate online markets, the ending of dark web markets is usually unannounced, difficult to predict, and frequently shrouded in mystery. At times, even disinformation might take place. This opens up an interesting challenge for cybercrime researchers, and we try to address this through the work presented in this paper.

There have been several instances of high-profile dark web markets being closed down. For example, *Hydra*, a Russian-language dark web market, was shut down by law enforcement agencies (LEAs) on April 5, 2022 (Tidy, 2022). The LEAs involved in this operation have indicated that, even after shutting down the servers and confiscating around €23 million in Bitcoin, they fear this will not end the *Hydra* cybercrime gang, as it has proved quite difficult to identify who was behind it (Tidy, 2022).

Apart from LEA operations, most closures are referred to as "exit scams", in which the market operators chose to close the market without prior notice, thus stealing any funds in temporary escrow from both vendors and buyers. In 2020, for example, the operators of the largest dark web market at the time, *Empire Market*, performed an exit scam and got away with around $30 million in Bitcoin (Redman, 2020).

In rare occurrences, the operators would "gracefully" close down the market, i.e. they would inform all customers in advance, allowing extra time for on-

[a] https://orcid.org/0000-0002-4633-3690
[b] https://orcid.org/0000-0002-1830-1587
[c] https://orcid.org/0000-0002-6432-5328

Wang, Y., Arief, B. and Hernandez-Castro, J.
Dark Ending: What Happens when a Dark Web Market Closes down.
DOI: 10.5220/0011681600003405
In *Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP 2023)*, pages 106-117
ISBN: 978-989-758-624-8; ISSN: 2184-4356

going orders to be completed and any remaining funds to be transferred to the appropriate parties. In 2021, *White House Market* did just that, via an announcement on their website stating that the project had already reached their goal and that they were retiring as planned (WIRED, 2021). The market operator immediately stopped the registration of new users, and they ceased to accept new orders on the site. They finally closed the site down after existing vendors fulfilled their open orders.

Nevertheless, new markets steadily appear to compete with existing ones – and to replace closed-down ones. We may never know whether the same people behind the existing or closed-down markets are running those new ones. For instance, an operator that previously performed an exit scam could launch another market with the same objective of exit scamming. In contrast, those operators that closed down their old market gracefully might transfer the reputation and skills they have built up to the new market.

Previous studies have investigated various aspects of dark web markets, but to our knowledge, none has specifically focused on the data collection and analysis of how, why or when dark web markets closed down. Thus, it is important to dig further into the ending phase of dark web markets, not only to improve our understanding, but also to help reduce the risk of people getting exit scammed, and to assist LEAs in securing evidence before these markets disappear.

While previous work has examined user records of bitcoin transactions to analyse the unexpected closure of dark web markets (Labrador and Pastrana, 2022), our work collected data directly from six markets and their associated forums due to the trend of not using Bitcoin (Monero instead) in existing dark web markets. By including multiple markets, we aim to increase the breadth of our understanding. This will also allow us to conduct meaningful comparisons among various instances of closed-down dark web markets, which can lead to more useful insights.

As such, the study presented in this paper aims to *understand what typically would happen before and after the closing down of dark web markets*, and *whether they have any common characteristics*. If we were able to identify some common features, we would also like to know *whether we can use these to predict whether a market is about to close down*.

Contributions. We collected datasets from six recently closed-down dark web markets and five of their associated forums in *Dread* (a dark web version of *Reddit*). Through data analysis and in-depth investigation, we classified the ending of dark web markets into three categories: *exit scams*, *voluntary closures*, and *taken down by LEAs*. We tracked some indicators and came out with insights into dark web market development and life-cycle, which we hope will be useful for future investigations.

The rest of the paper is organised as follows. First, we dissect and discuss existing relevant papers on the dark web in Section 2. We explain our method and approach in Section 3. We present our results in Section 4, while we discuss the implications of such results, along with the limitations of our study and future work in Section 5. We summarise our findings and remarks in Section 6.

2 RELATED WORK

With the rapid growth of technology over the years – including the popularity of cryptocurrencies, and privacy protection technologies such as The Onion Router (Tor) (Dingledine et al., 2004) – the dark web market has become a new platform for cybercriminals (Weber and Kruisbergen, 2019). In earlier years, researchers proposed systems for obtaining security intelligence in the dark web to gather warnings of cyber threats (Nunes et al., 2016). LEAs are also aware of the dark web's impact on the drug trade and have conducted preliminary research on it (European Monitoring Centre for Drugs and Drug Addiction, 2020).

Previous studies have covered many aspects of the dark web markets. In 2013, a study on the very famous dark web market called *Silk Road*, was comprehensively conducted (Christin, 2013). The paper found that most of the items sold were available for less than three weeks, and that most vendors disappeared within about three months of joining the market. Similarly, another study analysed 16 different dark web markets of their ecosystem over more than two years (Soska and Christin, 2015). This study found that the closure of *Silk Road* did not lead to the demise of the dark web as a form of commerce, but rather, inspired the development of an entire ecosystem of dark web markets. Georgoulias et al. looked into a mapping of dark web markets through qualitative methods covering 41 markets and 35 vendor shops (Georgoulias et al., 2021). Some studies also investigated a range of dark web markets in different languages for comparison and analysis (Bhalerao et al., 2019; Wang et al., 2021), highlighting the rapid, diverse dynamics of the dark web markets' uptake and internationalisation. All of these studies suggest that the dark web markets are an important part of the underground economy.

The *European Monitoring Centre for Drugs and Drug Addiction* and *Europol* published a poster in 2018 indicating the lifetimes and reasons for the clo-

sure of more than 100 dark web markets that offer drugs around the world (EMCDDA, 2018). The results showed that 13 markets were operating for one to two years. Nine markets were in operation for two to three years, while 14 were still active at the end of the study. Moreover, the poster shows that since 2016, dark web markets have become longer-lived than ever, i.e. mostly over one year. Similarly, Branwen also maintains a table to count the number of closed-down markets, last updated in 2019, but the market information is somewhat outdated (Branwen, 2019).

In 2015, *DeepDotWeb* interviewed the administrators of some of the then-active dark web markets, in order to gain their views on the state of the dark web market at that time (DeepDotWeb, 2015a; DeepDotWeb, 2015c; DeepDotWeb, 2015b). The administrator of *AlphaBay* mentioned that when other markets exit-scammed, trading continued anyway, so many vendors and buyers would move to alternative markets. This was reflected in the growth in the number of users, posts and transactions after the closure of a particular market. *TheRealDeal* was forced to close due to the arrest of some of the operators of the operation team, but relaunched after a period of time. Moreover, *Aurora Market* administrators said in a *DarkNetDaily* interview that greedy administrators would run away with three to five million in around five months (DarkNetDaily.com, 2021). Ironically, this market did an exit scam after about three months.

ElBahrawy et al. investigated how the dark web market ecosystem was affected by unexpected market closures between 2013 and 2019 (ElBahrawy et al., 2020). Their research is based on a dataset of Bitcoin transactions from 31 major dark web markets, 24 of which were closed down by scams or police raids. They also noted rapid migration following market closures, which mainly affected smaller vendors.

More recently, Labrador and Pastrana referred to a case study of market closure in their paper. They analysed the trends in prices and volumes of products in the period leading up to the closure (Labrador and Pastrana, 2022). They also mentioned the Distributed Denial of Service (DDoS) attack that preceded the closure of this market and possibly affected the economics of the market – causing prices to fall while losing trust from buyers – leading to the closure of the market. This study is quite similar to our study, however we enrich our dataset to provide a more comprehensive analysis of data prior to market closure, including the analysis of six markets – rather than only one market.

In terms of datasets, we found that most of the publicly available datasets are outdated. *Darknet market archives* (Branwen et al., 2015) and *AZSecure-data* (Alsayra, 2015) are two of the most comprehensive datasets of the past. The former contains data from 89 markets and over 37 relevant forums from 2013 to 2015. The latter offers *Dream Market* dataset from 2016 until 2017, which contains details of listed items. The dataset from the Cambridge Cybercrime Centre (Pastrana et al., 2018) is still being maintained and updated nowadays. It contains several underground forums on both the surface and the dark web, including more than 48 million posts, 4.5 million threads and 1 million accounts. Additionally, Noroozian et al. conducted a study with data from LEAs (Noroozian et al., 2019), which allowed the study to have more comprehensive and accurate data, as the authorities seized entire server backends.

Table 1: Reasons for the closure of 21 major dark web markets since September 2019.

Market Names	Reasons	Closure
Apollon Market	Exit scam	2020-01
Aurora Market	Exit scam	2021-04
BitBazaar	Exit scam	2020-07
Cartel Marketplace	Exit scam	2021-12
Dark0de Reborn	Exit scam	2022-02
Empire Market	Exit scam	2020-08
Grey Market	Exit scam	2019-12
Silk Road 3.1	Exit scam	2020-07
World Market	Exit scam	2022-03
Yellow Brick Market	Exit scam	2021-01
CannaHome Market	Voluntary closure	2022-04
Cannazon Market	Voluntary closure	2021-11
Dream Market	Voluntary closure	2019-04
The Versus Project	Voluntary closure	2022-05
ToRReZ Market	Voluntary closure	2021-12
White House Market	Voluntary closure	2021-10
Big Blue Market	Taken down by LEAs	2021-04
CanadaHQ	Taken down by LEAs	2022-01
Dark Market	Taken down by LEAs	2021-01
Hydra Market	Taken down by LEAs	2022-04
Monopoly Market	Taken down by LEAs	2021-12

Data collection on the dark web is considered to be challenging due to the fact that most dark web markets and forums apply different levels of security mechanisms against crawlers (Yannikos et al., 2022; Turk et al., 2020). As the development and evolution of the dark web are rapid and unpredictable, we decided to collect our own dataset over a long period of time. For this paper, we selected recently closed-down markets in our dataset to base our study on.

3 METHODOLOGY

This section explains our approach, mainly covering the data collection process and the ethical considerations. We also describe the crawling strategy of our

custom crawler software, and provide an overview of our datasets[1].

3.1 Approach

In order to understand what happened before and after the dark web markets being closed down, we collected data weekly[2], and analysed data from six dark web markets over a period of time before they closed. These six dark web markets are *Cartel Marketplace, Dark0de Reborn, The Versus Project, White House Market, Monopoly Market,* and *Tea Horse Road*. We also collected data from five of their associated forums in *Dread*. The data from forums are only collected once as those forums have been marked as archived, which means no new threads would be made after the archived date (usually a few days after the associated market being closed down).

Cartel Marketplace, Dark0de Reborn, The Versus Project, White House Market and *Tea Horse Road* are comprehensive markets where drugs, fraud-related material, stolen data and ransomware are all listed. All of these markets use some sort of escrow mechanism to maintain the operation of the market. *Monopoly Market* was promoted as a wallet-less and drug-focused market. Nevertheless, it seems that direct payment to vendors is only available to a select group of vendors with a good reputation (Darknetlive, 2022).

We categorised these six markets into three categories based on the different endings in which they were closed down. The criteria used to determine the category of each market are based on publicly available information. For reference, we roughly counted the reasons and time for the closure of major markets since September 2019, including 21 markets in English. Ten of them were considered exit scam, six voluntarily closed down, while five were raided by LEAs, as shown in Table 1. Due to the timing of this study and other limitations, we have only got data from six markets.

Dark0de Reborn and *Cartel Marketplace* shut down their sites and deleted the administrator's accounts on the forum without any prior notice. With some users complaining on the forums and no statement from the LEAs, we believe this is a classic exit scam. Voluntary closures include two markets, which are the *Versus Project* and the *White House Market*. The former chose to retire due to potential security concerns, and the operator sent private links to the vendors to access the market to complete transactions. The latter announced its retirement in a post on the website and immediately stopped accepting new orders. The admins claimed that the public link to the site would no longer work after all orders were completed. *Tea Horse Road* was a Chinese dark web market. A few months after its abrupt closure, screenshots of its home page appeared in reports about the fight against cybercrime. It is therefore identified as having been shut down by the LEAs. Similarly, the reason for the closure of *Monopoly* was due to the servers being seized, as claimed by the operator of *dark.fail*[3]. However, no one can verify the accuracy of the information as the LEA did not issue any statement. In this paper, we still classify it as taken down by the LEAs.

Smaller markets may not be very active in forums, but operators may introduce "cross-posts" to keep the market buzzing. The forums in *Dread* allow "cross-post", which means there are threads that can appear in one or more forums. For example, someone may post a review about a vendor in */d/review*, which can later be re-shared in */d/versus* as well. Therefore, when calculating the number, we count all the data in the forum, i.e. including the "cross-posts". We then comb through the results to find more meaningful insights, such as how users shift between markets and discuss them.

3.2 Data Collection

We used Python with both the Scrapy web-crawling framework (Kouzis-Loukas, 2016) and the Selenium suite of tools (Software Freedom Conservancy, 2022) to implement our own custom crawler. Benefiting from Selenium's ability to handle sessions automatically, our crawler can deal with the use of dynamic cookies in certain markets (i.e. each request would apply a new cookie based on the previous request). Our crawler employs two strategies to collect data in dark web markets:

- In situations where the site's security mechanisms would allow crawlers to operate at higher speeds with no restrictions – i.e. the site's sessions would not (or rarely) expire after a certain time, as long as the crawler keeps interacting with the site – our crawler would access and collect the details of each product through the listing page.

[1]Due to the potentially criminal content of the datasets, we had to choose an appropriate and ethical way to share them. We are happy to share our datasets with the academic community, security researchers and LEAs. Please contact the authors for further information.

[2]Some weeks' data may not be collected for unexpected circumstances, such as server downtime, crawler errors or personal reasons.

[3]https://twitter.com/darkdotfail

Table 2: A summary of the datasets obtained. *This market does not have a forum in *Dread*.

Market Names	Dates Covered (from/to)	# snap.	#Dread Threads	Size
Cartel Marketplace	2021-03-29/2021-12-20	38	701	352.3 MB
Dark0de Reborn	2021-04-06/2022-02-21	46	4976	542.1 MB
The Versus Project	2021-10-26/2022-05-16	31	3713	5.3 GB
White House Market	2021-05-17/2021-10-11	21	8793	315.0 MB
Monopoly Market	2021-10-18/2021-12-27	11	599	658.4 MB
Tea Horse Road	2021-07-27/2021-11-16	16	N/A*	117.8 MB

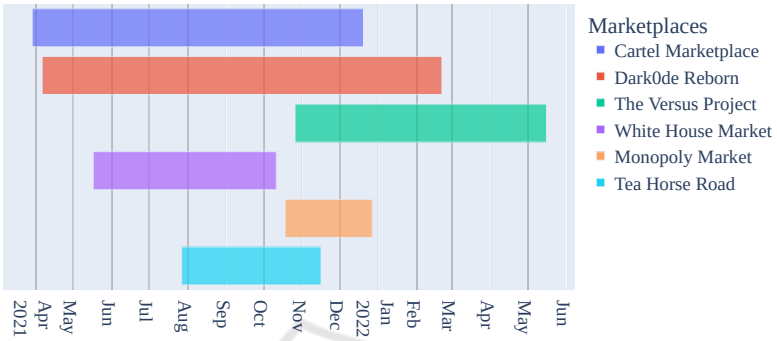


Figure 1: The time period of the data collection for each of the six dark web markets observed.

- In situations where the site would apply a strict security mechanism – whereby the session would expire after a specific number of requests, and then a CAPTCHA would be enforced – we tried to use multiple accounts to crawl in parallel and did our best to get statistical data other than text.

Our crawler is deployed in password-encrypted virtual machines to prevent data from being infected or compromised. VPN connection is used as an additional layer of protection. Since Scrapy cannot directly proxy to the Tor network using HTTP, Privoxy (Privoxy Developers, 2022) is needed as a relay to exchange the SOCKS5 and HTTP requests. When the weekly data collection is completed, we save the encrypted data to an offline portable hard drive.

Figure 1 shows the timeline for our data collection for different dark web markets. The start time of collection varies for each market, but the end time is the last time it is accessible. During these periods we obtained data once a week, so we could analyse the differences over time. For the *Dread* data, they were collected once on 14 August 2022, as those forums have been marked as archived. Table 2 provides information on the dataset obtained for each market. Table 3 shows some of the basic characteristics of the markets observed. In the dataset, we note that some markets use the Euro to display prices, and some use the US Dollar. Given the volatility of exchange rates, we have not converted them as the analysis of trends is limited to within individual markets. Still, we do make high-level comparisons based on trends in individual markets.

3.3 Ethical Considerations

Since we had to collect data on the dark web (the Tor network), and the data can potentially be related to cybercrime activities, we had to be very careful in dealing with the ethical issues of our research.

Our datasets contain items such as product information and discussions from the dark web markets and their associated forums, which are inherently public and easily accessible to the public. Nonetheless, we did not collect personally identifiable information. During data collection, we applied dynamic delays to our crawler, in order to prevent additional server stress to the observed sites (i.e. we did not want to disrupt or interfere with their operation).

The ethics of this study has been reviewed and approved by our university's research ethics committee.

4 RESULTS

In this section, we categorized six markets into three categories based on the different endings in which they were closed down. We describe some of the key things that happened before the closure, and also try to analyse different indicators depending on the availability of the data.

Table 3: A summary of the observed dark web markets.

Market Names	First Seen	Last Seen	Lifetime	#Vendors
Cartel Marketplace	2020-06	2021-12	18 Months	237
Dark0de Reborn	2020-05	2022-02	21 Months	2640
The Versus Project	2019-08	2022-05	33 Months	937
White House Market	2019-08	2021-10	26 Months	3450
Monopoly Market	2019-07	2021-12	29 Months	162
Tea Horse Road	2020-04	2021-11	19 Months	3275

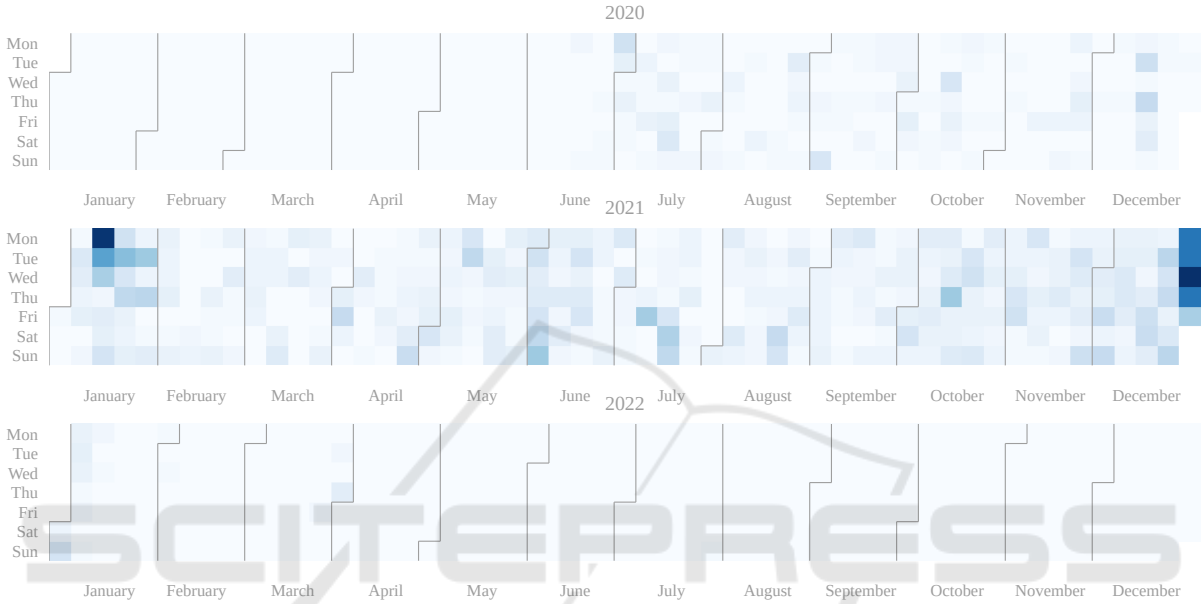


Figure 2: A heat map of the number of comments in the *Cartel Marketplace Dread* forum (darker colours mean higher numbers).

4.1 Exit Scams

Exit scams appear to be the most common type of closure, where the operator closes the site without any notice and takes all of the user's funds in their wallet. This happens when markets operate with escrow mechanisms. The escrow mechanism means that the market is a third party for vendors and buyers. The buyer deposits a certain amount of money into a cryptocurrency wallet provided by the market, and the fund is only released to the vendor's wallet when the transaction is completed.

Cartel Marketplace was launched in June 2020 and closed down in December 2021. The lifetime is about 18 months. Figure 2 shows the number of posts in the *Cartel Marketplace* sub-forum. In January 2021, that actually had an official announcement from *Dread* dominating the discussion. At the same time, there were plenty of advertisements from *Cartel* operators to attract new vendors and users. December 2021 is the month when the market closes and disappears. The problem was first identified on the 21st of December, when the market was suspected to be under DDoS attacks and down for a few hours. Users also started asking in the forums for a time for the market to return. On the 24th, probably the last appearance of the market operator. On the 29th, the forum administrator announced the market had been exit scammed, as the market operator did not reappear again, and the market website had not been online since the 21st.

Dark0de Reborn was launched in May 2020 and closed down in February 2022. The lifetime is about 21 months. Almost the same thing happens in this market. With the DDoS attack at the beginning of the month, it seemed they had the ability to bring the site back to normal. When the end of the month came, the operators disappeared. Unlike *Cartel Marketplace*, we did not observe many complaints, but people moved quickly to other alternative markets.

Figure 3 shows the number of listings and vendors in both markets, which keep increasing overall. An exception is in the number of listings in the *Cartel Marketplace*. The number peaked in September

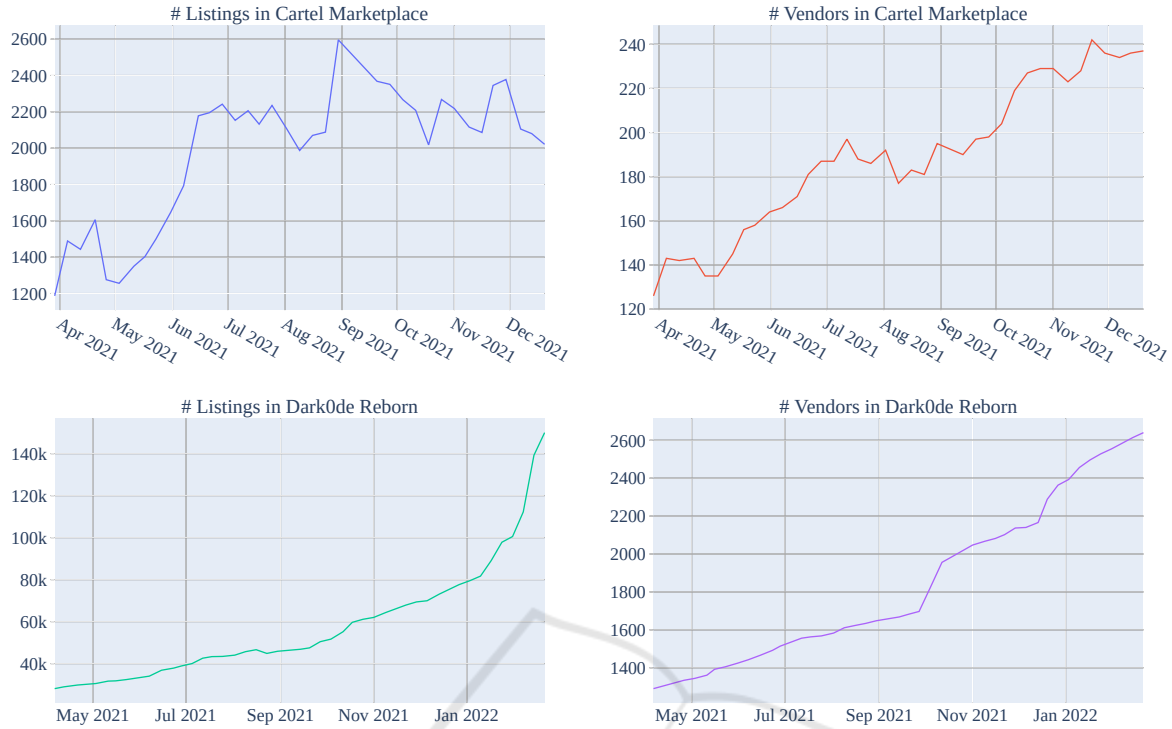
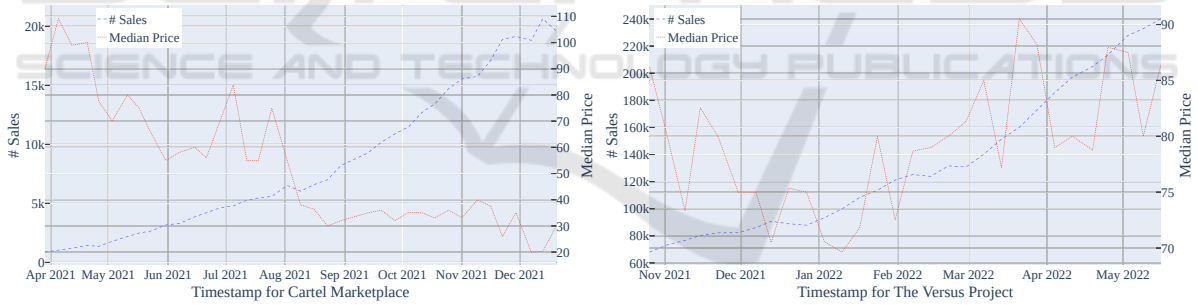


Figure 3: The number of listings in the *Cartel Marketplace* (top left), the number of vendors in the *Cartel Marketplace* (top right), the number of listings in the *Dark0de Reborn* (bottom left), and the number of vendors in *Dark0de Reborn* (bottom right).



(a) Median price and number of sales in *Cartel Marketplace*.

(b) Median price and number of sales in *Versus Project*.

Figure 4: Median price and number of sales comparison in two markets with different exit types.

2021, and then it started to decline. However, we did not find any interesting factors that could affect the number, and it was very quiet in the forum instead. In October, *Cartel Marketplace* operators began advertising for the recruitment of new vendors, while the closure of *White House Market* led some to transfer to this market, which is reflected in the growth of the charts. Therefore, we suspect that the drop in figures may be due to a small number of "dishonest" vendors (or "rippers" called in dark web communities) being banned from the market.

Interestingly, vendor numbers rose rapidly about two months before the *Dark0de* market closed. However, this was seemingly due to the closure of other markets leading to vendors changing places. In addition to *Cartel Marketplace*, another larger market closed at that time. Similarly, the closure of the *White House Market* is reflected in the increase in vendor numbers at the end of September and the beginning of October. It was also from this time (about four months before the market closed) that the discussion volume on the forum increased rapidly.

On the economic side, we have tried to analyse the median price and number of sales of the *Car-*

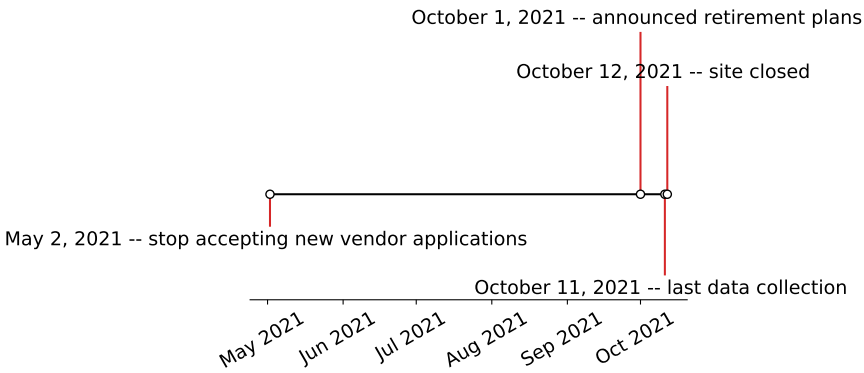


Figure 5: Key events occurring in the *White House Market* before it was closed down.

tel Marketplace in Figure 4. The number of sales has maintained consistent growth. The median price maintained a downward trend. In particular, median prices fell rapidly in August, and listings numbers did improve at that time, which should have influenced the overall results. It is worth noting that its median price fell again in the final weeks of the *Cartel Marketplace*. Interestingly, a vendor claimed the market operators have secretly revised stock quantities and reduced the prices of productions in the back end of the server. This behaviour is considered profitable for the market operators, as attracting more orders means more funds go into the market wallet (due to the application of escrow mechanisms in the market).

4.2 Voluntary Closures

Voluntary closures are usually a "win-win" for users and operators, which inform all customers in advance and allow extra time for ongoing orders to be completed. However, although this ending is usually less common in the past, it happens more frequently nowadays.

White House Market was launched in August 2019 and closed down in October 2021. The lifetime is about 26 months. Figure 5 shows the timeline of some key events before the market's closure. The market first announced in early May 2021 that it would no longer accept new vendors. On 1st October 2021, the market owners claimed their retirement, i.e. a voluntary closure of the market. We were allowed to access the site for the last time on the 11th, and then the site was shut down on the 12th. It took about 12 days from the announcement to the market's closing. Everything looks graceful from an observer's point of view, yet the truth could be different. On the same day that the market was closed, many vendors and users complained they did not get their coins back. These people have lost money either due to open orders or open disputes. Therefore, the forum's administrators marked the market as a dishonourable exit.

A different story took place in another market. The *Versus Project* was launched in August 2019 and closed down in May 2022. The lifetime is about 33 months. On 5th May 2022, the market operators claimed to have transformed the market into an invite-only community to maintain the quality of support, including invite-only vendors and invite-only buyers. Over the next few days, other forums appeared to discuss a major security breach in the market. Finally, in a statement dated 22nd May 2022, the operator described the fact that the market had a security breach and decided to close the market down. Unlike *White House Market*, the administrator did not disappear from the forum after the website was closed directly. Instead, after about four weeks, market administrators announced a link to complete all transactions.

The number of listings in both markets is growing steadily. The number of vendors in the *Versus Project* market has also continued to grow without many surprises. Figure 4 shows the median price and number of sales in the *Versus Project*. It should be noted that the currency unit of the price is EUR. Sales volumes are steadily increasing, but there are fluctuations in the median price. The median price is in a downward trend from November 2021 to January 2022, and then begins to rise until mid-March 2022. Sales also increased faster at that time, which may be the possibility that *Dark0de* closed at that time and caused many users to move in. After that time, the median price fluctuated between €75 to €85.

4.3 Taken down by LEAs

This is usually the hardest type to define, as it is difficult to establish authenticity across different sources of information other than the LEAs making a statement. The LEA may operate a market as a honeypot for a period of time after taking control of it before shutting it down, which sometimes looks like a vol-

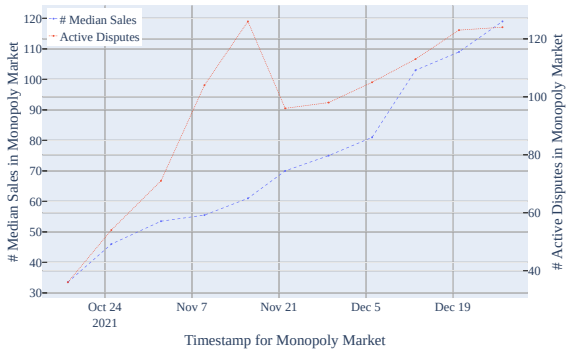


Figure 6: Median sales volume and number of active disputes in *Monopoly Market*.

untary closure.

Monopoly Market was launched in July 2019 and closed down in December 2021. The lifetime is about 29 months. It did not seem to have any attacks or exceptions until it was shut down. After closing, it was identified as sized by LEAs, claimed by the operator of *dark.fail*. The numbers of vendors and listings were quite stable, with an upward trend. As some vendors withdrew, the number of listings in this market began to decline in early December. But we can see in Figure 6 that there were still some disputes resolved at the end of November, while the median sales volume was still growing. This is considered a fairly normal pattern, and the market was growing rapidly.

Tea Horse Road is a Chinese dark web market which was launched in April 2020 and closed down in November 2021. The lifetime is about 19 months. The screenshots of its home page appeared in reports about the fight against cybercrime a few months after its abrupt closure. The numbers of vendors and listings were shown, where both numbers were rising continuously. The median price rose from $5 to $20 in the two months before the market closed, then remained flat.

Monopoly Market has been developing for over two years, and it has developed rapidly in the last two months, benefiting from the *White House Market* exit bringing some users. The market has a good reputation, and even with the slightly loss of vendors, sales are still stable. *Tea Horse Road* is also in a very smooth development stage, and all indicators are developing in a good place. Therefore, the LEAs have reason to crack down on fast-growing markets to deter criminals in their infancy.

5 DISCUSSION

Based on the results we observed, there are no significant indicators to show whether a market is heading for closure. However, we have gained some insights that may be useful for warning users that a market is going through some "difficulties", and these dynamics may lead to further moves by its market operators (including closure).

5.1 Insights

The life cycles of the six markets we observed were all greater than 18 months, with the largest being 33 months. This may be a bias caused by the fact that we picked the more popular markets when crawling, but the markets we picked contain different sizes. Therefore, we have reason to believe that, in the early days of some little-known reputable markets establishment, there is a high probability that they will not suddenly disappear. However, after a certain number of users, sales and profits have been achieved, the risk of closure becomes greater.

LEAs may be more interested in fast-growing markets, since the larger dark web market has a greater negative impact on society. Also, the market operators may have certain psychological expectations. For example, when a certain amount of profit is reached, they will try to prevent the market from becoming too exposed and uncontrolled – for instance, the market operators may choose to close it down in order to keep themselves safe from LEAs' take-down.

On the other hand, once growth is slowing down, the risk of a market closure begins to increase. In practice, when the median price falls, this may indicate a decline in the market economics to attract more customers. Dark web market operators may choose to exit at this time, meaning they try to get the last profit.

For similar reasons, we believe that markets that are not accepting new vendors are trying to become more "closed" communities because they may have significant circular revenues and do not want to take more risks. Nevertheless, several security issues (e.g. DDoS attacks), and possibly other reasons, have led market administrators to opt for the more conservative side – either exit scam or voluntary closure.

We also notice that people usually move to other popular alternative markets when a market closes. This is reflected in the data collected from our study, in which the increase of the number of comments associated to one market appears to coincide with the closure of another. Figure 7 shows the heat map of the volume of comments in *White House Market, Dark0de and Versus Project*, where darker colours mean more comments. We notice clear boundaries where people moved to the *Dark0de* market after *White House Market* exited, and to *Versus Project* after *Dark0de* was closed down. As users become ac-

Figure 7: A heatmap of the volume of comments in the Dread sub-forums of the White House Market, Dark0de and Versus Project, showing clear transitions of users (reflected by the comments' volume – the darker the square, the higher the volume) from one market to the next; Note that the timelines are synchronised, although Dark0de only covered the last three years.

tive, conflicts and problems may arise, but within two to four months, the market would either calm down and settle, or disappear into the darkness.

5.2 Challenges

Data collection is considered to be a challenge in this study. Firstly, we do not yet have the ability to predict which markets will close in the near future, so we can only do our best to collect data on some markets and then analyse them after they have closed down. Secondly, data collection is influenced by the accessibility of the market website. Dark web markets are often attacked by various parties, which may be LEAs or competitors. This makes the downtime for some markets very long, causing the crawling process to be interrupted and making the data incomplete.

Moreover, the security mechanisms of some markets result in a limited number of requests being sent at a time. For instance, *Cartel* market only allows 300 requests to be made in a session over a period of time (approximately 40-60 minutes). Therefore, we tried to use multiple accounts for parallel crawling, but were still limited by the site's measures not being able to access the full content of the market. In addition, we used two different software packages and two different strategies for data collection (see Section 3).

5.3 Limitations and Future Work

The data points obtained are not very comprehensive due to the security mechanisms implemented on some of the markets' sites. The main problem was due to the CAPTCHA employed on these sites causing our crawler to be disrupted. Additionally, our dataset contains relatively short snapshots (approximately 2-9 months) of the observed markets' data, even though the markets we observed all had lifetime greater than 18 months. Finally, the markets in our dataset represent only a small number of existing markets; as such, some bias might have been introduced as a result.

Further work could focus on dealing with the security mechanisms of different dark web markets, for example to understand their anti-crawling strategies (including the CAPTCHA features mentioned above, as well as cookies reset and rate-limiting constraints).

It would also be interesting to look further into the behaviour of cross-market vendors when a market is closed down. We observed that many vendors are selling in different markets simultaneously, which means they would suffer some losses when a market they are operating in was closed down. However, they do not seem to be too concerned about these losses and try to maintain their reputation by, for example, actively seeking out purchasers in relevant forums.

We also expect more long-term observational research on the dark web in general, for instance to better understand the development and evolution of a dark web ecosystem due to its dynamic and unpredictable nature.

6 CONCLUSION

In our study, we collected data from six dark web markets and five associated forums to investigate what happens when dark web markets are closed down. We describe and analyse several indicators for such events. The results showed that even though the markets may be closed down for various reasons, they still have some interesting commonalities.

Both exit scams and voluntary closures are more likely to happen when the market's economy starts to change (i.e. not in line with its own "normal" economic pattern). Measuring the stage of development of a market may depend on indicators such as the number of vendors, the median price, sales volume and the number of disputes.

It is also important to note whether the market continues to accept new vendors or not. If the market administrators are not looking to accept new vendors, they might want to be more stealthy or the periodic profit has likely met their expectations (which could mean they might try to become an invite-only community or simply shut down at some point). As for markets being shut down by LEAs, those markets seem to be in a period of rapid growth and showing no signs of slowing down – then suddenly disappear.

After a market closure, users and vendors will quickly move to other markets with a good reputation. However, after two to four months, these alternative markets will most likely go into the next darkness. We believe that these insights provide a way to gain a more comprehensive understanding of the development of dark web markets. We also hope our research will draw the attention of the academic community to this often-forgotten dynamic in the dark web.

REFERENCES

Alsayra (2015). Azsecure-data.org. https://www.azsecure-data.org/dark-net-markets.html.

Bhalerao, R., Aliapoulios, M., Shumailov, I., Afroz, S., and McCoy, D. (2019). Mapping the underground: Supervised discovery of cybercrime supply chains. In *2019 APWG Symposium on Electronic Crime Research (eCrime)*, pages 1–16.

Branwen, G. (2019). Darknet market mortality risks. https://www.gwern.net/DNM-survival.

Branwen, G., Christin, N., Décary-Hétu, D., Andersen, R. M., StExo, Presidente, E., Anonymous, Lau, D., Sohhlz, D. K., Cakic, V., Buskirk, V., Whom, McKenna, M., and Goode, S. (2015). Dark Net Market archives, 2011-2015. https://www.gwern.net/DNM-archives.

Christin, N. (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*, pages 213–224.

DarkNetDaily.com (2021). Interview with dark web marketplace aurora market. https://darknetdaily.com/2021/01/08/interview-with-dark-web-marketplace-aurora-market/.

Darknetlive (2022). Monopoly market. https://darknetlive.com/markets/monopoly-market/.

DeepDotWeb (2015a). Interview with alphabay market admin. https://gir-pub.github.io/deepdotweb/2015/04/20/interview-with-alphabay-admin/.

DeepDotWeb (2015b). Interview with german-plaza admin. https://gir-pub.github.io/deepdotweb/2015/11/04/interview-with-german-plaza-admin/.

DeepDotWeb (2015c). Therealdeal: This long-dead market was just relaunched! https://gir-pub.github.io/deepdotweb/2015/12/01/therealdeal-this-dead-market-was-just-relaunched/.

Dingledine, R., Mathewson, N., and Syverson, P. (2004). Tor: The second-generation onion router. Technical report, Naval Research Lab Washington DC.

ElBahrawy, A., Alessandretti, L., Rusnac, L., Goldsmith, D., Teytelboym, A., and Baronchelli, A. (2020). Collective dynamics of dark web marketplaces. *Scientific reports*, 10(1):1–8.

EMCDDA, E. (2018). Darknet markets ecosystem – lifetimes and reasons for closure of over 100 global darknet markets offering drugs, sorted by date. Technical report, EMCDDA.

European Monitoring Centre for Drugs and Drug Addiction (2020). Covid-19 and drugs – drug supply via darknet markets. Technical report, EMCDDA.

Georgoulias, D., Pedersen, J. M., Falch, M., and Vasilomanolakis, E. (2021). A qualitative mapping of dark-web marketplaces. In *2021 APWG Symposium on Electronic Crime Research (eCrime)*, pages 1–15.

Kouzis-Loukas, D. (2016). *Learning Scrapy*. Packt Publishing Ltd.

Labrador, V. and Pastrana, S. (2022). Examining the trends and operations of modern dark-web marketplaces. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 163–172.

Noroozian, A., Koenders, J., Van Veldhuizen, E., Ganan, C. H., Alrwais, S., McCoy, D., and Van Eeten, M. (2019). Platforms in everything: analyzing ground-truth data on the anatomy and economics of bullet-proof hosting. In *28th USENIX Security Symposium USENIX Security 19)*, pages 1341–1356.

Nunes, E., Diab, A., Gunn, A., Marin, E., Mishra, V., Paliath, V., Robertson, J., Shakarian, J., Thart, A., and Shakarian, P. (2016). Darknet and deepnet mining for proactive cybersecurity threat intelligence. In *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, pages 7–12.

Pastrana, S., Thomas, D. R., Hutchings, A., and Clayton, R. (2018). Crimebb: Enabling cybercrime research on underground forums at scale. In *Proceedings of the 2018 World Wide Web Conference*, WWW '18, page 1845–1854, Republic and Canton of Geneva, CHE. International World Wide Web Conferences Steering Committee.

Privoxy Developers (2022). Privoxy. https://www.privoxy.org/.

Redman, J. (2020). Sources say world's largest darknet empire market exit scammed, $30 million in bitcoin stolen. *Bitcoin.com*.

Software Freedom Conservancy (2022). Selenium project. https://www.selenium.dev/.

Soska, K. and Christin, N. (2015). Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. In *24th {USENIX} security symposium ({USENIX} security 15)*, pages 33–48.

Tidy, J. (2022). Hydra: How german police dismantled russian darknet site. *BBC News*.

Turk, K., Pastrana, S., and Collier, B. (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)*, pages 428–437.

Wang, Y., Arief, B., and Hernandez-Castro, J. (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)*, pages 1–13. IEEE.

Weber, J. and Kruisbergen, E. W. (2019). Criminal markets: the dark web, money laundering and counterstrategies-an overview of the 10th research conference on organized crime. *Trends in Organized Crime*, 22(3):346–356.

WIRED (2021). The demise of white house market will shake up the dark web. *WIRED*.

Yannikos, Y., Heeger, J., and Steinebach, M. (2022). Data acquisition on a large darknet marketplace. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, ARES '22, New York, NY, USA. ACM.