Shedding Light on Monopoly: Temporal Analysis of Drug Trades

Daniel Dolejška(✉), Vladimír Veselý, Jan Pluskal, and Michal Koutenský

Faculty of Information Technology, Brno University of Technology, Božetěchova 1/2, Brno, Czech Republic
{dolejska,veselyv,ipluskal,koutenmi}@fit.vut.cz
https://fit.vut.cz/

Abstract. Dark marketplaces pioneered a new way to monetise illicit goods. A unique combination of technologies (such as overlay networks, end-to-end encryption, and cryptocurrencies) guarantees anonymity for dark marketplace users (including operators, vendors, and buyers).

We have developed a tool for monitoring and investigating dark marketplaces (namely, collecting and processing evidence directly from their websites), which we used for real-time detection of various illicit activities.

This paper presents a well-described and structured dataset that contains high-frequency web-scraped information from Monopoly Market (one of the most popular dark marketplaces in 2021). The evaluation demonstrates how high-resolution temporal analysis can reveal mission-critical information about the frequency of trades, vendor activities, and the drug market.

Keywords: dark market · drug trade · illegal trade · purchase detection · temporal data set · market analytics · web scraping · dataset · crypto · cryptocurrency · dark marketplace · cryptomarket

1 Introduction

The dark web offers users a high level of anonymity, resulting in a digital environment that encourages nefarious activities by design. That goes hand in hand with increased interest from cybersecurity researchers and law enforcement agencies (LEAs), who are the primary audience for this paper. While the first group is investigating the dark web because they want to, the second group is doing the same thing because they need to. Especially LEAs in charge of countering cybercrimes, preventing the distribution of child sexual abuse materials, and fighting illegal trades with drugs and firearms are also focused on dark marketplaces.

1.1 Motivation

Dark marketplaces are analogous to e-commerce shopping malls from the surface web. Vendors offer their products to potential buyers through listings that

S. Goel et al. (Eds.): ICDF2C 2022, LNICST 508, pp. 151–168, 2023.
https://doi.org/10.1007/978-3-031-36574-4_9

contain product descriptions, prices, and delivery options. Buyers give the score and provide reputation comments to vendors based on their customer experience (e.g., quality of products, duration of delivery). Dark marketplace operators resolve disputes (e.g., via escrow) and receive fees from each trade.

LEAs target dark-market vendors (usually for distributing illegal commodities) and operators (usually for trafficking and money laundering). We, cybersecurity researchers, cannot credibly comment on LEA methods and approaches. Nevertheless, we assume that: a) the vendor's investigation pursues to uncover individual(s); b) the operator's investigation attempts to discover a server hosting a dark marketplace. Any successful investigation most probably involves the application of open source intelligence (OSINT, as an enabler for the Alpha Bay case [16]), human intelligence (HUMINT, its importance was shown during the Silk Road case [17]), and interception of delivery chains [9].

Our work is inspired by previous attempts to conduct a similar long-term monitoring of dark marketplaces such as [14,19], or [18]. These works have also been used by LEAs as an essential source of information when investigating criminal activities [11]. The difference between our approach and the works mentioned above is that we use up-to-date programmatic tools (enabling us to overcome particular limitations encountered by our predecessors), which allows us to web-scrape more data at a higher frequency, resulting in more granular and detailed analytical output.

1.2 Problem Statement

The conditions and circumstances regarding datasets on dark marketplaces pose a challenge that limits their general availability. The existence of such markets is very ephemeral compared to the surface web, which means that much more work needs to be done to discover and monitor them. Marketplaces appear, disappear, and reappear at various points in time at multiple locations on the dark web.

In addition, these markets are designed to be hidden and resilient and, as a result, employ numerous mechanisms to make accessing them more complex than their surface web counterparts. Their technology stack (depicted in Fig. 1) includes the following:

- *overlay network* (e.g., Tor, I2P), which provides network layer anonymity, IP traffic encryption, and covert hosting services;
- *end-to-end encryption* for communication (such as PGP for emails/files, 7z/RAR file archives) on the application layer and above it;
- *cryptocurrency* (e.g., Bitcoin, Monero, Litecoin) as a fast, decentralised, and trustless carrier of value;

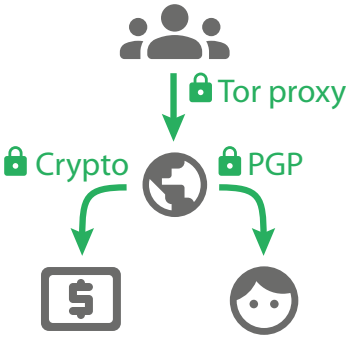

Fig. 1. Darkmarket Technology Stack. This figure shows a visualisation of the technology stack used.

– *anti-crawling protection*, such as URL rotation or CAPTCHA [1] verifications, to hinder any kind of automated web processing workflow.

Although technical challenges can always be overcome, another aspect needs to be considered, which refers to the nature of the data collected. As dark markets are commonly used for illicit activities, information on them is of great interest to LEAs. Public disclosure of which data are being collected or what is possible to collect, using which methods can be viewed as undesirable and in direct opposition to the goals of LEAs, as it gives up an essential operational intelligence advantage. Therefore, data are often kept private to maximise their usability.

Commercial companies[1] focus on indexing and archiving dark web content. Such companies apply OSINT tools to scrape content from dark web pages periodically. Collecting dark web content may yield a Big Data problem. Due to that, these companies collect mainly textual data and provide full-text search capabilities within their products. However, textual form, which usually lacks temporal and contextual data, is insufficient for the primary audience of this paper. More intelligence is needed (including pictures, spotted differences, correlated blockchain events, etc.) to successfully understand the operation of a dark marketplace, which takes into account all involved actors (i.e., operators, vendors, buyers).

Therefore, we aim to explore new methods to investigate and analyse dark marketplaces.

1.3 Selection of Monopoly Market

In 2021, we thoroughly analysed trending dark marketplaces to select a good candidate for our web scraping platform prototype. Among the most notable features of Monopoly Market were:

– *accountless* website access, product browsing, and shopping (which would maintain our anonymity not associated with any account when browsing the site);
– completely *walletless* (to avoid exit scams), which mandates *direct deals* between users (i.e., the dark marketplace does not provide its users with a custodial cryptocurrency wallet. Hence, cryptocurrency transfers between users are visible on the blockchain);
– only *single-product orders* are possible;

[1] On the one hand, we purposely do not want to mention the name of any company or product. On the other hand, we want to provide at least some leads for the reader interested in getting more information. Therefore, we advise checking out participants of commercial cybersecurity conferences for LEAs such as ISS World, Milipol, or Security and Policing.

– relatively *simple CAPTCHA* prompts when accessing the website (unlike hard-to-overcome "community-driven" aliveness check called EndGame: Onion Service DDOS Prevention Front System[2]);
– link distribution network (LDN) always provides a reliable point through which to get the most up-to-date marketplace address;
– leveraging Bitcoin as a primary cryptocurrency (compared to these dark marketplaces, which prefer cryptocurrency with built-in obfuscation techniques such as Monero, Zcash, or Dash).

However, the features listed above were not only appealing to users of Monopoly Market. They are also precious to any third party interested in automated monitoring of websites that use them. The account-less feature for website access, the use of reasonably simple CAPTCHA challenges, and a presence of a dedicated LDN have allowed more straightforward automation of the entire web-scraping process. Furthermore, the features and content structure of Monopoly Market aligned well with our intention to correlate the detected trades with comparable transactions on the Bitcoin blockchain.

Monopoly Market[3] was one of the e-commerce-based marketplaces (see Sect. 2.1 for details on classification). The launch of this website was announced [5] in August 2019. Monopoly Market became particularly popular in 2021.

This applies especially after the publication of White House Market (WHM) retirement announcement [6]. WHM was one of the largest and most popular marketplaces at that time with 326,570 active user accounts [6] and more than 45,000 advertised product listings [2]. Monopoly Market has been explicitly mentioned in the announcement as a viable alternative for active WHM users [6]. However, that was just a few weeks before Monopoly Market went dark itself [7,8] in late December 2021.

1.4 Contribution

The outcomes of this paper are intended for anyone who is (hopefully just) researching the dark web. Our results may also interest LEA representatives investigating generally dark marketplaces (not only Monopoly Market). This paper has two main ambitions:

1. to provide the research community with a dataset containing real-life information collected not only during a one-time run but periodically (approximately one year) from a single dark marketplace (i.e., Monopoly Market);
2. to demonstrate how such a dataset (enhanced with temporal dimension) can reveal mission-critical information about dark marketplace operation and activities of its users.

[2] Publicly available source code can be found on this GitHub repository https://github.com/onionltd/EndGame.
[3] Review available at https://darknetlive.com/markets/monopoly-market/.

The paper is structured as follows. Section 2 outlines currently available datasets targeting dark marketplaces and briefly elaborates on dark marketplace typology and monetising models. Section 3 thoroughly describes a) the syntax and semantics of the data within the dataset; b) their relations; and c) their quality with respect to the collection process. Section 4 selects a relevant subset of purchase detection data and illustrates its temporal dimension together with its analysis. Section 5 concludes the paper with some provocative findings and indicates the next steps in the publication of our research.

2 State of the Art

Dark marketplaces may seem like emerging technologies, but their history, in various forms, spans the roots of the Internet. At least in the time when the Internet generally became available for the masses to use. These markets have not always been hidden behind overlay networks, but in the beginning, they have been a part of the surface web on IRC, web forums, regular e-commerce sites and others. [20].

The driving force behind the dark web/darknet/hidden web/cryptonet, call it as you like, may be traced back to like-minded people as Tim May, the author of "Crypto Anarchist Manifesto" [12]. Rereading it with hindsight, we believe you agree that his prediction matches the current state two decades later. This work predicts that illicit activities will be conducted over anonymisation networks using cryptographical principles and that trust between the transacting parties will be based on their reputation.

The most popular, one of the first dark markets as we know them today, was the Silk Road marketplace, launched by Ross Ulbricht in 2011 and operated until 2013. Detailed analysis provided by Christin [4] explains his investigation methodology and crawling approach (each run on average 14 h) focused on the details of the items sold and the collection and analysis of the vendor rating (customer feedback). Christin and Soska update the dataset [14] with data from 16 different marketplaces over more than two years (2013- 2015). With the help of Tai, Soska and Christin created the resulting dataset [15] as a combination of multiple sources covering eight years (2011–2018), 12 marketplace websites, and 996 snapshots.

A very unorthodox dataset was created by Buskirk et al. [18], who manually (in opposition to automated crawling) collected almost 1150 weekly snapshots of a total of 39 active cryptomarkets during October 2013-November 2015. Manual collection allowed visual verification and filtration of misleading data obtained during market downtime. The extraction of structured data was done manually using Excel and macros.

The most notable dataset is Darknet Market Archives (DNM) [3], which is a collection of 89 marketplaces and more than 37 forums, totalling about 1.6 TB of publicly available data. These data were scraped mainly between 2013 and 2015, with some older entries (2011–2012), at daily or weekly intervals. The content is categorised first by source and then by the date on which it was obtained.

The data format varies; some of it is in the "raw" form of HTML/CSS and accompanying media files, but the dataset also includes processed structured CSV files. Despite its age, it remains a popular and comprehensive dataset and was used by the scientific literature as recently as 2022.

A more recent effort is the AZSecure dataset [10]. Compared to DMA, it is much more focused on its vision. The AZSecure dataset is mainly interested in cybersecurity threats and contains both marketplaces and communication channels such as forums and IRC channels. This dataset contains information from 12 dark markets gathered between 2016 and 2018, with roughly half of all listings belonging to the Dream Market. It is not stated how often the scraping was performed. The dataset itself contains only structured information about the sellers and listings collected.

2.1 Typology of Dark Marketplaces

How the marketplaces are presented may differ. Online forums were regularly used by people to create posts in moderated categories when they needed to buy or sell something. E-shops will be user-friendly and guide the user through the shopping experience, including payment and delivery information [13].

Dark marketplaces in the form of community forums do not account for most marketplaces. However, this allows for greater flexibility in the products or services demanded or sold. The listings have to be correctly categorised. Forums are more versatile than e-commerce-based services, although they lack their counterparts' simplicity and ease of use.

The e-shop-based services are considerably more user-friendly for vendors and customers alike. They provide a familiar environment to their users and define an easy-to-understand management interface for the shop. Hosting and managing such services should be considerably easier than running a forum-based community. There are two main branches to the e-shop-based services:

1. *vendor shops*, where the operators of such services usually sell their own goods directly without any external vendors present;
2. *marketplaces* whose operators aim to provide a reliable platform for other vendors to sell their goods at (under a commission).

In summary, marketplaces may take many forms, but, ultimately, they are the places where illicit online trades occur.

2.2 Monetising Models

The wallet-less marketplaces, such as Monopoly Market, cannot force users to move their funds into their web account wallet (and thus into the hands of service operators) before making a purchase. This reduces the risk of fund loss for any customer as they completely control their funds until the product payment itself. When the purchase is handled in a direct deal mode (shown in Fig. 2), this risk is even further reduced since the funds go from the customer directly to the vendor and not to the marketplace itself.

An alternative mode is an escrow deal, shown in Fig. 3. This happens when the customer pays for their order through the marketplace. This, in turn, gives the money to the vendor later, depending on whether the delivery is confirmed or disputed by the customer.

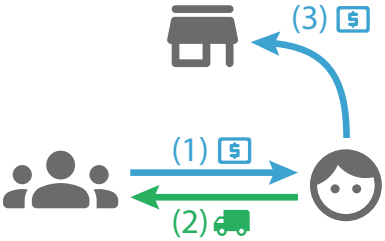

Fig. 2. Direct Deal Payment. (1) First, the user sends their funds directly to the vendor wallet. (2) After the order is paid, the vendor ships the order. (3) Finally, the marketplace receives a commission.

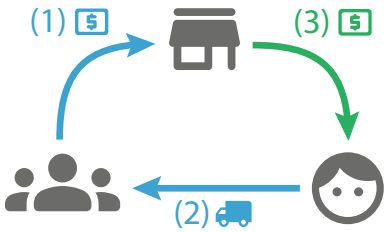

Fig. 3. Escrow Payment. (1) First, the user sends their funds to the marketplace escrow wallet. (2) After the order is paid, the vendor ships the order. (3) Finally, the vendor receives their portion of the payment.

3 Dataset

Existing datasets generally focus on complete snapshots of multiple websites, mainly dark marketplaces, IRCs, and forums. Snapshots include HTML, CSS, JavaScript files, images, fonts, and more.

Our dataset targets only a single darknet market website, namely Monopoly Market. It does not contain full web page snapshots but specific and structured data already extracted from the web page source code. The main feature is the temporal dimension of the data. Data have been periodically extracted, approximately every 15 min for over 10 months, from the website with a focus on information on available products and purchase detection.

This level of temporal resolution provides a unique opportunity to examine and analyse dark marketplace operations in unprecedented detail. Product purchase detection can be used to cross-correlate with public cryptocurrency blockchains or any other relevant open-source or network intelligence.

The structure and content of the dataset are described in detail in Sect. 3.1. Section 3.2 quantitatively describes the features of this dataset. Various visualisation analysis demonstrations are shown in Sect. 4.

3.1 Content Description

The collection of source data focused mainly on the detection of product purchases. However, it also contains additional information from the marketplace:

- **vendor usernames** and their:
  - corresponding **PGP key history** with pre-extracted **key metadata** (such as user-provided name, email, or time of creation),
  - **open order limit** history,
  - **open order count** history,
- **product categories** and their tree structure,
- published **product listings** and their metadata of:
  - **country of origin**,
  - allowed **shipping destinations**,
  - listing **view count**,
  - **time of creation**,
  - and its **age**,
- product listing **sold-count** and **stock-count deltas** between scrapes,
- and historical marketplace-provided USD, BTC and XMR **exchange rates**.

The data are separated into various tables; relationships between the tables can be seen in Fig. 4 (page 9). The complete schema diagram of the database can be found in Fig. 11 on page 16. The tables included in the dataset are as follows:

`pgp__items` Contains unique PGP public keys, their fingerprints, and the time of the first scraping encounter.
`pgp__meta` Contains extracted public PGP key metadata, such as exact time of creation, user name, user mail, and subkey data.
`product__items` Contains basic information on unique products: their category, name, and vendor.
`product__categories` Contains unique product categories. Defines a tree structure with parent and subcategories.
`product__variant__items` Contains all unique variants that can be purchased for each advertised product, a combination of the amount of the product and the shipping options.
`product__variant__prices` Contains historical prices of all variants of products in USD, BTC, and XMR.
`service__items` Contains records of monitored services, in case of this dataset only Monopoly Market.
`service__urls` Contains recorded and used `.onion` URLs belonging to services.
`vendor__items` Contains basic information on unique vendor accounts: their name and time of the first scraping encounter.
`vendor__keys` Contains links between vendor accounts and the public PGP keys used by them.

The dataset itself is available in CSV format, where the contents of each table are located in a single CSV file under the name of the source table. Furthermore, the schema of the database tables can be created using prepared PL/pgSQL scripts, which are also part of the provided archive. For access conditions and download instructions, see Sect. 5.

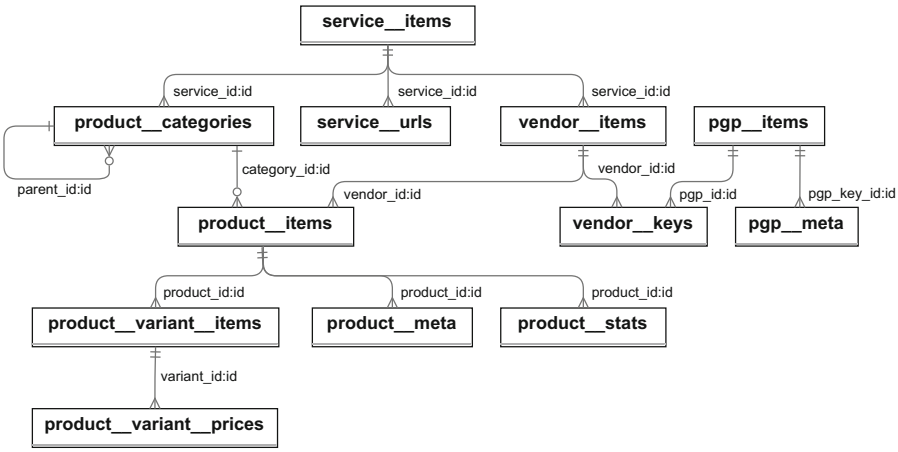

Fig. 4. Simplified Entity Relationship Diagram. This UML diagram displays relationships (foreign keys in relational databases) between tables from the source database.

3.2 Metrics

The first record in the dataset is from 25$^{\text{th}}$ February 2021, about a year and a half into the existence of the marketplace. The dataset ends with the last record from 28$^{\text{th}}$ December 2021 at 07:54 UTC. The median timestamp between scrapes of all available product pages is 15 min and 44 s.

Although the objective was always to be as consistent in web scraping as possible, it proved very difficult. The counts of product pages visited each day can be seen in Fig. 5 (page 10). A decreasing trend in visit/scrape counts can be clearly seen almost throughout the entire dataset. This is due to the active efforts of marketplace operators to mitigate this kind of user behaviour. Time intervals without scraping count data were caused by downtime of the marketplace website or the scraping framework itself.

Empty data intervals (where no web scraping was done) can also be found. Multiple reasons may be responsible for these events, such as internal software bugs, service availability issues, deployment problems, or active access prevention and security updates by marketplace operators. The most significant events are denoted in Table 1 (page 10). There are 64 of 307 days (20.8%) of scraping with complete outages. During these days, we do not have any monitoring data available.

The marketplace website has been monitored for 307 days. During that time, 211 different verified and active vendors were detected. Customers could browse a selection of more than 2,200 unique products related to controlled substances from all over the world. Almost 10,000,000 product page snapshots have been taken using web-scraping software. The corresponding and other counts of database table records can be found in Table 2 (page 11).

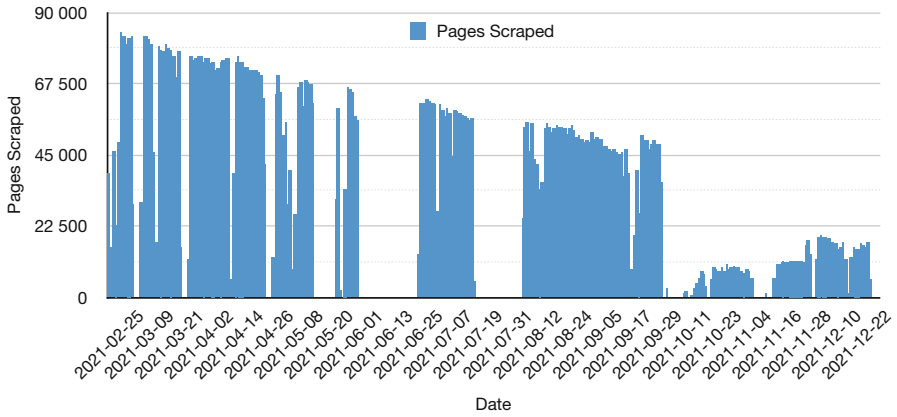

Fig. 5. Website Page Visits per Day. The Y-axis displays the total number of pages scraped daily (shown on the X-axis). A decreasing trend can be seen in the graph – this is due to the active efforts of marketplace operators to limit the amount of web scraping. A rapid drop can also be seen around 2021-09-29 – this signifies the time, when new anti-scraping prevention has been deployed on the marketplace.

Table 1. Data Acquisition Outages. This table displays various timespans during which there were issues with the web-scraping process. There are no monitoring data available in the dataset during these times.

From	To	Days	Reason
2021-03-08	2021-03-09	2	Development and deployment issues
2021-03-27	2021-03-28	2	Deployment issues
2021-04-30	2021-05-01	2	Development and deployment issues
2021-05-19	2021-05-26	8	Major SW optimisations and fixes, monitoring rework
2021-05-30	2021-05-30	1	Deployment issues
2021-06-06	2021-06-28	23	Major SW changes, automation and stability fixes
2021-07-23	2021-08-09	18	Major SW changes, automation and stability fixes
2021-10-06	2021-10-13	7	Implementation of new protection workaround
2021-10-24	2021-10-24	1	Deployment issues
Summary		64	Accounts for 20.8% of the dataset

Table 2. Database Table Sizes. This table shows the final disk usage of dataset tables in the database.

Table Name	Row Count	Data Size	Index Size	Total Size
`product__variant__prices`	78 949 534	6 045,4 MB	8 154,4 MB	14 200,1 MB
`product__meta`	61 973 933	4 462,5 MB	8 466,6 MB	12 929,4 MB
`product__stats`	9 865 452	756,9 MB	1 024,5 MB	1 781,8 MB
`product__variant__items`	26 187	3,3 MB	1,2 MB	4,5 MB
`pgp__items`	217	0,2 MB	0,0 MB	1,0 MB
`pgp__meta`	2 058	0,3 MB	0,2 MB	0,5 MB
`product__items`	2 231	0,4 MB	0,1 MB	0,5 MB
`vendor__keys`	217	0,1 MB	0,0 MB	0,1 MB
`vendor__items`	211	0,1 MB	0,0 MB	0,1 MB
`product__categories`	51	0,0 MB	0,0 MB	0,1 MB
`service__items`	1	0,0 MB	0,0 MB	0,1 MB
`service__urls`	31	0,0 MB	0,0 MB	0,1 MB

4 Evaluation

This section aims to demonstrate the analytic possibilities provided by this dataset and its unique temporal properties. First, various simple aggregation queries yield interesting counts and other analytics. There are records of 77,316 individual orders in more than 2,200 distinct products. These orders correspond to total minimum revenue (calculated from the price of the cheapest variant of the product) of 4,229,736 USD generated by the vendors; 5% of which (211,486.8 USD) is the commission of the market service (plus a bonus in the form of all funds in the escrow wallets after the shutdown of the marketplace). All the aforementioned statistics are calculated within the context of the whole dataset.

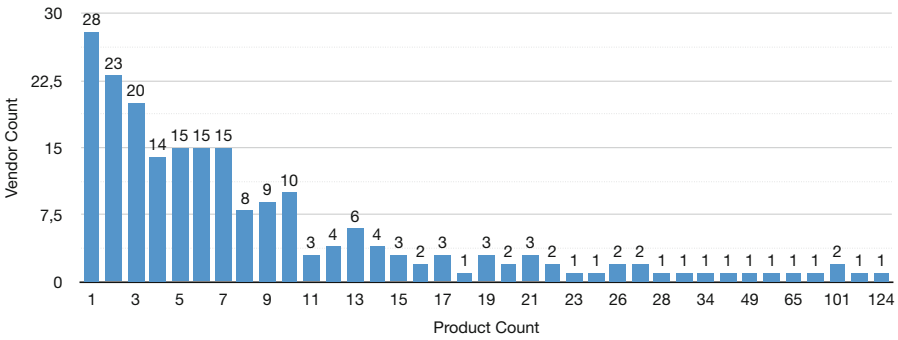

Fig. 6. Advertised product count by the number of advertising vendors. This chart shows how many products (X-axis) were advertised by how many vendors (Y-axis). It can be seen the graph follows the reciprocal distribution.

Figure 6 (page 11) shows how many products are advertised by how many vendors. It tells us that the upper 5% of the vendors (11) with the highest number of advertised products represents 35% of all available products (780) on the entire marketplace. As can be seen, there was a real mix of vendors active on this marketplace – some selling only a handful of products and some offering over a 100 distinct products.

Another possible analysis: show the number of purchases summarised by the country of origin of the corresponding product. The relevant visualisation can be seen in Fig. 7 (page 12). The chart shows us the most prominent countries featured on the marketplace. This strategic information is of interest to local governments and LEAs.

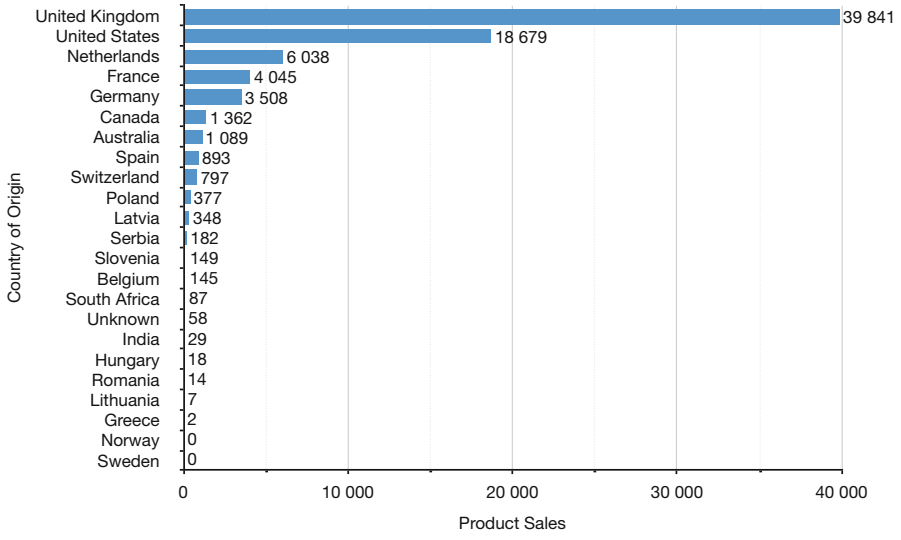

Fig. 7. Sales by a product's country of origin. This chart show a complete summary of all detected purchases by the corresponding product's country of origin.

Another analysis relates to vendors active on the marketplace website. Figure 8 (page 13) shows a weekly total count of verified and active vendors along with weekly change. The extent of information available about new vendors that become active can be closely related to their potential success on the website, the public opinion of the marketplace as a whole, and other significant events on the dark web, as shown and discussed by Nicolas Christin [4].

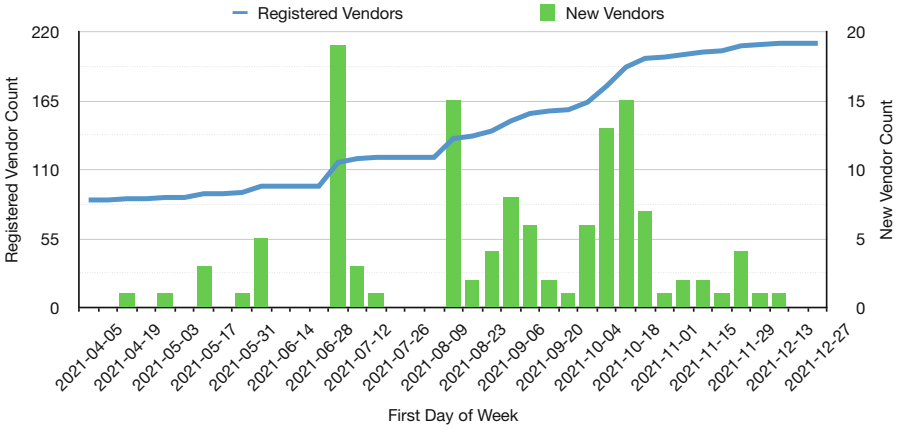

Fig. 8. Weekly count of verified and active marketplace vendors. This chart shows the number of verified and active vendors on Monopoly Market in the given week. A weekly change is also displayed as a separate series in green. (Color figure online)

Finally, plotting high-level trends among product categories can show deviations in the popularity of specific product categories in favour of others. This graph can be seen in Fig. 9 (page 14). Thanks to the temporal resolution of the dataset, these changes can also be detected on a scale of days/hours.

Visualisations leveraging the high-resolution temporal dimension of the data can provide unprecedented analysis of user activity on the marketplace. Figure 10 (page 14) shows the number of purchases detected during a given time interval, on the X-axis, in each day over a period of approximately 6 weeks (from 12$^{\text{th}}$ August to 22$^{\text{th}}$ September), on the Y-axis. Such data can reveal information about the primary demographics of customers on the marketplace, assuming people buy in between their regular day-to-day routine and not, for example, during the night when they would usually sleep.

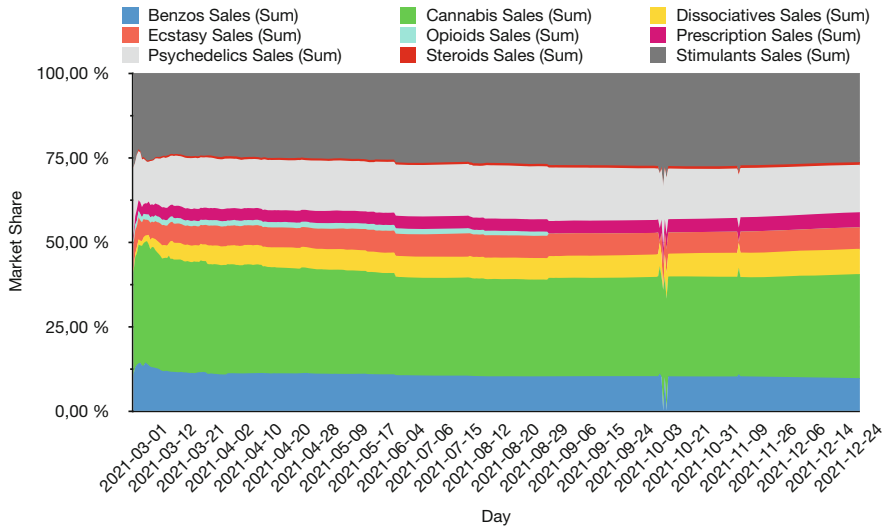

Fig. 9. Product category market shares over time. Displays purchase count share (in percentages) of product categories over the monitored timespan. *Note*: some days have been filtered out to prevent gaps and false values in the chart.

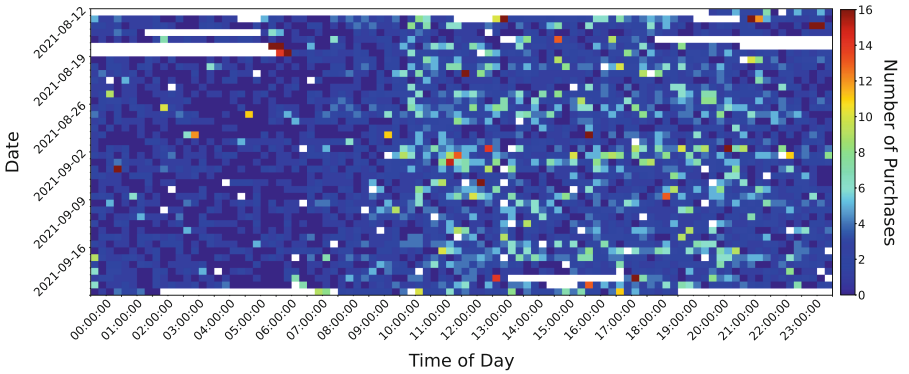

Fig. 10. Counts of detected individual product purchases over time. Visualises the number of individual product purchases detected by the automated scraping in a given time-of-day intervals (X-axis) of a given day (Y-axis). *Note:* white intervals represent that no records were collected during that time. Possible reasons include service outages, connection problems, CAPTCHA challenges or internal program issues.

5 Conclusion

This paper makes two significant contributions to anyone interested in dark web monitoring. First, we gathered and documented a unique dataset that observed activities in the significant dark marketplace during a year of its existence. This dataset is made available to fellow researchers and LEA representatives, who authenticate themselves by email using address from a verifiable domain owned by an academic or government institution. Please contact the leading author at their faculty email in order to receive your copy of the dataset. The results reproduction is available at the paper's webpage[4]. Secondly, we have shown the potential of such temporal data to corroborate evidence for both short- and long-term investigations involving dark marketplaces and their users.

As we have shown, this dataset has witnessed more than 77,000 drug trades by people from all over the world with unprecedented timescale detail. The most successful Monopoly Market vendor, NextGeneration, with more than 19,000 product sales, managed to generate an absolute minimum of 763,463 USD in revenue.

We plan to publish the dataset acquisition process. This would include comprehensive information on the automation of a) parallel access to the web pages; b) authentication, authorisation, and aliveness check bypassing; c) decoding and parsing of the web page content; and d) post-processing and archiving of extracted information. Our web scraping platform allowed us to monitor Monopoly Market so that we could use these data and correlate purchases with corresponding cryptocurrency transactions. As a next step, we would like to receive a peer review of this method and tooling.

The publication of this paper was possible thanks to the support from the Czech national research grant BAZAR (identifier VJ01030004, more information about the project is available at the project's website[5]) funded by the Ministry of Interior of the Czech Republic during 2021 and 2022.

Thanks also to the Brno University of Technology project FIT-S-20-6293 for allowing us to publish and present this paper in person at ICDF2C 2022 in Boston.

[4] https://gitlab.nesad.fit.vutbr.cz/papers/icdf2c22-shedding-light-on-monopoly.
[5] https://bazar.fit.vutbr.cz/.

A Figures

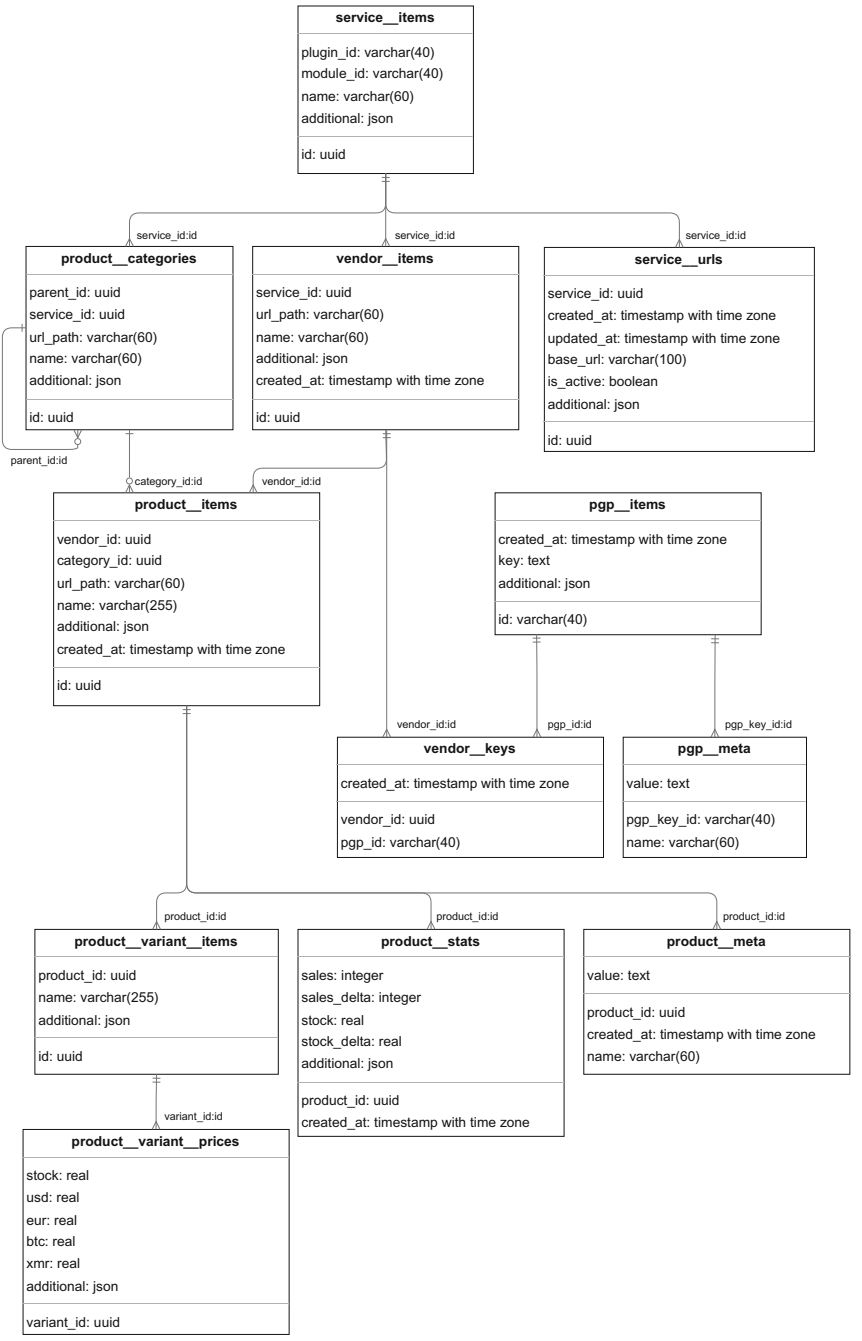

Fig. 11. Complete Dataset Database ER Diagram

References

1. von Ahn, L., Blum, M., Hopper, N.J., Langford, J.: CAPTCHA: using hard AI problems for security. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 294–311. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-39200-9_18
2. Barratt, M.J., et al.: Exploring televend, an innovative combination of cryptomarket and messaging app technologies for trading prohibited drugs. Drug Alcohol Depend. **231**, 109243 (2022)
3. Branwen, G., et al.: Dark net market archives, 2011–2015 (2015). https://www.gwern.net/DNM-archives. Accessed 27 June 2022
4. Christin, N.: Traveling the silk road: a measurement analysis of a large anonymous online marketplace. In: Proceedings of the 22nd International Conference on World Wide Web, pp. 213–224 (2013)
5. Darknetlive: Market announcement: Monopoly is open for business (2019). https://darknetlive.com/post/market-announcement-monopoly-is-open-for-business/. Accessed 29 June 2022
6. Darknetlive: PSA: White house market is retiring (2021). https://darknetlive.com/post/psa-white-house-market-is-retiring/. Accessed 29 June 2022
7. Darknetlive: Monopoly market and cartel market are gone (2022). https://darknetlive.com/post/monopoly-market-and-cartel-market-are-gone/. Accessed 29 June 2022
8. Darknetpages: Monopoly market and cartel market disappeared (2022). https://darknetpages.com/monopoly-market-and-cartel-market-disappeared/. Accessed 29 June 2022
9. Décary-Hétu, D., Giommoni, L.: Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of operation onymous. Crime Law Soc. Chang. **67**(1), 55–75 (2017)
10. Du, P.Y., et al.: Identifying, collecting, and presenting hacker community data: forums, IRC, carding shops, and DNMs. In: 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 70–75 (2018)
11. EMCDDA, E.: Drugs and the darknet: perspectives for enforcement, research and policy (2017)
12. May, T.: The crypto anarchist manifesto. High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace (1992)
13. Molnar, D., Egelman, S., Christin, N.: This is your data on drugs: lessons computer security can learn from the drug war. In: Proceedings of the 2010 New Security Paradigms Workshop, NSPW 2010, pp. 143–149. Association for Computing Machinery, New York (2010)
14. Soska, K., Christin, N.: Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. In: 24th USENIX Security Symposium (USENIX Security 2015), pp. 33–48 (2015)
15. Tai, X.H., Soska, K., Christin, N.: Adversarial matching of dark net market vendor accounts. In: Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, pp. 1871–1880 (2019)
16. United Nations Office on Drugs and Crimes: United States of America v. Alexandre Cazes aka "ALPHA02" aka "ADMIN" (2017). https://web.archive.org/web/20220702065615/https://sherloc.unodc.org/cld/en/case-law-doc/cybercrimecrimetype/usa/2017/united_states_of_america_v._alexandre_cazes_aka_alpha02_aka_admin.html. Accessed 07 July 2022

17. United Nations Office on Drugs and Crimes: United States of America v. Ross William Ulbricht, No. 15-1815-cr (2d Cir. May 31, 2017) (2017). https://web.archive.org/web/20220702065806/https://sherloc.unodc.org/cld/en/case-law-doc/cybercrimecrimetype/usa/2017/united_states_of_america_v._ross_william_ulbricht_no._15-1815-cr_2d_cir._may_31_2017.html. Accessed 01 July 2022
18. Van Buskirk, J., et al.: The recovery of online drug markets following law enforcement and other disruptions. Drug Alcohol Depend. **173**, 159–162 (2017)
19. Van Buskirk, J., Naicker, S., Roxburgh, A., Bruno, R., Burns, L.: Who sells what? Country specific differences in substance availability on the agora cryptomarket. Int. J. Drug Policy **35**, 16–23 (2016)
20. Wehinger, F.: The dark net: self-regulation dynamics of illegal online markets for identities and related services. In: 2011 European Intelligence and Security Informatics Conference, pp. 209–213. IEEE (2011)