Toad in the Hole or Mapo Tofu? Comparative Analysis of English and Chinese Darknet Markets

Yichao Wang, Budi Arief, Julio Hernandez-Castro
School of Computing, University of Kent, United Kingdom
{yw300, b.arief, j.c.hernandez-castro}@kent.ac.uk
ORCID: 0000-0002-4633-3690, 0000-0002-1830-1587, 0000-0002-6432-5328

***Abstract*—The popularity of online shopping and cryptocurrency has contributed to drive the economy of darknet markets in recent years. These are often perceived to be conducive to (or may even facilitate) cybercrime related activities. It is, therefore, worthwhile to have a deeper understanding of how various darknet markets operate, so that researchers and law enforcement agencies can test and deploy appropriate countermeasures to fight against online crime. Currently, there is a knowledge gap regarding the similarities and differences among darknet markets in different languages. This study aims to compare between darknet markets operating in English and Chinese. Data from three English and two Chinese darknet markets was collected. The gathered data is described, compared, and analysed in six main aspects: operation model and structures, product categories, market policies, payment methods, security mechanisms, and vendors' characteristics. Our datasets were collected during a seven-week period between 17 July and 30 August 2021, and they contain data from 384 vendors in the English darknet markets and 4,429 in the Chinese ones. The Chinese darknet markets generally seem to have more liberal policies than their English counterparts, as demonstrated by the variety and types of goods and services offered, many of which would have been banned in the English speaking ones. All darknet markets suffer from reputation issues. Cross-market actors are active, but they represent only a small proportion of the vendors observed in our study. In summary, our findings reveal key characteristics of darknet markets in two widely used languages. This information can provide useful insights for security researchers and law enforcement agencies in combating cybercrime.**

***Index Terms*—e-crime, cybercrime, darknet, anonymous online markets, vendors, comparative study, data collection.**

I. Introduction

As the Internet became an integral part of everyone's lives, more and more people conduct business transactions online. The stakeholders include not only legitimate vendors and buyers, but also cybercriminals, who tend to engage in online trading to boost profits, evade capture and expand their criminal operations. Anonymous online markets – popularly known as *darknet markets* – have played a big role in the modern cybercrime ecosystem. The Onion Router (Tor) provides a key building block for enabling anonymous online markets. Tor is an open-source software that uses volunteer nodes for hiding its users' IP addresses through multiple hops [1]. Tor was initially used for privacy protection [2], but darknet markets also leverage the Tor network, in order to provide anonymity for their stakeholders. This poses some difficulties to law enforcement agencies (LEAs) in identifying and tracking the stakeholders involved, which include both cybercriminals and, at times, victims.

The Silk Road was one of the first and most prominent darknet markets, but it was shut down in October 2013 [3]. The US government seized over $1 billion worth of bitcoin connected to the old Silk Road market [4]. Nevertheless, shutting down a market is not the end of the "game" for many of the people involved. Vendors usually continue to trade on other platforms, at times after changing their username. As a trend, new markets will appear just weeks after others are closed. Vendors and customers will move to already existing, alternative smaller markets.

With the increasing number of markets in operation, it is important to study cybercrime stakeholders (such as cybercriminals and victims) comprehensively. Gaining in-depth insights from such an investigation will provide LEAs and security researchers with a clear understanding of the operation and the evolution of darknet markets, which in turn will enable the creation of appropriate countermeasures and mitigation techniques to combat cybercrime.

Previous studies have measured a wide range of darknet markets, but they are heavily skewed towards those conducting their business mainly in English. However, English darknet markets are not the only platforms of interest here. Investigations into other language darknet markets – such as those in Chinese or Russian – are still scarce, and this is a gap that needs to be addressed. Furthermore, and due to the rise of cryptocurrency despite their hard stance towards bitcoin, Chinese LEAs have also increased their effort to fight criminal activities in darknet marketplaces [5]. The development and acceleration of economic globalisation have also made it necessary to study the diversity and impact of darknet markets in different regions of the world.

The study presented in this paper aims *to investigate, analyse and compare several current popular English and Chinese darknet marketplaces*. The main research question is whether there are key differences between marketplaces operating in English and those in Chinese. As a secondary research question, we would also like to know if such differences – assuming they are noticeable – would influence the behaviour of vendors and the market policies, as well as the characteristics of cross-market actors.

Contributions. We collected datasets from five active and popular darknet markets, three operating in English and two in Chinese. Through statistical analysis and in-depth investigation, we track some indicators and come up with a summary of key characteristics, and how these characteristics compare between the two different languages marketplaces. We described, analysed, and compared the results of our investigation in six main aspects: (i) operation model and structures, (ii) product categories, (iii) market policies, (iv) payment methods, (v) security mechanisms, and (vi) vendors' characteristics. We share our insights into market development and vendors' behaviour, which are helpful for future investigations.

The rest of the paper is organised as follows. First, we provide an overview of relevant related work in Section II. We then explain our approach and how we carried out our data collection in Section III. We show the results in six different aspects (as mentioned above) in Section IV. We discuss the implications of such insights, along with the challenges and limitations of our study in Section V. We summarise the implication of this study and present our conclusions regarding the nature of cybercrime in darknet markets in Section VI.

II. Related Work

Several prior works studied darknet markets and forums. Christin [6] performed a comprehensive measurement analysis of the Silk Road, showing that drugs were the main concern. The paper also estimated the overall market profit and possible intervention methods. Wegberg et al. [7] tracked the evolution of commoditisation on eight English darknet markets over six years. The paper concluded that retail has a large share in the darknet markets, and the overall revenue for cybercrime commodities was $15 million between 2011 and 2017. More recently, Vu et al. [8] described the evolution of the Hack Forums marketplace through the set-up, stable state and Covid-19 pandemic eras. They found that the market centralised heavily around influential users and threads.

There are other studies focused on identifying the characteristics of key actors, which can then be used to obtain more insights and to understand the cybercrime ecosystem [9] [10] [11] [12] [13] [14] [15]. More specifically, Yip et al. [16] examined the structure of organised cybercrime by quantitative analysis of data coming from online underground markets. The paper concluded that trust is an important factor in promoting the prosperity of the underground economy. Holt [17] described the relationship between actors influenced by the price, customer service, and trust in ten Russian underground forums through a qualitative investigation, focusing on malware and attack tools. Bhalerao et al. [18] tried to identify supply chains from major English and Russian cybercrime forums.

However, there is still limited research looking into how different language darknet markets compare. Zhou and Zhuge [19] analysed and described the differences in darknet markets between Chinese and English speaking communities. They mainly looked at three aspects: market operation, security, and goods sales. They also described the difference in selling goods depending on relevant laws and regulations. Our work has been informed by this study. We have included more comprehensive data about the English and Chinese darknet markets under study regarding market policies, payment methods, crawling restrictions, and some vendor's indicators and main characteristics. We also found a new type of trading model in a Chinese darknet market, namely the "request-to-buy mode". Our datasets also contain the most recent descriptive information, e.g. product posts and vendor profiles, which can be valuable for analysis purposes and are available to any LEAs or academic researcher, after proper identification.

Most of the publicly available datasets for darknet markets are out of date. These include the 2016 and 2017 DreamMarket datasets from AZSecure-data [20]. The Dark Net Market archives from 2011 to 2015 by Branwen et al. [21] is another example of useful, but quite out of date dataset. CrimeBB is the only dataset that is still maintained and updated by the Cambridge Cybercrime Centre [22]. The dataset includes one underground forum containing roughly 180,000 contracts. However, we decided to do our own data collection due to the more specific types of data we need, namely specific languages constraints and continuous data spanning several weeks.

III. Methodology

This section outlines our approach and provides an overview of the data collection process, including the description of the two crawling mechanisms, a detailed outline of our datasets[1], and the specific details of the technical set-up used. We also briefly discuss ethical considerations at the end of this section.

A. Approach

In order to understand how different language darknet markets work, we carried out a study based on a combination of observational, retrospective, and longitudinal approaches [23]. We constructed our datasets during a seven-week period between 17 July and 30 August 2021, containing data from 384 vendors in the English darknet markets and 4,429 in the Chinese darknet markets.

Data on the *operation model and structures* include the markets' basic information, as well as changes in the market size and the possible reasons behind such changes. The *product category* displays the proportion of different types of items in the markets based on the average number of each snapshot. The more comprehensive data available in the Chinese darknet markets means we can also estimate the revenue generated by the main product categories. The *market policy* mainly focuses on what goods or services are explicitly banned. The *payment methods* describe what currencies are accepted. The *security mechanisms* describe the crawling restrictions in each darknet market, as well as general account security. In terms of *vendors' characteristics*, we analysed vendor location, trust level and active/inactive status and time. We also selected some top and cross-market vendors in the English darknet markets, and some top vendors in the Chinese darknet markets. We define top as the ones that make more profits, have more sales and have more positive feedback or better reputations

[1] Due to the potentially criminal nature of the datasets, we have to choose an appropriate and ethical way for sharing them. We are happy to share our datasets with academics, security researchers, and LEAs.

TABLE I: Summary of the Observed Darknet Markets

Market	First seen	# Listings	# Vendors	Lang
Dark0de Reborn	2020-05	45876	1648	EN
White House Market	2019-08	44740	3453	EN
Cartel Marketplace	2020-06	2596	195	EN
Chinese Exchange Market	2018-03	10949	2636	CN
Tea Horse Road	2020-04	8302	1793	CN

during the observation period. Top vendors are sometimes defined and shown on the home page in the darknet markets. Top vendors are mostly calculated and selected based on the materials mentioned above. Cross-market vendor refers to the vendor who sells at the same time in multiple markets. We were particularly interested in the vendors' behaviours and operating model of cross-market vendors when comparing. Finally, we highlight some stark differences between English and Chinese darknet markets based on the six aspects above.

B. Data Collection

We used Python with the Scrapy web-crawling framework [24] to implement a custom crawler. Depending on the restriction policies of different markets and the information contained in each market, we used two sets of strategies:

1) If the market had stringent anti-crawl measures, the website would take a long time to crawl, or/and the session might expire during crawling. In this case, we would only collect data based on what is shown on the website home pages. For instance, most websites display highly rated vendors, promotional products and featured listings. Therefore, we could get selected vendors' data.
2) If the market had less stringent protections and restrictions, we would try to get as much information as possible through the listing pages.

The listing page URLs can usually be traversed easily in both strategies because their URLs are generally sequential. The product pages and vendor pages are partly obtained and parsed depending on the darknet marketplace website structure. Crawling restriction details are described and compared further in Section IV.

The data was collected once a week to avoid stressing the markets' website and being as inconspicuous as possible. In some circumstances, e.g. a DDoS attack on the website, the data collection was slightly delayed.

Table I provides a summary of the observed darknet market names, when they were first seen, the number of active listings of products, the number of active vendors, and the language used. The active numbers are as of 30 August 2021.

Dark0de Reborn is one of the English-based darknet markets, and it started in the early days of the Covid-19 outbreak, 24 May 2020. It has the most number of listings, and vendors are able to import feedback scores from other popular markets. Therefore, it has attracted a large number of vendors with good reputation. The market has strict crawling restrictions. A single session will expire in about an hour, and the number of requests is also limited. We focus on the top vendors (an average of 20 top vendors per week) and collect data from their product pages. Data includes the vendors' profile pages and some of the feedback received. We also collected some statistical data to study market trends.

White House Market (WHM) is one of the most popular darknet markets in English language. The market has been in operation since 24 August 2019. A decline in Empire Market's reputation led to a rise of WHM [25], which has a very high reputation. It also has the strictest crawling restrictions. The market only allowed a limited number of requests in ten minutes. We used six accounts to crawl to ensure that enough data was collected before the session expired. We were only able to collect top vendors (an average of 25 top vendors per week) mentioned on the homepage and some statistical data. Data includes vendors' profile pages and their product listings.

Cartel Marketplace is a medium size darknet market in English. Although it is not as large as the previously mentioned markets, it still has a good reputation in dark web forums. So we think it should be included in the research. It has a relatively less stringent crawling policy, which allowed about 300 pages per session within about 40 minutes to 50 minutes. We used three accounts to crawl. The product URLs are more likely random or coded, which means we had to traverse the whole listing with the page numbers. We saved all product URLs in a list, then sent requests accordingly. We were able to collect all vendor's information (an average of 186 vendors per week) and listing pages in this market.

Chinese Exchange Market is the most active and oldest darknet market in Chinese. It was developed from a forum. It has a less stringent crawling policy, and the cookie structure is also very simple. The market has no restrictions on the number of requests per session and is given a long lifetime of a single session. Therefore, we collected all active listing pages and parsed them. Technically, the product URLs are sequential. It can be traversed easily using a brute force approach.

Tea Horse Road represents the new generation of Chinese darknet markets. It has a user-friendly interface with an innovative "request-to-buy" model. It is a market with several historical versions, the earliest can be traced back to October 2019. The current version of the market was launched around April 2020. It also has a less stringent crawling policy (similar to the Chinese Exchange Market), although the structure of the cookies is a bit complicated. Dynamic cookies is used, which means we need to change the cookie every time we send a request (this cookie value is obtained from the previous response). We managed to collect all active listing pages because the product URLs are, again, sequential so they can be traversed exhaustively.

Table II compares the indicators and features of the collected markets. The symbol ✗ means either the indicator does not exist in the market or it was not collected due to crawling limitations. Overall, a total of 1,968 pages and 168,398 listings were collected. They contain 143 pages of vendor information and seven status pages (one per week) in Dark0de Reborn; 516 pages of vendor information in WHM; 1,302 pages of vendor information and 20,776 listings in Cartel Marketplace; 75,224

TABLE II: Comparison of the Indicators and Features of the Collected Markets

		Dark0de Reborn	**White House Market**	**Cartel Marketplace**	**Chinese Exchange Market**	**Tea Horse Road**
Vendor Characteristics	Username / ID	✓	✓	✓	✓	✓
	Profile	✓	✓	✓	✗	✗
	Member Since	✓	✓	✓	✓	✗
	Last Seen	✓	✓	✓	✓	✗
	Total #Sales	✗	✓	✓	✓	✓
	Rating	✓	✓	✓	✗	✗
	Disputes	✗	✓	✓	✗	✗
	Feedback	✓	✓	✗	✗	✗
	PGP	✓	✓	✓	✗	✗
	#Listing	✓	✓	✓	✓	✓
Product	Title	✓	✓	✓	✓	✓
	Price	✓	✓	✓	✓	✓
	Category*	✓	✓	✓	✓	✓
	Sales	✓	✗	✓	✓	✓
	Shipping From	✓	✓	✓	✗	✗
	Shipping To	✓	✓	✗	✗	✗
Market	Total #Vendors	✓	✓†	✓	✓	✓
	Total #Products	✓	✓	✓	✓	✓
	BTC	✓	✗	✓	✓	✓
	XMR	✓	✓	✓	✗	✗
	Fiat Currency	✗	✗	✗	✗	✓
	CAPTCHA	✓	✓	✓	✓	✓

*** This is not for each product, but as an overall number. † Shown only in real-time**

listings in the Chinese Exchange Market; 72,398 listings in the Tea Horse Road.

C. *Technical Environment*

We connected to the Tor network using a Virtual Machine (VM) for a secure and anonymous access to the darknet markets. The VM runs Ubuntu 20.04.2.0 LTS with four cores, eight-thread, 8 GB RAM, 200 GB storage and NAT network from the host computer. A VPN tunnel is established on the host computer and forwarded to the VM through the NAT network. To ensure our crawling was not detected, the `stem` library (https://stem.torproject.org/) was used for changing the Tor circuit every time we got a non-200 response code. Changing the circuit does not always mean a new IP was given. We only used it to increase the chance of a successful connection to the darknet market. Since Tor uses SOCKS5 proxy and Scrapy uses HTTP proxy, Privoxy (https://www.privoxy.org/) was used to relay Tor and Scrapy. Once collected, the data was encrypted and saved into offline devices.

D. *Ethical Considerations*

Since our study collected data from activities that could potentially be related to cybercrime – such as drug dealing, sexual abuse and exploitation of vulnerable groups and other criminal activities – we had to ensure that we obtained ethical clearance before we commenced our study. The ethics for this study have been reviewed and approved by our university's Research Ethics Advisory Group (Reference: 057-04-2021).

IV. Results

In this section, we present the results of our comparison for the darknet markets in English and in Chinese. The findings are divided into market, vendors, market policies, payment methods and security mechanisms.

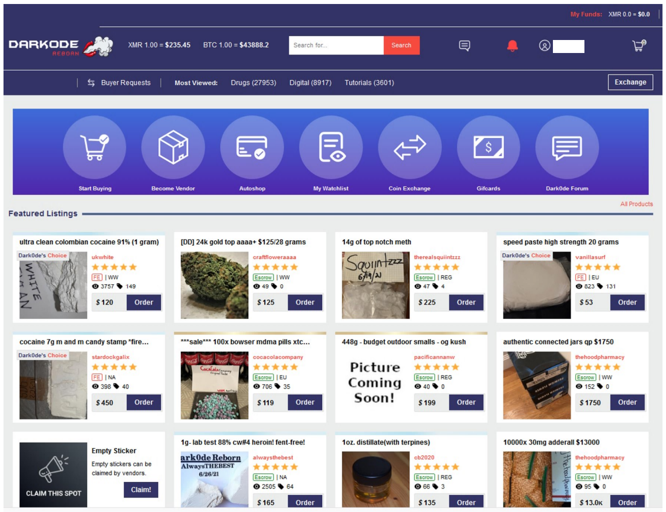


Fig. 1: Dark0de Reborn Homepage

A. *Darknet Markets in English*

1) Market: **Operation structures.** All three English darknet markets have a website interface similar to Silk Road. Figure 1 shows the Dark0de Reborn homepage. They all have multiple sections on the homepage, including promotional products, trending products and recommended top vendors. There is usually a category list on the homepage, and users can browse all products under this category. Most web pages also support a mobile-friendly interface.

Number of listings and vendors. The number of listings and vendors indicates the state of a market. Figure 2 shows the number of listings in WHM between 18 July and 30 August

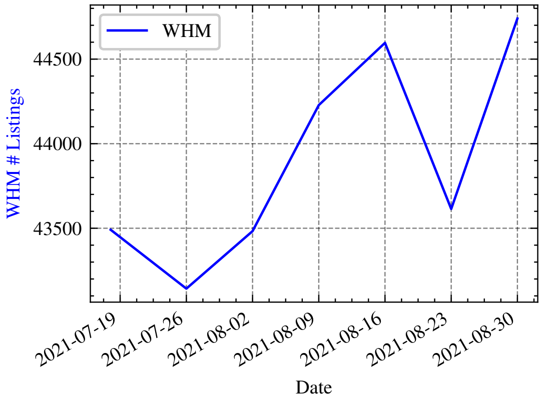


Fig. 2: Number of Listings in White House Market

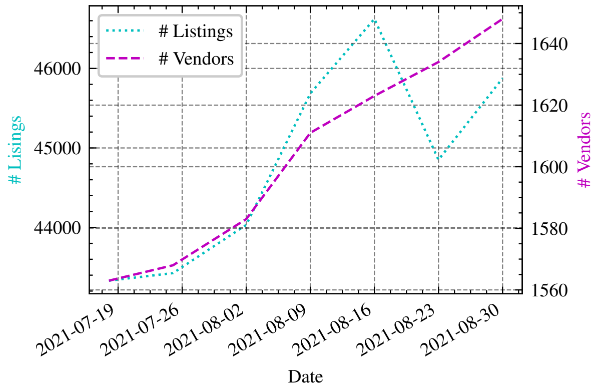


Fig. 3: Number of Listings and Vendors in Dark0de Reborn Market

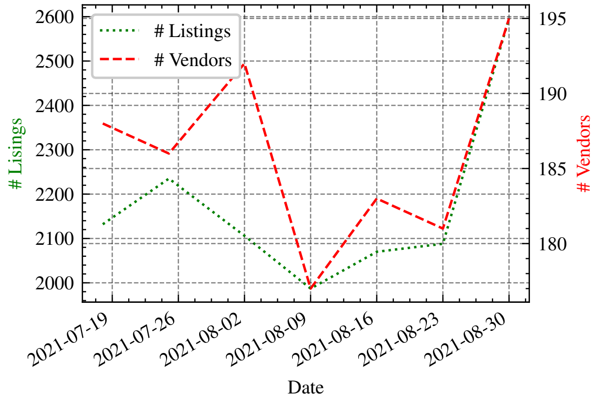


Fig. 4: Number of Listings and Vendors in Cartel Marketplace

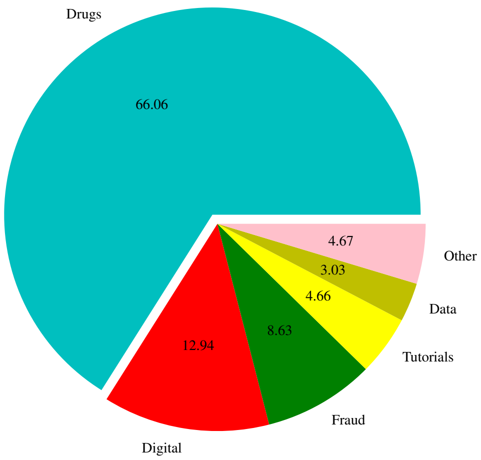


Fig. 5: Categories Breakdown in English Darknet Markets

2021[2]. Figure 3 shows the number of listings and vendors in Dark0de Reborn. The number of vendors in Dark0de contains all vendors, even if the vendor does not have any active listings. The overall listing number keeps rising, accompanied by some fluctuations in both markets. WHM and Dark0de Reborn introduced a new Product Quality and Harm Reduction Program on 17 June 2021. The program aims to provide high-quality products and lower levels of risk to buyers. Vendors who send products and receive positive test results can get badges and display them on the product page to increase credibility, facilitate trust and increase sales. Also, the vendors can apply for a reduced fee on WHM if they test regularly. This program causes some non-compliant products to be removed. Figure 4 shows the number of listings and vendors in Cartel Marketplace over the observation period. Those two lines are consistent in most weeks. As the number of vendors increases, the number of listings also rise. In Cartel Marketplace, the data collection strategies may cause fluctuations in the number of vendors. If the vendors did not list anything, are on vacation status, or sell items that are out of stock, their posts would not appear on the listing pages. Hence, the number of vendors should be considered as the number of active vendors when the data was collected.

Product category. Figure 5 shows that drugs take the largest proportion of the three darknet markets. We count those by using the website information listed in the navigation interface. Drugs account for over 66% of products, followed by digital products and fraud related materials. Digital products contain pirated software, exploit kits, digital services (DDoS services), botnets and malware. Another category of trending products in all three markets is physical items such as smart devices, jewellery, and watches. According to the vendors' descriptions, most of them are fakes or reshipping drops.

2) Vendor: **Inactive days.** Figure 6 shows the joining date and inactive days of 264 vendors from Cartel Marketplace. We define the number of inactive days as the number of days from the last seen date to the date when the data was collected. A few vendors were not very active over 50 days, but most vendors were still active, even if they have been registered for more than one year. Over 89% of the vendors have appeared within the last ten days. Even though the total number of

[2] The vendor information on WHM is shown only in real-time, hence we do not have historic information on the number of vendors on WHM. Furthermore, in early May 2021, WHM stopped accepting any new vendors applications, making the number of vendors plateau at about 3,450. In comparison, Dark0de Reborn maintained a continuous vendor growth.

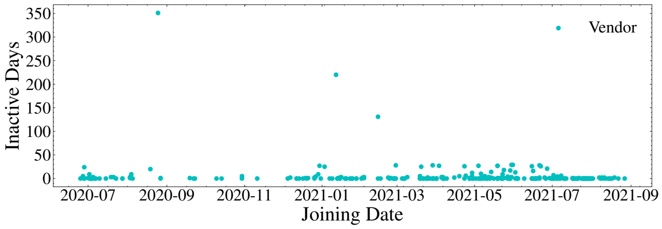


Fig. 6: Inactive Days and Joining Date in Cartel Marketplace

TABLE III: The Proportion of Vendors' Locations in English Darknet Markets

Location	Number	Percentage
United States	124	32.29%
Worldwide	65	16.93%
United Kingdom	38	9.90%
Europe	37	9.64%
Netherlands	32	8.33%
Germany	19	4.95%
Australia	19	4.95%
N/A	11	2.86%
France	7	1.82%
North America	7	1.82%

vendors in the market is small, they seem to be very active.

Location. In all three English darknet markets, we collated the location of 384 vendors based on their profiles. Table III shows the top ten countries and regions where those vendors are located, covering 359 vendors, or 93.49% of the 384 vendors. The United States and Europe are the main supply locations. Approximately 62% of European vendors are from the United Kingdom, the Netherlands and Germany. This result is consistent with previous reports [26]. In terms of "Worldwide" or "N/A", these mean that some vendors do not want to reveal their location, particularly when they only sell virtual items. According to observations on dark web forums, buyers tend to buy drugs in local countries and regions to reduce the risk of being discovered by customs and LEAs. Therefore, we have reason to believe that the location information provided by the vendor is mostly accurate, in order to attract target customers better.

Trust Level. This is usually the way to show the credibility of vendors in the English darknet markets. In different darknet markets, the trust level may be calculated by their own algorithms designed by the operators. Figure 7 shows the relationship between trust level and sales, feedback, number of disputes, joining date and vendor population distribution in Cartel Marketplace. The numbers displayed are the median value at each level, except the population distribution. For example, in level 10, the median sales volume is 104. Level changes are affected by a combination of these aspects. High-level vendors usually have higher sales volumes and better reviews. The duration of registration has a limited impact on the level reached. For example, *Vendor_EN_1* is a level 10 vendor who joined the market in July 2021 with 185 sales, only one dispute, and 141 positive feedbacks. Please note that not all orders compulsorily require feedback. In comparison, *Vendor_EN_2*, trust level 5, joined the market in March 2021 with 526 sales but 15 disputes and only 187 positive feedbacks. As a result, in addition to sales, the number of complaints and positive feedback also influence the trust level.

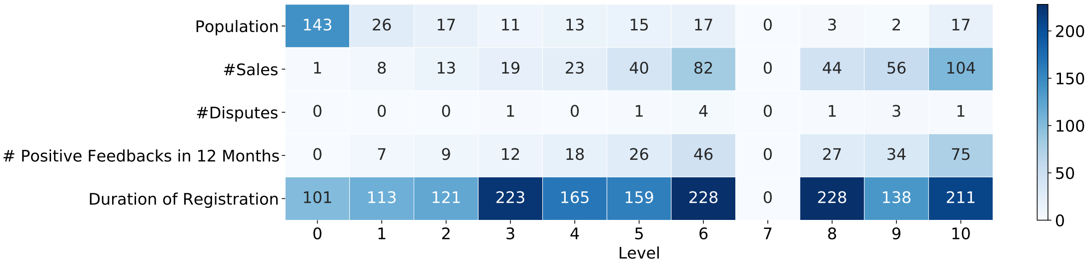
Behaviour. We selected some vendors to describe and analyse their behaviours from WHM. *Vendor_EN_3* joined the market in July 2020, with currently 3,680 sales and 95% positive feedback. In the seven weeks included in our datasets, the number of orders was at least 830. The vendor had over 7,000 transactions in the previous Empire Market, with 99% positive feedback. This vendor mainly sells cocaine products in the US. The largest displayed unit can reach 500 grams, and the price is close to $20,000. According to the smallest sales unit, we calculated that their total estimated profit is at least $2.7 million with around $207,500 made during the observation period. As a successful big vendor, they can usually use their name as a symbol of their brand. *Vendor_EN_4* also confirms this point. The vendor has good reviews in its own region and sells drugs in multiple darknet markets simultaneously. Most successful vendors sell in different English darknet markets at the same time. They use the same format and language style in their profile. Since the feedback rating of English darknet markets can be imported into another, buyers can easily identify cross-market vendors. Some vendors also regularly update the product or their own situation in their profile. This can be used as a signal if they do not appear for a long time. They may be arrested or just quit, warning past and potential customers that they may be at risk.

3) Market Policy: This subsection describes what products are banned on the three English darknet markets, and the regulations regarding communication between users.

In Dark0de Reborn, the policy is called "selling policies and seller code of conduct". It is strictly forbidden to sell any images of sexual abuse of children, Fentanyl related products and any product or service related to terrorism. Fentanyl is an analgesic generally used in surgery; excessive use can quickly lead to addiction, hypotension and death due to respiratory depression. The website stipulates the use of in-site messenger as the means of communication between buyers and sellers and for customer service. Also, the exchange of large amounts of communications should be avoided unless paid for via Dark0de's services. To protect the competitiveness and security of the market, external links and external dissemination of user information are not allowed.

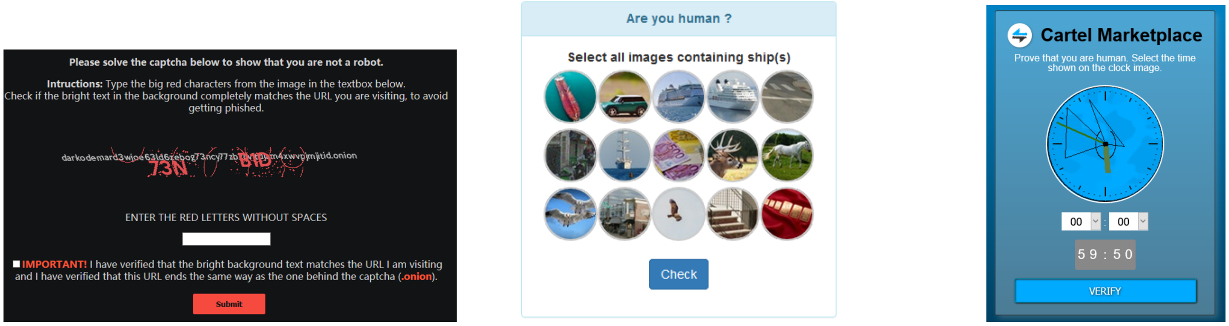
In comparison to Dark0de Reborn, WHM is more comprehensive and detailed. The policy strictly forbids any child abuse, human or animal abuse, murder for hire, weapons, Fentanyl and terrorism-related products. During the Covid-19 pandemic, products that purportedly can cure the virus are banned, but discounts on related tests and promotional codes are available. In terms of communication, they also ban external links and any external contact information.

Cartel Marketplace has tough market rules. The policy forbids child abuse, biological, radiological, or chemical weapons, murder for hire, scamming or deceptive tutorials. Searching for and publishing private or identifying information



Level	0	1	2	3	4	5	6	7	8	9	10
Population	143	26	17	11	13	15	17	0	3	2	17
#Sales	1	8	13	19	23	40	82	0	44	56	104
#Disputes	0	0	0	1	0	1	4	0	1	3	1
# Positive Feedbacks in 12 Months	0	7	9	12	18	26	46	0	27	34	75
Duration of Registration	101	113	121	223	165	159	228	0	228	138	211

Fig. 7: Trust Level Correlation Matrix in Cartel Marketplace



Please solve the captcha below to show that you are not a robot.

Intructions: Type the big red characters from the image in the textbox below.
Check if the bright text in the background completely matches the URL you are visiting, to avoid getting phished.

darkodemard3wjoe63ld6zebog73ncy77zb[illegible]m4xwvpjmjitid.onion

ENTER THE RED LETTERS WITHOUT SPACES

□ **IMPORTANT!** I have verified that the bright background text matches the URL I am visiting and I have verified that this URL ends the same way as the one behind the captcha (**.onion**).

(a) Dark0de Reborn CAPTCHA

Are you human ?

Select all images containing ship(s)

(b) White House Market CAPTCHA

Cartel Marketplace

Prove that you are human. Select the time shown on the clock image.

00 : 00

5 9 : 5 0

(c) Cartel Marketplace CAPTCHA

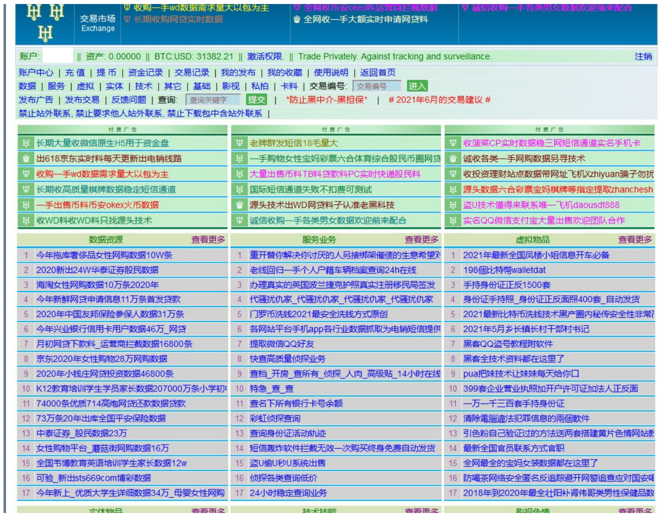
Fig. 8: CAPTCHA Samples from English Darknet Markets

are not tolerated. In terms of communication, the website bans direct deals but does not limit external links or contact.

4) Payment Method: All three markets use the on-site wallet mode. Users are given a deposit address, and they then add funds by using Bitcoin or Monero. Dark0de Reborn and Cartel Marketplace allow both Bitcoin and Monero. In WHM, since Bitcoin is much easier to track, only Monero is allowed, for security reasons. In Dark0de Reborn, users can also use the website balance to purchase gift cards and send them to other accounts. That means Dark0de Reborn supports the transfer of funds within the market. On the website, the default currency is USD. However, users can choose between CAD, EUR, GBP, RUB, AUD, etc. The website also displays real-time market exchange rates.

5) Security Mechanisms: All three markets studied have strict crawling restrictions, such as the use of CAPTCHA. Figure 8 shows the CAPTCHAs in the three English darknet markets. Dark0de Reborn only implements a simple letter and number combination verification code. In WHM, the bot-check consists of choosing the images that match a specific description out of 15 pictures. Those are randomly rotated, for added security. In Cartel Marketplace, the user needs to indicate the time shown by the analogue clock. Then, there is another simple verification code to be entered when logging in. WHM and Cartel Marketplace allow users to choose how long the session will be kept alive – available options range from ten minutes to 48 hours. After those verification processes are completed, a user can access the market's home page.

The number of pages that can be accessed per minute or per hour is strictly limited as well. WHM only allows a limited number of requests in ten minutes. Even if a (human) user tries to open multiple tabs at once, it is easy to trigger the detection system which will force logout and require re-login. Moreover, the trigger conditions may vary, but approximately 40 requests are allowed within 30 minutes. We applied a dynamic delay of 16 seconds to 90 seconds with six accounts. The dynamic delay is based on the corresponding time of the server to ensure that the page is returned. Sixteen seconds is the minimum interval between each request in an ideal



交易市场 Exchange

收购一手wd数据需求量大以包为主

长期收购网贷实时数据

全网收币安okex料运营商拦截数据

全网收一手大额实时申请网贷料

诚信收购一手各类男女数据欢迎前来配合

账户: || 资产: 0.00000 || BTC:USD: 31382.21 || 激活权限. || Trade Privately. Against tracking and surveillance. 注销

账户中心 | 充 值 | 提 币 | 资金记录 | 交易记录 | 我的发布 | 我的收藏 | 使用说明 | 返回首页

数据 | 服务 | 虚拟 | 实体 | 技术 | 其它 | 基础 | 影视 | 私拍 | 卡料 | 交易编号: 交易编号 进入

发布广告 | 发布交易 | 反馈问题 | 查询: 查询关键字 提交 | *防止黑中介-黑担保* | # 2021年6月的交易建议 #

禁止站外联系, 禁止要求他人站外联系, 禁止下载包中含站外联系 |

付费广告	付费广告	付费广告
长期大量收微信原生H5用于资金盘	老牌群发短信18毛量大	收菠菜CP实时数据稳三网短信通道实名手机卡
出618京东实时料每天更新出电销线路	一手购物女性宝妈彩票六合体育综合股民币圈网贷	诚收各类一手网购数据另寻技术
收购一手wd数据需求量大以包为主	大量出售币料TB料贷款料PC实时快递股民料	收投资理财站点数据带网址飞机Xzhiyuan骗子勿扰
长期收高质量棋牌数据稳定短信通道	国际短信通道失败不扣费可测试	源头数据六合彩票宝妈棋牌等指定提取zhanchesh
一手出售币料币安okex火币数据	源头技术出WD网贷料子认准老黑科技	盗U技术懂得来联系唯一飞机daousdt888
收WD料收WD料只找源头技术	诚信收购一手各类男女数据欢迎前来配合	实名QQ微信支付宝大量出售欢迎团队合作

	数据资源 查看更多		服务业务 查看更多		虚拟物品 查看更多
1	今年拖库奢侈品女性网购数据10W条	1	重开替你解决你讨厌的人另接绑架催债的生意希望X	1	2021年最新全国凤楼小姐信息开车必备
2	2020新出24W华泰证券股民数据	2	老线回归一手个人户籍车辆档案查询24h在线	2	198個比特幣walletdat
3	海淘女性网购数据10万条2020年	3	办理真实的英国波兰捷克护照真实注册移民局签发	3	手持身份证正反1500套
4	今年新鲜网贷申请信息11万条首发贷款	4	代骚扰仇家_代骚扰仇家_代骚扰仇家_代骚扰仇家	4	身份证手持照_身份证正反面照400套_自动发货
5	2020年中国友邦保险参保人数据31万条	5	门罗币洗钱2021最安全洗钱方式原创	5	2021最新比特币洗钱技术黑产圈内秘传安全性非常
6	今年兴业银行信用卡用户数据46万_网贷	6	各网站平台手机app各行业数据抓取为电销短信提供	6	2021年5月乡长镇长村干部村书记
7	月初网贷下款料_运营商拦截数据16800条	7	提取微信QQ好友	7	黑客QQ盗号教程附软件
8	京东2020年女性购物28万网购数据	8	快查高质量侦探业务	8	黑客全技术资料都在这里了
9	2020年小钱庄网贷投资数据46800条	9	查档_开房_查所有_侦探_人肉_高级贴_14小时在线	9	pua把妹技术让妹妹每天给你口
10	K12教育培训学生学员家长数据207000万条小学初	10	特急_查_查	10	399套企业营业执照加开户许可证加法人正反面
11	74000条优质714高炮网贷还款数据贷款	11	查名下所有银行卡号余额	11	一万一千三百套手持身份证
12	73万条20年出库全国平安保险数据	12	彩虹侦探查询	12	清除電腦違法犯罪信息的兩個軟件
13	中泰证券_股民数据23万	13	查询身份证活动轨迹	13	引色粉自己验证过的方法送两套搭建黄片色情网站教
14	女性购物平台_蘑菇街网购数据16万	14	短信轰炸软件拦截无效一次购买终身免费自动发货	14	最新全国官员联系方式官职
15	全国韦博教育英语培训学生家长数据12w	15	盗U偷U秒U系统出售	15	全网最全的宝妈女装数据都在这里了
16	可验_新出sts669com博彩数据	16	侦探各类查询低价	16	防喝茶网络安全匿名反追踪避开网警追查应对国安喝
17	今年新上_优质大学生详细数据34万_母婴女性网购	17	24小时稳定查询业务	17	2018年到2020年最全壮阳补肾伟哥类男性保健品数

Fig. 9: Chinese Exchange Market Homepage

network situation. One of the six accounts was randomly used for each request. The probability of one account being used continuously is relatively low. This method simulates the real situation where humans browse the web, and at the same time, collects data most efficiently without being detected. In Cartel Marketplace, the limit of requests is 300 pages per session within about 40-50 minutes. Once a user reaches such a threshold, the session expires automatically. We applied a dynamic delay of three seconds to ten seconds with three accounts. An account was used to traverse the listing page of the market. The remaining two were randomly used to request vendor pages. For Dark0de Reborn, the threshold is unclear. We noticed a large number of requests that cannot be parallelised in the crawler, and we applied a dynamic delay between 5 to 60 seconds. We were able to use one account to collect the required data. In terms of the structure of cookies, they seem to be static in all three markets, which means the cookies of a session do not change.

In terms of the user account, all three marketplaces use PGP public key to ensure account security. Once a user sets up the PGP public key in their profile, they are able to use Two-Factor Authentication (2FA). PGP has also been used widely in on-site communication. At the registration stage, the user needs to set up a username and password, and then the markets will send a set of English words to create a wallet.

6) Key Takeaway: The English darknet markets have a complete ecosystem, which means the features are fully supported and implemented. Vendors in the English darknet markets are active, which also includes cross-market vendors. The English darknet markets tend to have more restrictive policies in terms of what products can be sold. Drugs are the most popular category. Bitcoin and Monero are commonly used as the main payment methods. The English darknet markets usually have strict crawling restrictions.

B. Darknet Markets in Chinese

1) Market: **Operation model and structures.** In the Chinese Exchange Market, the website structure is simple and similar to a community forum. Figure 9 shows the Chinese Exchange Market homepage. It displays the latest posts under each category on the homepage. On each category page, each post contains the title, price, post time and vendor. In the Tea Horse Road, the interactive interface is more modern, and users can also browse by category. The Tea Horse Road also supports the request-to-buy mode, where users post the products they want to buy and describe their requisites, then vendors can provide quotes. Even though the structure of the two websites is relatively simple, the user experience is good: there are no redundant functions, and the products are easy to browse based on their category.

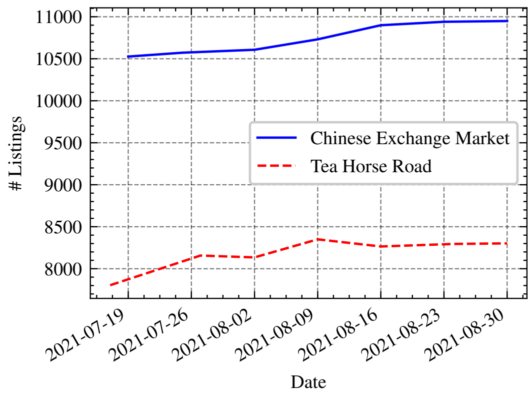


Fig. 10: Number of Listings in Chinese Darknet Market

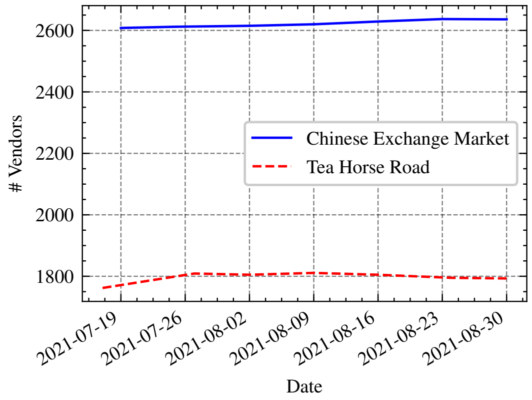


Fig. 11: Number of Vendors in Chinese Darknet Market

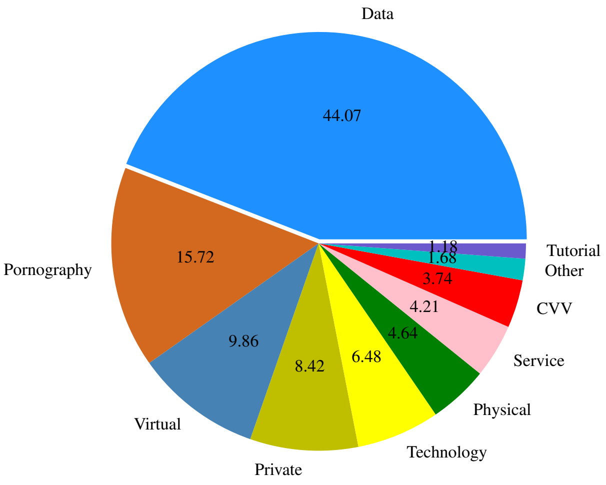


Fig. 12: Categories Breakdown in Chinese Exchange Market

Number of listings and vendors. Figures 10 and 11 show the number of listings and vendors over the observation period. In terms of the number of listings, both markets maintain an overall upward trend. The number of listing only includes the normal sale mode in Tea Horse Road. For Request-to-Buy mode, the number of listing remains stable at 2,400 during the observation period. Due to the operating mode of both Chinese darknet markets, once the advertisement is posted on the website, the post will be kept for a long time even if the vendor is not active. On the contrary, if the vendors do not show for a long time in the English darknet markets, their status could be changed to inactive. In this case, the listing

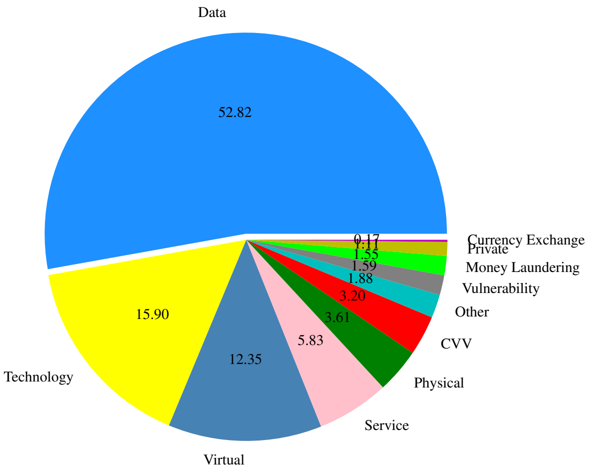


Fig. 13: Categories Breakdown in Tea Horse Road with Sale Mode

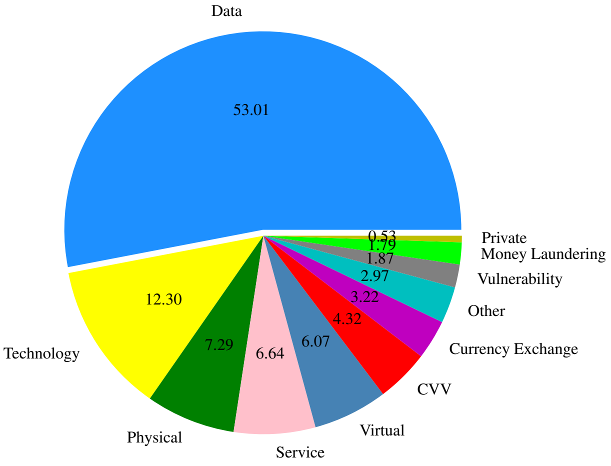


Fig. 14: Categories Breakdown in Tea Horse Road with Request-to-Buy Mode

page will not cover their posts. Moreover, according to the data, the number of vendors remains stable. Even if the number of listings keeps growing, the number of vendors remains at a certain level. A new vendor may bring more than one listing.

Product category. We described the breakdown of categories separately for those two Chinese darknet markets as they used different criteria to classify categories. Figure 12 shows the percentage of items that belong to each category in the Chinese Exchange Market. Leaked data and personal information accounted for the largest proportion, which is 44.07%. Pornography is the second most sold category with 15.72%, which includes child abuse. Private is a category that allowed buyers and vendors to use the market as the secured way to carry out their transaction. They usually have previously communicated and agreed to a deal.

Two figures show the percentage of each category in all items in the Tea Horse Road. Figure 13 shows the normal selling mode. Figure 14 shows the request-to-buy mode. Leaked data and personal information accounted for the largest proportion in both sections, approximately 53%. Pornography is classified as virtual items, and drugs are classified as physical items. Buyers request more physical items for sale.

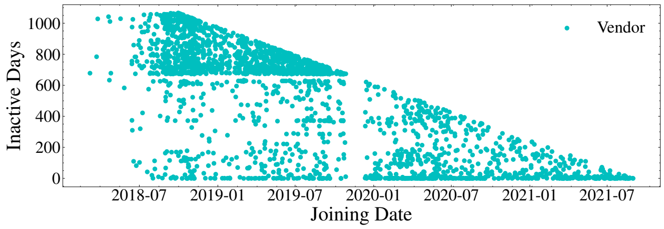


Fig. 15: Inactive Days and Joining Date in Chinese Exchange Market

In the Chinese darknet markets, the most profitable category is related to leaked personal data. We used the data from the first week and the seventh week to estimate the revenue. If a product does not appear in the first week, we marked the initial sales as zero. Otherwise, We calculate the difference in seven weeks. After obtaining the profit of a single product, it was taken into account according to the category. In the Chinese Exchange Market, all vendors are estimated to have made profits of at least $86,984.98 during the observation period. The profit related to personal data is $35,749.21, or 41.1% of all profits. The second is service, which usually are personal information query services or hires to harm others. Following is pornographic except private section, because the private section is usually priced as $1 or in the smallest unit (e.g., per gram, record, picture, video), which causes the sales number to be inaccurate. The pornographic category generated 1489 sales with $10,211.75 profits during the observation period. In the Tea Horse Road, the sales volume is displayed only within a certain period instead of cumulative (that is, the numbers count to this period will be deleted after a certain period of time), so the estimated profit is not as accurate.

2) *Vendor:* **Inactive days** Figure 15 shows the vendors' joining date and inactive days from the first post to the last seen in the Chinese Exchange Market with 2,537 vendors. At the end of 2019, there is a clear dividing line. We speculate that the market was maybe temporarily closed, banned many vendors, scam exited or updated for a long period of time. It seems like a large number of vendors exited the market at this point. Only a small part of the vendors before the end of 2019 have survived to present times, and some vendors that joined after 2020 are still active nowadays. After 2020, some people remained active until now.

Behaviour In both Chinese darknet markets, we selected some typical vendors to describe their behaviours. *Vendor_CN_1* has 113 sold items over a month with $6,773 estimated profits. The vendor first posted in June 2019, and generated a total of $29,021 in estimated profits. The vendor lists 88 posts about personal data, including pornography, virtual items and CVV related items. This personal data contains express delivery information in China, Japanese phone numbers, a set of Chinese ID card numbers with names, phone numbers and emails, email accounts with plaintext passwords, personal information in loan databases, motor vehicle registration information and much more, covering data all over the world. Pornography includes child abuse and hidden camera shots. Virtual items include VPN accounts and software. The CVV related items include card information and carding methods. In almost all posts, this vendor has screenshots to augment trust.

Vendor_CN_2 also sells personal data. The vendor sold 59 items with $2,124 estimated profits over the observation period. The most valuable product is the records of student data who attend university. The personal data contains name, age, phone number, e-mail address, school name and subject. *Vendor_CN_3* and *Vendor_CN_4* also provide services for e-whoring and hiring to hurt, respectively. However, there is not too much information in their posts, but they recommended using on-site communication for details. Since they do not have a clear price, the profit is difficult to estimate.

3) Market Policy: In the Chinese Exchange Market, there is no official policy pages just user instructions for new users and vendors. The instructions mainly ask the vendor to describe the product as accurately as possible when posting and give some tips for buyers to prevent fraud. As a guarantee intermediary, the market operation does not prohibit any products or services. Posting tutorial products needs to explain that why vendors cannot do this by themselves and describe the potential risks. Otherwise, they will not be allowed to advertise. In a prominent position on the website, it is reminded that external connections and external communications are not allowed. Tea Horse Road forbids child abuse, unethical resources, materials to subvert state power, and political and political leaders related resources. In terms of communication, the website allows users to use off-site communication but avoid off-site transactions. Also, the website does not explain whether it is possible to use external websites, but we did found clean net links and other external websites in some product descriptions.

4) Payment Method: In the Chinese Exchange Market, the on-site wallet mode is used. The user needs to transfer Bitcoin to the Bitcoin wallet of the market administrator. The corresponding amount will be shown in their account on the market. On the advertisement post, the price is displayed in USD and Bitcoin. Tea Horse Road also uses the on-site wallet mode. The market allowed adding credit to their wallet by Bitcoin and Tether. Moreover, a difference with the Chinese Exchange Market is that users are allowed to use common fiat currency with daily payment methods, including Alipay, Wechat, and even debit cards, by contact market-authorized exchange via Telegram. On the advertisement post, the price is displayed in USD and Bitcoin.

5) Security Mechanisms: In both Chinese language markets, the crawling restrictions are easy to bypass. Both use simple four character letters and numbers combination CAPTCHAs when login-in. Figure 16 shows the CAPTCHAs in both Chinese darknet markets. Both markets lack request limitations. In order to avoid any bandwidth stress, we also applied a dynamic delay of 0.5 seconds to 2 seconds with a low number of concurrent requests. Hence, this causes the total crawling time to vary from four hours up to 12 hours. In terms of the structure of the cookies, the Tea Horse Road uses a dynamic approach in which it will change every time a request is sent. It does not seem to affect the crawling process, but was noticed when setting up the initial cookie and we let the program follow up. We also noticed that the post page URLs are consecutive. This may lower the website's security level because of the potential for exhaustive cracking and crawling. Overall, both markets have low level crawling restrictions.

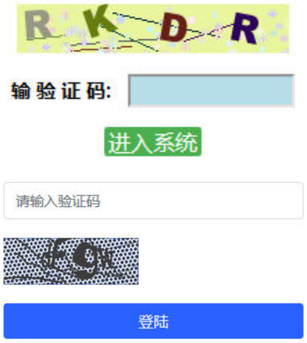


Fig. 16: CAPTCHA Samples from Chinese Darknet Markets

In terms of the user account, the two Chinese darknet markets have different mechanisms. In the Chinese Exchange Market, the user only needs to set a password. Then the website will assign an ID to the user. Interestingly, this user ID is a counter, which means that every time a new account is registered, the ID is increased by one. We tracked back our dataset and found that the ID is very likely to increment by 1. Our latest data shows that this ID is currently 677653. Although this is certainly not the number of active users in the market, it is the cumulative number of registered users in the market since its inception. The user needs to subscribe to the "post" and "reply" types of activity, respectively, to post and buy. The "post" cost 0.00024 and 0.0006 Bitcoin for three months and one year, respectively. The "reply" cost 0.00012 and 0.0003 Bitcoin for three months and one year, respectively. In the Tea Horse Road, the user needs to set a username, password and payment password. The payment password is used when a user purchases a product. Accounts need to be activated before publishing or purchasing products. The user needs to pay $10 in equivalent Bitcoin for the activation. There are no account password recovery options in either market.

6) Key Takeaway: The Chinese darknet markets remain incomplete and less developed, but at the same time, they try to be innovative, for example by adding the request-to-buy mode. Vendors are less active than the English darknet markets. The cross-market vendors are hard to track as the vendor ID is made of immutable numbers (i.e. they cannot be personalised, which would allow more obvious cross-market tracking). Leaked/personal data is the most popular category.

There is no official policy to prohibit any products or services in the Chinese darknet markets we studied. Bitcoin is the main payment method, however, fiat currency has also been accepted in Tea Horse Market. The Chinese darknet markets usually have less strict crawling restrictions.

C. Comparison of Darknet Markets in English and Chinese

The differences between the Chinese and English darknet markets are reflected in many aspects. This section focuses on the market and vendors characteristics.

1) Market: **Operation model and structures.** English darknet markets tend to be a real online market, while Chinese darknet markets tend to be more similar to forums. Some built-in functions in the English darknet markets, such as credit systems, feedback systems, build a mature ecosystem. In the Chinese darknet markets, they only serve as an intermediate platform for posting. It is, therefore, quite difficult for users to judge the credibility of the vendor. In terms of novelty, one of the Chinese darknet markets provides request-to-buy mode. Users are no longer limited to browsing the displayed products but can make a request, which can be customised. The website structure of the Chinese darknet markets is simple but functional and helps locating products faster. Nevertheless, considering the profitability of the market itself, the English darknet markets are usually mixed with promotional products in all lists, and the promotional items are difficult to distinguish. On the other hand, in homepages, the English darknet markets use both pictures and text, while the Chinese darknet markets only have text. Physical items often need more pictures to display, while virtual items could use descriptive text only. This phenomenon reflects that different strategies apply to different types of popular products in different language darknet markets.

Product category. Drugs dominate the English darknet markets, while in the Chinese darknet markets the most popular category is personal data. Due to the convenience of express delivery in North America and Europe, and the different laws and regulations of each state or country, drug shipments are difficult to spot and stop. However, Chinese law enforcement is characterised by a heavy crackdown, deep inspection, severe sentencing, and heavy propaganda against drugs abuse. As of 2020, the number of drug abuse users in China has kept falling for three years in a row [27]. Regarding personal data, Chinese LEAs have been cracking down on telecom fraud in recent years. Most of them are related to the leakage of personal information. Due to the convenience of disseminating virtual items such as personal information, it is difficult to stop it. Pornography is the second-largest category in the Chinese darknet markets, which also contains child abuse. In the English darknet markets, they are clearly stated that child abuse is not allowed.

Market policy. English darknet markets restrict most high-risk products, such as arms, chemical weapons, child abuse, animal abuse, etc. There are no special restrictions on items in the Chinese darknet markets, but fraudulent behaviours with fake products in the market will be banned.

Payment method. Bitcoin is still the main currency in both English and Chinese darknet markets. Most English darknet markets also accept Monero for better privacy. Users can use fiat currency for small deposits in Chinese darknet markets.

Security mechanisms. The English darknet markets usually have stricter security measures than Chinese ones. More complex CAPTCHAs are used in the English darknet markets. The session time in the English darknet market usually has different time-window options, but it must be within a certain number of requests. Otherwise, users will be kicked out. However, since there is usually no limit on the number of requests in Chinese darknet markets, as long as the session is active, it will not be automatically logged out. In terms of account security, the Chinese darknet markets use the pay-to-activation method to control malicious registration, while the English darknet markets use the PGP public key.

2) Vendors: **Inactive days**. Vendors in the English darknet markets are more active than the Chinese darknet markets. The English darknet markets usually have a shorter life cycle. The three English darknet markets were established later than the Chinese Exchange Market. In the past, most English darknet markets were being shut down or exit scams at the end, and then those market operators will usually change their identities and operate new markets. The new vendors in English darknet markets will remain active and establish their brand in dark web forums. Even if the market is closed, they can quickly sell in the new market because buyers usually follow good vendors. However, in Chinese darknet markets, even if the operators scam, they would not exit the market. They keep the operation as new vendors will not know because of lack of communication. Vendors in the Chinese darknet markets do not have to consider such feedbacks, so they also spend less time in the market for such customer service. By comparing Figures 6 and 15, we can clearly find that some vendors are not active within a few months after posting their posts in the Chinese darknet markets. On the contrary, most vendors were still active in the English darknet market, even over a year after they first registered.

Location. In the English darknet markets, the proportion of international vendors is greater because of the widespread use of English. For instance, some non-English speaking countries in Europe have more lax drugs regulation, contributing to some vendors from such countries. In comparison, we found that most of the vendors in the Chinese darknet markets are native speakers, as indicated by the jargon being used. However, since mostly virtual products and pornography are sold, the vendor's real geographic location is difficult to measure.

Behaviour. Vendors in the English darknet markets pay more attention to building their own brands. They usually use their vendor profile or description section to promote themselves. Successful vendors claim and show their sales numbers and ratings in other well-known English darknet markets. They also explain the return policy, e.g. what will happen if the items are lost in transit. Vendors sometimes update new products or their personal status. In the Chinese darknet markets, it is difficult for the vendor to do the same in the English darknet market because of the lack of functionality. However, we noticed that vendors in the Chinese darknet markets sometimes have their own language style, but it is still difficult to define the cross-market actors.

V. Discussion

A. Insights

In comparison to their English counterpart, even though the ecosystem in the Chinese darknet markets remains incomplete and less developed, it tries to be innovative, for example by adding new selling modes. The lack of any feedback and rating system likely contributes to make the vendors slightly less active. Chinese markets seem to serve mainly as a safer first point of contact rather than a full trading platform. Goods exchanges and price negotiations are likely to be carried out of the market, using other means of communication. We observed that both of the analysed Chinese darknet markets have a "private deal" section, allowing vendors to trade with specific target buyers. With the request-to-buy mode, buyers have more options than in English darknet markets. Chinese darknet markets may be improving and upgrading the functionality and security of their services by learning from the practices of English darknet markets. Moreover, as automated language translation becomes more and more accurate, markets in different languages can be accessed without the need for complex applications. That could become a new challenge for us. On the other hand, we can delve into how to use those technologies against crimes too, for example by creating a system that can detect cross-market illegal activities.

Chinese darknet markets have less stringent policies than English darknet markets. There are resources for child abuse, weapons and hire-to-harm in the Chinese darknet markets. The administrators usually do not care about the products sold, which is not the case in the English darknet markets. English darknet market administrators have also began to focus on the quality of their products, for example by implementing the Product Quality and Harm Reduction programmes.

All markets suffer from reputation issues. On English dark web forums, we can see discussions or comments for each English darknet market. New markets will always appear, and most of the old markets will always gradually lose vendors and buyers for some reasons. Some closed down, either being seized or the operators performed exit scam. The Chinese darknet navigation website also displays comments from anonymous users on the Chinese darknet market. They usually complain about customer service and potential scamming activities. We may be able to explore such methods using specific indicators to predict scams before widely occurring.

Cross-market actors are active. We have seen the same vendors in all major English darknet markets. We speculate that international vendors are likely, especially for personal data, in both English and Chinese darknet markets. We found that the personal information data sold in markets contain leaked data from all over the world. Cross-market behaviour exists, and even on dark web forums, they use the vendor's identity to participate in discussions. It should be noted that this may also be one of the means to promote their own items. We also observed that they use other accounts to assume other identities. If we can track and link these accounts, we will be able to understand e-crime operations better.

B. Challenges

The main technical challenge we faced is the many restrictions these markets implement to stop or at least slow down automatic crawling and scraping of their websites. This is, obviously, a serious challenge for data collection. This is compounded with the instability of the Onion service, resulting in frequent but irregular interruptions to the data collection process. In addition, we must manually log in to each of our accounts before starting the crawler in order to get the cookies needed for the session. English markets are severely more restrictive in their anti-crawling measures, so we needed to maintain and operate multiple accounts simultaneously. In addition, markets operators frequently change the structure and the design of their websites, sometimes causing crawlers to fail. At times, markets operators update their security mechanisms without any notice, typically in ways that are damaging for bots but transparent for humans. For instance, Cartel Marketplace updated their CAPTCHAs, and the Tea Horse Road also redacted the number of requests per session. In each of those cases, we must reconfigure our crawler. So data gathering becomes a continuous cat-and-mouse game, costly to maintain for large periods of time.

C. Limitations

Due to technical and time issues, there is an imbalance in the number of vendors between the English and the Chinese darknet markets. The more stringent crawling restrictions in the English darknet markets caused our crawler not being able to scrape all of the market content, resulting in a smaller amount of data being collected. In comparison, the Chinese darknet markets have less stringent restrictions, leading to more data points. Our dataset also contains a relatively short period of time in both English and Chinese darknet markets, so further work to expand our dataset would be worthwhile.

We have considered and dealt with bad data in our analysis, however, despite our best efforts, we still cannot guarantee the integrity of all the figures such as prices and sales in any darknet market. As such, figures presented in this paper are based on our best estimation, which can and shall be improved in follow-up research.

VI. Conclusion

In conclusion, this paper has investigated and analysed the differences between darknet markets using English and Chinese as their main languages. The differences found are, at times, quite interesting and have a basis that is not only linguistic but also cultural. For this research, we collected data from five trending darknet markets, comprising three English and two Chinese darknet markets. Data collection was carried out for seven consecutive weeks.

English darknet markets generally seem to offer a more mature and complete ecosystem, with more active vendors than their Chinese counterparts. We found that the multiple differences between English and Chinese darknet markets are reflected across many aspects, including selling modes, product categories, market policies, payment methods, security mechanisms and vendors. In Chinese darknet markets, vendors are on average less active than in English darknet markets, but the demand and number of sales of personal data and pornography are relatively large. In English darknet markets, the main product sold are drugs. Moreover, the policies of Chinese darknet markets show that there are very few products banned, and the problem of child abuse material is extremely serious. In one of the Chinese darknet markets, fiat currency can be used, and the anti-crawling restrictions in both of the observed Chinese markets are easy to bypass.

Some interesting insights from our research is the existence of request-to-buy modes and some uncommon policy issues. We believe that these provide a way to gain comparative insights into darknet markets, and attract the attention of law enforcement agencies. In particular, this request-to-buy mode could be a good way to launch sting operations – where allowed by law. We hope that our study will provide a better understanding of darknet markets, particularly Chinese darknet markets. Future work can focus on vendor behaviour and cross-market operations in different language darknet markets. For instance, by using natural language processing techniques, we may be able to discover connections between vendors and identify potential cross-market international large-scale operators. Finally, the tracking of payment methods and profits is an additional interesting research path for the future.

REFERENCES

[1] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," Naval Research Lab Washington DC, Tech. Rep., 2004.

[2] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous connections and onion routing," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 482–494, 1998.

[3] U.S. Attorney's Office, "Ross ulbricht, the creator and owner of the silk road website, found guilty in manhattan federal court on all counts," 2015. [Online]. Available: https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-the-creator-and-owner-of-the-silk-road-website-found-guilty-in-manhattan-federal-court-on-all-counts

[4] A. Hern, "Us seizes $1bn in bitcoin linked to silk road site," the Guardian, Tech. Rep., 2020, accessed: 10 December 2021. [Online]. Available: https://www.theguardian.com/technology/2020/nov/06/us-seizes-1bn-in-bitcoin-linked-to-silk-road-site

[5] CNWest, "The "clean net" operation launched, six departments worked together to rectify harmful information on the internet," *CNWest*, 2021, accessed: 10 December 2021. [Online]. Available: http://news.cnwest.com/tianxia/a/2021/06/08/19728920.html

[6] N. Christin, "Traveling the silk road: A measurement analysis of a large anonymous online marketplace," in *Proceedings of the 22nd International Conference on World Wide Web*, ser. WWW '13. New York, NY, USA: Association for Computing Machinery, 2013, p. 213–224. [Online]. Available: https://doi.org/10.1145/2488388.2488408

[7] R. van Wegberg, S. Tajalizadehkhoob, K. Soska, U. Akyazi, C. H. Ganan, B. Klievink, N. Christin, and M. van Eeten, "Plug and prey? measuring the commoditization of cybercrime via online anonymous markets," in *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 1009–1026. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/van-wegberg

[8] A. V. Vu, J. Hughes, I. Pete, B. Collier, Y. T. Chua, I. Shumailov, and A. Hutchings, "Turning up the dial: The evolution of a cybercrime market through set-up, stable, and covid-19 eras," in *Proceedings of the ACM Internet Measurement Conference*, ser. IMC '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 551–566. [Online]. Available: https://doi.org/10.1145/3419394.3423636

[9] K. Soska and N. Christin, "Measuring the longitudinal evolution of the online anonymous marketplace ecosystem," in *24th {USENIX} security symposium ({USENIX} security 15)*, 2015, pp. 33–48.

[10] A. Abbasi, W. Li, V. Benjamin, S. Hu, and H. Chen, "Descriptive analytics: Examining expert hackers in web forums," in *2014 IEEE Joint Intelligence and Security Informatics Conference*, 2014, pp. 56–63. [Online]. Available: https://ieeexplore.ieee.org/document/6975554

[11] V. Benjamin and H. Chen, "Securing cyberspace: Identifying key actors in hacker communities," in *2012 IEEE International Conference on Intelligence and Security Informatics*, 2012, pp. 24–29. [Online]. Available: https://ieeexplore.ieee.org/document/6283296

[12] B. Collier, R. Clayton, A. Hutchings, and D. Thomas, "Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies," *Workshop on the Economics of Information Security*, 2020. [Online]. Available: https://www.repository.cam.ac.uk/handle/1810/306682

[13] P. H. Meland, Y. F. F. Bayoumy, and G. Sindre, "The ransomware-as-a-service economy within the darknet," *Computers & Security*, vol. 92, p. 101762, 2020.

[14] S. Pastrana, A. Hutchings, A. Caines, and P. Buttery, "Characterizing eve: Analysing cybercrime actors in a large underground forum," in *International symposium on research in attacks, intrusions, and defenses*. Springer, 2018, pp. 207–227. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-00470-5_10

[15] N. Christin, "An eu-focused analysis of drug supply on the alphabay marketplace," *EMCDDA commissioned paper*, 2017.

[16] M. Yip, C. Webber, and N. Shadbolt, "Trust among cybercriminals? carding forums, uncertainty and implications for policing," *Policing and Society*, vol. 23, no. 4, pp. 516–539, 2013. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1080/10439463.2013.780227

[17] T. J. Holt, "Examining the forces shaping cybercrime markets online," *Social Science Computer Review*, vol. 31, no. 2, pp. 165–177, 2013. [Online]. Available: https://doi.org/10.1177/0894439312452998

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

[19] G. Zhou and J. Zhuge, "Adapting to local conditions: Similarities and differences in anonymous online market between chinese and english speaking communities," in *International Conference on Digital Forensics and Cyber Crime*. Springer, 2020, pp. 164–181.

[20] Alsayra, "April 5, 2011-may 1, 2012. azsecure-data.org version," 2015. [Online]. Available: http://azsecure-data.org/getdata/forums/alsayra.txt

[21] G. Branwen, N. Christin, D. Décary-Hétu, R. M. Andersen, StExo, E. Presidente, Anonymous, D. Lau, D. K. Sohhlz, V. Cakic, V. Buskirk, Whom, M. McKenna, and S. Goode, "Dark net market archives, 2011-2015," July 2015, accessed: 23 November 2021. [Online]. Available: https://www.gwern.net/DNM-archives

[22] S. Pastrana, D. R. Thomas, A. Hutchings, and R. Clayton, "Crimebb: Enabling cybercrime research on underground forums at scale," in *Proceedings of the 2018 World Wide Web Conference*, ser. WWW '18. Republic and Canton of Geneva, CHE: International World Wide Web Conferences Steering Committee, 2018, p. 1845–1854. [Online]. Available: https://doi.org/10.1145/3178876.3186178

[23] I. Albery and M. Munafò, *Key concepts in health psychology*. Sage, 2008.

[24] D. Kouzis-Loukas, *Learning Scrapy*. Packt Publishing Ltd, 2016.

[25] J. Redman, "After empire's exit scam, darknet market patrons scramble to find alternatives," *bitcoin.com*, 2020. [Online]. Available: https://news.bitcoin.com/after-empires-exit-scam-darknet-market-patrons-scramble-to-find-alternatives/

[26] European Monitoring Centre for Drugs and Drug Addiction and Europol, "Drugs and the darknet: perspectives for enforcement, research and policy," 2017.

[27] China Anti-drug, "China's drug situation 2020 report," 2021. [Online]. Available: http://www.nncc626.com/2021-07/16/c_1211244064.htm