In the market for a Botnet? An in-depth analysis of botnet-related listings on Darkweb marketplaces

Georgoulias, Dimitrios; Pedersen, Jens Myrup; Hutchings, Alice; Falch, Morten; Vasilomanolakis, Emmanouil

Published in:
Proceedings of Symposium on Electronic Crime Research 2023

Publication date:
2023

Document Version
Peer reviewed version

In the market for a Botnet? An in-depth analysis of botnet-related listings on Darkweb marketplaces

Dimitrios Georgoulias
Cyber Security Group
Aalborg University
Copenhagen, Denmark
dge@es.aau.dk

Jens Myrup Pedersen
Cyber Security Group
Aalborg University
Copenhagen, Denmark
jens@es.aau.dk

Alice Hutchings
Computer Laboratory
University of Cambridge
Cambridge, United Kingdom
alice.hutchings@cl.cam.ac.uk

Morten Falch
Cyber Security Group
Aalborg University
Cambridge, United Kingdom
falch@es.aau.dk

Emmanouil Vasilomanolakis
DTU Compute
Technical University of Denmark
Kongens Lyngby, Denmark
emmva@dtu.dk

***Abstract*—The Darkweb is highly popular and widely used for several types of cybercrime. Darkweb marketplaces in particular, are meeting places that provide anonymity, illegal product and service variety, and ease of use. Botmasters can utilize these platforms to acquire the necessary components needed to set up and maintain a botnet infrastructure, but also provide their services to clients. Since botnets can also be viewed from a business perspective, these components can be characterized as elements of a business model, each associated with a different botnet set of activities. In this paper, we crawl 26 marketplace and with focus on botnet-related listings form a dataset of 36,314 listings, along with 1,163 vendors. We present our aggregated findings in regard to marketplace characteristics, listings, and vendors. Additionally, we utilize the botnet *Value Chain Model* to correlate the targeted listings to specific model segments. With this approach we gain insight on how the business model relates to the botnet market in real time, and what significance this holds from a botmaster's point of view. Our results suggest that botmasters have a wide variety of options on all of the activities related to the botnet setup, maintenance, and revenue generation, all available within the marketplaces, at quite low prices. Lastly, we utilize the usernames and PGP keys of the vendors, in an effort to detect their potential cross-platform activity throughout the 26 platforms.**

***Index Terms*—botnets, darkweb, marketplaces, illegal trading, cryptocurrency, cybercrime, natural language processing**

I. Introduction

Cybercrime is a convenient pathway for malicious actors to easy profit through digital means. It is an ongoing threat that does not seem willing to go away. On the contrary, it seems that every year cybercrime becomes an even more successful venture. As reported in 2022 [1], cybercrime is on an ascending course, with damage costs increasing by 15% per year, until 2025 when it is estimated to reach 10.5 trillion USD [2]. Considering that in 2015 cybercrime caused 3 trillion in damages, the number disparity estimated to be created over the course of a decade is particularly troublesome.

A key part of the success that cybercrime has had over the years, is the anonymity that can be provided when one is operating in the cyber world. The *darkweb* plays a significant role in providing that anonymity to its users, be it for benign or malicious purposes. Apart from browsing the web without any compromise in privacy, the darkweb, and specifically the *Tor* network with its Hidden Service (HS) feature, has been established as a go-to meeting place for cybercriminals. HSs can only be accessed from inside the Tor network, and only if one knows the Tor equivalent of an IP address, called the *onion address*. Thanks to to their effectiveness in obfuscating both the source and destination of the traffic, they are being used for a large number of purposes with varying legality, ranging anywhere from *Facebook* and journalism forums, to ransomware gang sites, and illegal selling platforms.

Darkweb marketplaces are popular platforms and are widely used by individuals interested in selling or buying various products and services. Some examples are drugs, firearms, malware, leaked databases, and hacked accounts (e.g. social media, streaming platforms). Marketplaces are comprised of a specific set of characteristics that regulate their operation, ranging from the initial access and registration, to the trust mechanisms applied, or the cryptocurrencies and payment methods preferred [3]. All of these elements result in a trading environment ideal for anonymous transactions, attracting many sellers and buyers that trade in an assortment of illegal products and services.

As one would expect, botmasters have jumped at the chance of incorporating these platforms into their frameworks. They utilize these selling points to provide their products and services (e.g. Distributed Denial of Service (DDoS) and spam attacks), but marketplaces can also be used from the potential botmaster's perspective. Users eager to join the cybercrime world in relation to botnets, can acquire the components needed to build a botnet infrastructure from the ground up.

Over time, researchers have approached botnets from more of a business-oriented point of view. They have focused on specific botnet types and their respective business side, e.g.

botnets that trade in spam attack services [4], while some have targeted specific economic elements of botnets such as payment [5]. There are also approaches that focus on the business model of botnets as a whole, such as the work of *Georgoulias et al.* [6], who attempt to map out all of the components associated with building and running a botnet business in a darkweb context, using their own adaptions of two popular business models.

In this paper, we crawl all of the 26 darkweb marketplaces that were available during the time period of October to December 2022, resulting in a dataset of $248,216$ total listings, along with the corresponding vendor profiles, which lead to $7,187$ unique vendor entries. After parsing and classifying the data through Natural Language Processing (NLP) methods, we then conduct our analysis on $36,314$ botnet-related listings, and the $1,163$ profiles of the vendors providing them. We correlate these listings, with segments of the botnet *Value Chain Model* adapted by *Georgoulias et al.* [6] (see Appendix A, Figure 5), with the goal of uncovering how each component of a botnet infrastructure can be mapped to darkweb marketplace listings in a practical manner. This translates into gaining insight on the availability of products and services that could be utilized by potential botmasters to build up and maintain a botnet infrastructure, but also on listings that describe services/products provided by botmasters, after their business has been established. We analyze the specifics that surround these listings, with pricing and payment as two examples, aiming to document how accessible creating a business of this type actually is. Lastly, with sellers naturally playing a key part in every trading environment, we study the role of vendors, with a focus on elements such as cross-platform availability and reputation, through their usernames and Pretty Good Privacy (PGP) keys.

We summarize the contribution of this work in the following points. In this paper we:

- fully crawl 26 darkweb marketplaces and present our architecture in combination with the methodology applied, to encourage and facilitate future research (the dataset will also be made available to researchers after publication),
- focus on the available botnet-related services and products, along with the corresponding vendors, and present their aggregated details (e.g. listing type, amount, pricing, vendor reputation),
- document significant properties of these platforms (e.g payment methods and reputation systems)
- correlate these listings with segments of the botnet *Value Chain Model*, illustrating how the business model is reflected in the real world. This is interpreted as acquiring the necessary components required to profitably set up and run a botnet business, as well as providing botnet services,
- attempt to track vendor activity throughout the 26 darkweb platforms.

The rest of the paper is structured as follows: In Section II we offer the methods applied in the context of this work. Section III is dedicated to our system's architecture and technical aspect of the project, while in Section IV we present our results and their interpretation. Lastly, Section V describes notable previous research efforts that can be related to our own, with Section VI concluding this paper.

II. Methodology

A. Defining Botnet Listings

The first step before deploying our crawlers, was to make sure we have established which listings we would be targeting. The basic idea was to focus on services and products that can be associated with *acquiring, establishing, maintaining, and weaponizing a botnet infrastructure for malicious purposes, in order to generate profit*. This can be viewed from the side of a botmaster that is providing these products and services, but also from the potential botmaster/client point of view. This approach led to the following listing types (for more details on each type see Section IV-B):

- Banking/Carding (e.g. bank-drops, cash-outs, stolen credit cards, stolen *PayPal* and cryptocurrency wallet accounts, gift cards). These listings can be utilized in the laundering of the earnings made by the botnet [7], [8], [9].
- Malware/Malicious tools, as well as guides on how to develop and use them (e.g. banking trojans, Remote Access Trojans (RATs), loggers, cryptojackers, botnet applications, access to established botnets)
- Hacking (e.g. guides, courses, and services)
- Databases (e.g. mailing lists and logs)
- Phishing-related listings
- VPN services, which can be used for obfuscation purposes
- Hosting and proxy servers (e.g. Command and Control (C&C) server hosting services)
- Attacks (e.g. DDoS and spamming)
- Exploits
- Personal information listings, also known as "Fullz" (e.g. name, address, email credentials, social security numbers)
- Account login credentials, which mainly refer to streaming and social media platforms
- Bot and carding shop invites
- Combo listings, which can include a wide variety of products (e.g. VPN, hosting, proxies etc.)

B. Technical Setup Overview

In regard to the technical aspect of the project, there are three distinct phases: **crawling**, **parsing**, and lastly the **filtering** of the acquired dataset.

For the crawling and parsing phases, we use the *Selenium* web driver in combination with a *Firefox Geckodriver* and the *Tor* application. The profile and binary used along with the Geckodriver are adopted from the Tor browser distribution. The crawled listings are stored locally in HTML form, and backed up after the completion of the crawl. The HTML files are then parsed and the data stored in CSV file form, one

for each of the marketplaces, both for listings and vendors, amounting to two CSV files per platform. The parsers we use were developed specifically for this project.

For the filtering step, we utilize *Deep Learning*, and specifically three *NLP* models based on the pre-trained model *DistilBERT*, which we further train using the harvested data on a remote server provided by our university research group. The *Keras* API and *TensorFlow* platform are also used in this phase. Lastly, after discarding the data irrelevant to the project through these models, and normalizing certain values from both the vendor and listing files (see III-C6), we insert both locally in a *MySQL* database. This allows for the execution of SQL queries, making the analysis of the data much more intuitive.

In the development of all three stages, we use the Python 3 programming language. Our entire setup is elaborated upon in detail in Section III and presented on Figure 1.

C. Ethical Issues

This section is dedicated to the measures we took to make sure our approach is ethically well-founded. First and foremost, we would like to establish that our focus is solely the botnet service and product trading ecosystem, and we are not in any way trying to negatively impact the operation, or contribute to the shutdown of these platforms. Our reasoning, is that as it has been argued by researches in the past [10], [11], [12], [13], [14], [15], the operation of these marketplaces can be viewed as a means to avoid the dangers that surround the physical illegal drug trade. Hence, we apply the approach presented in this section, to make sure that our research does not cause any harm whatsoever. The data that we harvested was public and free to access, available to all users visiting the sites. We also decided against making our presence on the sites known, since by doing so we could unwillingly affect the outcome of our measurements (*Heisenberg* principle) [10], [16], [17]. Additionally, we do not interact with any sensitive user data which could potentially jeopardize the anonymity of any individual.

Carrying out too many requests to these services, would certainly have a negative impact on their operation, the experience of the users, as well as, to some extent, to the operation and performance of the entire Tor network. For that reason we apply rate-limiting to our crawlers, using a random delay of seconds in the [4,10] range (after trial and error, the specific range seemed to result in the fewer session losses), which also assisted in our crawler remaining undetected (see Section III-A1). For the same purpose, we also try to use all of the mirror links provided by each marketplace, whenever they were available, in an effort to evenly divide our request traffic throughout as many servers as possible. This, combined with a delay time on the lower side of the range mentioned above, resulted in speeding up the crawling process, while also further lightening the traffic load handled by each server. Moreover, as also conducted by other researchers in the past [17], we have been providing a relay node to the Tor network, still running in University premises to this day (September 2023), to make up for the resource consumption by our crawlers.

Lastly, we want to address the reasons behind not disclosing the list of the 26 marketplaces chosen for this project. We feel that explicitly mentioning the names of each platform could drive traffic to the sites, which is something we would not like to have contributed towards. However, the marketplace list along with the onion addresses of the sites will be made available for the reviewers during the submission process, and can be found in Appendix A.

III. The Architecture & Data

As argued by *Cuevas et al.* [18], researchers in the past have often omitted the technical details of their system, which can present challenges in accurately evaluating the contribution of their work. Additionally, this approach fails in assisting future researchers to carry out this type of research. With this in mind, in this section we go over the four parts of our system, namely the **crawler**, the **parser**, the **NLP models** used to filter the data, and finally the **database** designed to store the final dataset and help carry out our analysis. An overview of the system architecture is illustrated on Figure 1.

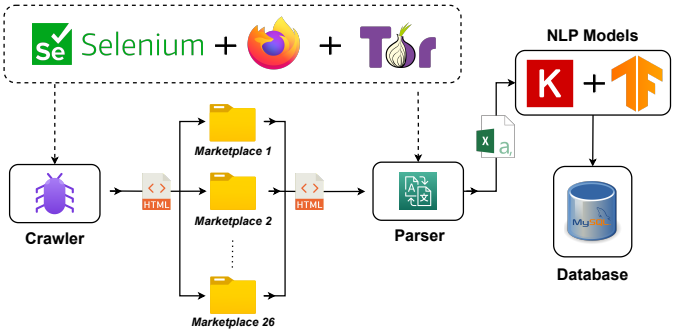

Figure 1: The architecture of our system

A. The Crawler

Designing our crawler was the foundation for this work, and was carried out with several principles in mind. In this part of the paper, we describe these principles, how they were applied, and how they affected the crawling process. As mentioned in Section II, the setup we used is a combination of the *Selenium* web driver, the *Firefox Geckodriver*, and the *Tor* application, with a Tor browser Firefox binary and profile. All of the web elements needed were located using the *XPath* values.

1) Crawling strategy: All of the 26 marketplaces were fully crawled for all of the categories, listings, and vendors, and the data stored in raw HTML form. The reasoning behind crawling all of the categories, and not targeting specific ones more relative to the types described in Section II-A, was the fact that after manually browsing through some of the marketplaces, we identified some cases of listings that were miscategorized. Hence, for measurement accuracy reasons, we decided upon

crawling all of the listing categories and then filtering the results.

For the purposes of this paper, we decided to go with a single snapshot of each of the marketplaces. The reasoning behind this decision, is the fact that we were only interested in the availability of products at that point in time, not its fluctuation over a period. Additionally, a single snapshot is sufficient to provide a good overview of the site properties, such as payment type and cryptocurrency usage.

As mentioned in Section II-C, our crawler was implemented with a rate-limiting function between 4 and 10 seconds. Apart from the ethics aspect, this function of the system also allowed for us to remain undetected and complete our crawls in a discrete manner. It ensured that our crawler would not raise any suspicion, lowering the chance of triggering any platform defensive mechanisms, which could result in our access getting blocked, and in some cases our account getting suspended (wherever one was needed to reach the listing section of the marketplace). This latter scenario was a rare occurrence, but interestingly enough, at one point we did run into a platform that had such an aggressive defensive mechanism setup, that even normal user browsing behavior would get our accounts blocked, making the site unusable. In general, we faced several instances of time-out connections, but we cannot be certain whether it was a premeditated defensive mechanism response, or a Tor connection issue. However, a more aggressive crawling profile without rate limiting would have resulted in many more timeouts on most platforms.

With the purpose of achieving as much simplicity and effectiveness as possible for our system, we decided to split up the tasks each component would have to carry out. In the case of the crawler, instead of fully crawling each category along with its listings and vendors in one run, we divided the process into two separate sub-tasks: *harvesting the links* of the listings and then *crawling* their content along with the vendor profiles.

a) Harvesting the links: In all of the platforms apart from one, after deploying the crawler we were met with CAPTCHA mechanisms, and in some cases with more than one, e.g. both in the landing page of the site and then the login page as well, which we would solve manually. After using our account credentials to log in, we would initially acquire the links of the featured listings hosted on the homepage, and then catalogue the product categories available on the site. The next step was to visit all of the product category pages, acquire the page number, and then visit every page harvesting the links of the listings. On some of the sites, all of the available products of all categories would be presented on the homepage of the site, beneath the featured listings, spread over a number of pages. On these platforms we would directly store the links of the listings by visiting each of these pages, instead of working on each category individually. Additionally, in some rare cases, manually tweaking the homepage URL to show an irregularly large amount of listings per page, allowed for the process to become even more effective by reducing the number of pages our crawler had to navigate through. After every page crawled, the links were stored in a CSV file, in a folder named after each marketplace. Finally, the crawler would update a text progress file which included the category and page number that were crawled last, making it possible to resume the crawling process in case any kind of disruption occurred (e.g. connection error, scheduled crawler halt).

b) Crawling the links: In this phase, the initial process in regard to the CAPTCHAs and site login remained identical, since our system had to gain access to the platform once again. After gaining access, the crawler would go through the entries in the listing link CSV file, visit each listing page, download its raw HTML content, and repeat the procedure for the vendor profile (sometimes for the PGP key of the vendor as well, in the cases there was a separate page). The HTML code would then be stored in the marketplace corresponding folder, using the same ID assigned to the listing by the platform, along with the crawl date. Similarly to the previous step, the progress of the crawler would be documented in a text file, which would be updated after both the listing and vendor profile crawls would be successfully completed. The file would keep track of the listing link index based on its place in the CSV file. In addition to the progress file, we also designed the crawler to keep track of the failed attempts in a CSV file, since in some cases some of the links provided for the listings, would be invalid or broken.

B. The Parsers

The component of our system sitting in the middle of our architecture is the parsing application. In this phase we yet again used the *Selenium* web driver alongside the *Firefox Geckodriver*, but this time in offline mode since we did not need a connection due to the nature of the task. The *XPaths* of the web elements were once again used to harvest the needed values from the HTML files.

1) Parsing strategy: Since the data was stored locally as HTML files, during phase two the parsing was carried out offline. The reasons for not parsing *"on the fly"* were simplicity, ease of use, and to also avoid any issues from the first process spilling over to the second one (e.g. Tor connections errors affecting the parsing of the crawled listings), hence eliminating potential points of failure for our system. Additionally, this course of action allowed for the HTML files to be available for re-parsing, if the need arose in the future. Considering the highly dynamic nature of the darkweb market in terms of availability and uptime, storing the raw HTML files can prove particularly beneficial.

In regard to using already available solutions, or developing our own parsers, we decided to opt for the latter option. This decision, from early on, seemed to offer more diversity and flexibility to the operation of our system, by allowing for a more nuanced parsing approach. Since the vendor profiles and the listings were stored in different HTML files, the parsing was carried out in two cycles, one for each type, resulting in a total of 52 different parsers. After going through the parsing of several files from a variety of marketplaces, we started forming

a basic template for both HTML file types, which sped up the process of developing the applications quite noticeably.

2) Data fields of interest: The parsing application was designed to extract a large variety of field values from the HTML files, with fluctuating in availability throughout the various listings and marketplaces (e.g. digital versus physical products, in terms of shipping methods). The final number for the listing HTML files amounted to 17 fields, while for the vendor files we parsed 19 value types. For more details regarding the value types, see Appendix A.

C. NLP, Normalization & Database

The crawling and parsing phases of the project resulted in a total of $248,216$ listings and $7,187$ unique vendors. Based on the definition of botnet listings provided in Section II-A, the third phase was dedicated to filtering the listings, tailoring the dataset to fit our goals. This was achieved through the training of three *Deep Learning NLP* models (M1, M2, M3), based on the pre-trained *DistilBERT* model. The technical setup consisted on the *Keras API* and *TensorFlow* platform. In this section we go over the three models, and how each contributed towards transforming the initial dataset to its final version we carried our analysis on. Details on the training parameters and F1 scores can be seen on Table I.

1) BERT vs DistilBERT: Before diving into the details of each of the models, we need to address the reasoning behind choosing the *DistilBERT* model. In our previous work [19] we found that the BERT and DistilBERT models had the highest performance when working with similar data. We tested the two models to evaluate which would handle our dataset better. We found that transitioning from *BERT* to *DistilBERT* improved the F1 score of all three models by approximately 3-5% across the board, regardless of which specific values (e.g. titles or descriptions of products) we trained the models on. After selecting DistilBERT, we started fine-tuning and finalizing our models.

2) Model 1 - Digital products: After the dataset had been formed, the first priority was to filter out the more distinguishable of the listing categories that we deemed unrelated to the project. These categories were all physical products, namely drugs, counterfeit products (e.g. fake money bills, clothes), forged documents, and firearms. We manually labeled approximately 2.25% of our entire dataset of $248,216$ listings into two categories (0 or 1), since the problem was binary in nature. The final trained model achieved an F1 score of 94.8% and after applying it to all of the data, the end result was $55,699$ listings for digital products.

3) Model 2 - Botnet-related products: In the second part of filtering, the goal was to separate the digital listings that could not in any way be associated with the botnet market. This included numerous different product types, with some of the main ones being cracked software and listings related to pornographic content. Since we were once again faced with a binary classification problem, we manually labeled over 10.4% of the listings, dividing them into the 0 and 1 categories. For M2 we managed to reach an F1 score of 91.1%, and running the $55,699$ listings that were the output of M1, through the model, reduced the size of the dataset to $36,314$ botnet-related listings. At this stage we also filtered the vendor profile entries, which dropped from $7,187$, to a total of $1,163$.

4) Model 3 - Type classifier: The last of the three models, M3, was tasked with the multi-class classification of the $36,314$ listings. When going through the labeling process of the M2 training dataset, we decided that we would develop a dataset that could be also used in the training of M3, for the provided ease of use and effectiveness of our system. This was achieved by deciding on the labels that would be used in the training of M3, and populating the dataset with the appropriate listings, as evenly as possible. Hence, at this stage we used the positive listings from the training dataset of M2 and further labeled the entries using 13 new tags. The model achieved an F1 score of 91.2%.

Based on the definition of what we consider botnet-related listings, given in Section II-A, we grouped our training data for this model using the labels presented on Figure III.

5) Training the models: Regarding the data used in the training process, all of the entries were labeled manually. With M1 and M2, since the classification was binary, we aimed to approximate a 50-50 data split. The same rationale was followed when training the third model, in which we opted for an even split between the 13 classes. Aiming to increase the accuracy of the models, we also removed the special characters from the entire dataset. After training all of the models with and without including numeric characters in the data, we noticed a bump in accuracy in the range of 0.3-0.5% in the latter case, hence we decided to remove all numbers during the training phase. While M2 and M3 seemed to achieve the best performance when trained solely on the *listing titles* of the products, M1 proved more accurate when trained on both the *listing title* and *description* of the products/services. We believe this is due to the fact that the listing descriptions were distinctively different between widely different listing types. One example is drug listings when compared to malware listings, in which case adding the description contributed towards M1 identifying the listing type more easily. On the other hand, if the listing types were more similar, e.g. malware and cracked anti-virus software listings, the descriptions did not differ as vividly, which seemed to in some cases confuse the model when predicting the classes.

Throughout the entire training process, we followed the same procedure for all three models in order to reach the highest F1 score without over-fitting them. The data split percentage that was applied was 80%/10%/10%, 80% for training, 10% for validation, and finally 10% for testing. All of the models were then trained on 100% of the each respective dataset. We tested a wide variety of learning rates, but in the end a learning rate of *1e-2* proved to be the most efficient for all three models, providing the highest F1 scores across the board. Lowering the learning showed to slightly decrease the final performance of the model in most cases, while at the same time increasing the number of the epochs needed to reach similar F1 scores. Epochs on the other hand, seemed to differ

DistilBERT Model	Learning Rate	Epochs	Training Data	Mean F1 Score	Task
M1	1e-2	3	Titles & Descriptions	94.8%	Digital listing filtering
M2	1e-2	5	Titles	91.1%	Botnet-related listing filtering
M3	1e-2	6	Titles	91.2%	Type classification

Table I: Purpose and training hyper-parameters of the three NLP models.

between each model, with M1, M2, and M3, being trained for 3, 5, and 6 epochs respectively. Lastly, after preparing our three training datasets, and finalizing the training parameters for each of the models, the final step was carrying out the actual training process. We used 10 random numbers as seeds for the data split, resulting in 10 different combinations of training, validation, and testing sets per model, which in turn provided 10 different F1 scores, from 10 different training runs. In order to best estimate the performance of each of the models, we chose the mean F1 score value from these runs as the best evaluator, which we present on Table I as the final F1 score for M1, M2, and M3.

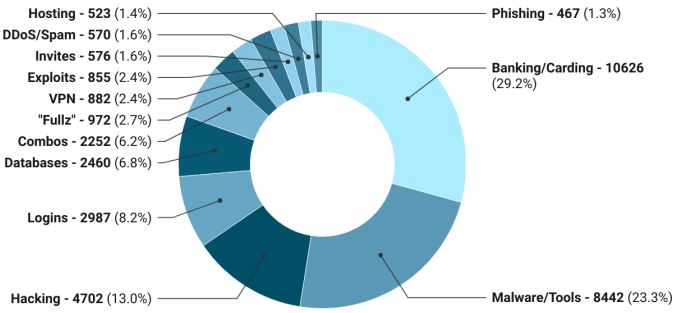

Figure 2: Distribution of listing types in the dataset.

6) Normalization & Database: Due to the fact that darkweb marketplaces apply a large variety of different reputation systems and metrics for the vendors [3], in order to carry out our analysis on the data we had to normalize these values. For the reputation gained by the vendors based on the number of sales carried out (where it was available), the scale chosen was [1, 10]. Similarly, for the rating achieved by the vendors based on the grading provided by buyers, we went for a scale of [0, 5], to better simulate the star reward system, while positive feedback scores were in the form of percentages. At this point we want to mention that we also run into cases that in either of the reputation fields mentioned above, would have negative values, or would mention the fact that a vendor was banned or had negative reputation. For these cases we used -1 as the reputation indicator (for more details on the reputation systems refer to Section IV-A3).

Regarding the pricing provided for the listings on each of the marketplaces, we found that there were only four currencies used across the platforms: United States dollar (USD), Euro (EUR), British pound sterling (GBP), and Canadian dollar (CAD). For the purposes of the project, all of the entries were converted to USD.

Lastly, after normalizing the vendor reputation systems and the listing prices, we inserted both the listing and the vendor CSV files in a local *MySQL* database, assigning a dedicated table to each of the files. In the specific case of vendors, we de-duplicated the entries from each individual vendor CSV file, per marketplace, using the username value, allowing for vendors using the same username across different marketplace to maintain more than one entries in the database, one per marketplace they were found on. This approach enabled tracking the vendors throughout the different platforms (see Section IV-D3).

IV. Data Analysis & The Botnet Business Model

A. Currency & Payment Methods

In this section, we dive into the use of cryptocurrencies and various payment methods.

1) Payment methods: In all of the 26 marketplaces, we found use of the *escrow* payment method. Escrow allows for the marketplace to act as a middle-man, holding onto the funds paid by the client, until the delivery of the product/service has been verified and the order has been *"finalized"*. When that occurs, the funds are released to the vendor. This mechanism, although safer than direct payments, is still susceptible to *exit scams*, where the owners shut down their marketplace without notice, and keep all of the funds that were being held in escrow.

To reassure clients that this will not happen on their platforms, some marketplaces implement *multi-signature escrow*, or *"multisig"* (exclusive to Bitcoin (BTC)). According to this mechanism, out of the three parties involved in a transaction, namely the buyer, seller, and marketplace, there needs to be authorization from at least two, in order from the funds to be released from the escrow. In the case of exit scam attempts, this translates into the client and vendor both signing off on the release of the funds. Out of the 26 platforms, we found only 3 were implementing multisig.

Lastly, the last payment method used on the marketplaces was *Finalize Early (FE)*. This mechanism allows for the funds to be immediately released from escrow and reach the vendor right after the client payment, before the delivery of the product/service. This method is also used as an indicator of particularly good reputation and high trust status of the vendor, since a dishonest vendor could walk away with the funds without providing the service/product they were paid for. Hence, this status is only provided to vendors that have proven to be exceptionally trustworthy through such as sale numbers, and client feedback (e.g. rating, reviews). We found FE vendors in 18 of the target marketplaces, with 348 (4.8%) out of the 7,187 vendors having the FE reputation badge,

while for the botnet-related listings this number shrunk down to only 19 out of 1,163 (1.6%) vendors.

2) Currency: While harvesting data from the marketplaces, we also turned our attention towards documenting which are the cryptocurrencies of preference throughout all of the platforms. According to our findings, the most widely used cryptocurrency is still BTC, which was found on 23 out of the 26 marketplaces (88%). At this point, it was interesting to see that BTC is still favored over Monero (XMR), which XMR followed in second place, with use in 15 (58%) platforms, even though it offers improved anonymity properties over BTC [20], [21]. Additionally, Litecoin (LTC) and Ethereum (ETH) were utilized in 5 (19%) and 2 (8%) marketplaces respectively, while we also run into single use instances of the Bifrost Coin (BNC), Dash (DASH), Zcash (ZEC), Bitcoin Cash (BCH), and Binance Coin (BNB) cryptocurrencies. We summarize all of our findings on Figure 3.

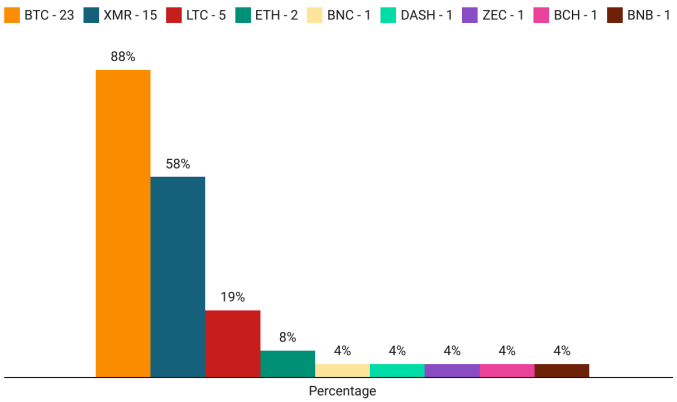

Figure 3: Cryptocurrency usage in the 26 marketplaces.

3) Vendor reputation systems: Regarding vendor reputation, we run into different implementations of three basic systems: *positive feedback scores*, *trust rating*, and *sale levels*. Positive feedback score was the percentage of the $positive/total$ feedback ratio that resulted from the assessment clients provided for the vendors, after completing a transaction with them. In some of the platforms that the system was applied, the final percentage would either be provided, or it had to be calculated during the parsing process using the aforementioned ratio. In these instances the vendor profiles would include the amount of positive/negative/neutral client assessments. We run into this mechanism in 22 out of the 26 marketplaces, amounting to a 84.6% application.

Trust rating also refers to client feedback, but this time it would usually be provided through a grading scale usually from 0 to 5, or 0 to 10, and in many cases came in the form of star rating. It was met by our crawlers on 17 (65%) of the marketplaces.

Another popular metric used across the marketplaces, was *sale levels*. As the name indicates, the vendor would be assigned a level based the amount of sales carried out. Each marketplaces had its own scale of calculating the level, and it would come in the form of a number in the range of [0, 5], or [0, 10]. Sales were part of the reputation system in 69.2% of the marketplaces, which translates into a total of 18 platforms.

Finally, for the two cases of negative reputation, as mentioned in Section III-C6 where we discuss the normalization for the reputation systems, we applied a -1 value score.

B. Business Model Segment Correlation

In this section, we focus on creating a correlation between the segments of the Botnet Value Chain Model [6] (see Appendix A, Figure 5), and the listing types available on the 26 marketplaces we crawled. We target 4 specific segments of the model, *Assimilation*, *Monetization*, *Technology*, and *Firm Infrastructure*, since they compose the part of the model that can, in various manners, be associated with products and services available on the darkweb, with some of the listings categories falling under multiple blocks of the model.

1) Assimilation: The *Assimilation* model block is associated with acquiring a healthy bot supply for the botnet, but also the ability to maintain it. This translates into activities linked to acquiring the bots, coordinating their behavior (e.g. issuing DDoS attack orders), as well as the evasion/recovery mechanism, as a fallback in case a disruption occurs and the bots need to rejoin the network anew [6].

From our dataset, this block can be associated with **Malware/Tools** listings. The reasoning is, with RATs as an example, that a malicious actor could gain remote access to a device, and recruit it as a bot for their army, without the user's knowledge. **Phishing** listings are also very relevant, since an unsuspected user visiting these sites would be at risk of compromising their device, and falling under a botmasters control. Assimilation also relates to **Hosting/Proxy** services, since acquiring Bulletproof Hosting Services (BPHS) is a vital part of a botnet infrastructure. This applies to both the coordination and recovery mechanisms. For the same reason, **Combo** listings fall under this block as well, since many of them also include hosting services. Adding new bots to the ranks can also be achieved through directly bypassing the target devices' security, hence **Hacking** listings are also linked with this model segment. This can be achieved by acquiring hacking services, but also from the side of the botmaster's botnet infrastructure in place (e.g. attempting hacks independently, utilizing hacking guides). **Database** and **"Fullz"** listings can be a part of the target selection process by botmasters, in the sense that the information gained (e.g. private information, mail lists) can be used in combination with methods such as social engineering, spamming, and phishing, to lure in victims and finally recruit new devices for the bot army. Similar logic applies to the *Invite* listings, since the information bought from bot shops (e.g. mail account access credentials) can be utilized to spread the bot malware to more devices. Lastly, **Exploits** can be utilized to take advantage of vulnerable systems, compromise them, and add them to the botnet ranks.

2) Monetization: Monetization can be summarized as the segment that describes the methods used by botmasters to generate profit. This can include a variety of approaches, such

Segment	Assimilation	Monetization	Technology	Firm Infrastructure
Banking/Carding	✗	✓	✓	✓
Malware/Tools	✓	✓	✓	✓
Databases	✓	✓	✗	✗
Hosting/Proxies	✓	✗	✓	✗
Hacking	✓	✓	✓	✓
Combos	✓	✗	✓	✗
Phishing	✓	✓	✗	✗
VPN	✗	✗	✓	✗
DDoS/Spam	✗	✓	✗	✗
Exploit	✓	✗	✓	✓
"Fullz"	✓	✓	✗	✗
Account Logins	✗	✓	✗	✗
Invites	✓	✓	✗	✓
Listings	21,249 (58.5%)	31,446 (86.6%)	27,926 (76.9%)	24,845 (68.4%)
Price Median	5$	7.9$	5.1$	7$

Table II: segment/listing type/vendor relation table, along with the median price values for each segment.

as extortion, banking fraud, DDoS attack services, bot sales etc. **Malware/Tools** are one of the main types of listings of the block, since they can be weaponized by botmasters for revenue purposes (e.g. ransomware and extortion of the victim user). **Database** listings are also included in this segment, both in the context of sales from the botmasters, but also in the case that the botmasters acquire these products as clients, and use the data for their own malicious purposes. Two respective examples are sales of leaked/hacked databases, and the purchase of mail lists, which can be used to create **spamming** and **phishing** campaigns, and carry out DDoS attacks. These activities can ultimately lead to profit, hence they are also linked with the Monetization segment. As mentioned above, **Hacking** activities can lead to the recruitment of new bots, which translates into long-term profit for a botnet business. Trading in **"Fullz"**, **Account Logins**, as well as **Banking/Carding** information harvested by the botnet can be a profitable venture for botmasters, hence all of these categories have a place in the segment. Last but not least, botmasters can sell stolen credentials and other harvested information on bot shops, and for that reason listings of **Invites** to such platforms also lie within this category.

3) Technology: Here, we link listings that relate to the software and hardware used in the botnet infrastructure. The **Malware/Tools** type includes the botnet applications (botmaster, bot, coordination and recovery mechanisms), which are fundamental components of a bot network. This segment also includes cryptocurrency wallets, which is a subcategory in the **Banking/Carding** category, as well as **VPNs**, **Hosting/Proxies**, and **Combos** (since they very often include VPN services), due to their utilization for obfuscation purposes. Hosting specifically, refers to the C&C server of the botnet. Additionally, we relate Technology to **Exploit** listings, since they can be utilized to update and strengthen the botnet applications, and specifically bot binary that infects and runs on the victim host. **Hacking** related listings can also serve as a potential stepping stone to acquire the necessary technical savvy that can then be utilized to enhance the current implementation of the various botnet application components. Some examples are the propagation, coordination, and recovery mechanisms, as well as obfuscation techniques.

4) Firm Infrastructure: The last segment of the botnet value chain model that we believe can be correlated with our listing dataset, is *Firm Infrastructure*, which mostly refers to the maintenance of the infrastructure. This ranges from the technical aspect to the financial, with money laundering as an example of the latter. For this reason, listings in the *Banking/Carding* category, since they include bank-drop and cash-out listings, as well as *Invites* to carding shops, also have a place in the segment. Lastly, **Malware/Tools**, **Exploit**, and **Hacking** listings can be utilized to further improve on the botnet applications, as mentioned in the previous paragraph.

C. Botnet-related listings

In this section, we go over the details of the $36,314$ listings that we found to be relevant to the darkweb botnet trade.

1) Listing concentration: Before going into the different categories of the listings, we focused on the presence of all products and services on the platforms. We noticed that 28.6% of the entire dataset originated from a single marketplace, known to be the largest at the time we carried out our experiments. Additionally, our analysis indicates that 5 out the 26 marketplaces accounted for the bulk of the listings, at around 76.2%, while 94.3% of the listings were found on the top 10 platforms (for more details see Table III).

As shown by previous work [19], listings related to carding take up a particularly large part of the darkweb trade. Due to that fact, we were not surprised to find that the *Banking/Carding* category came in first with $10,626$ (29.3%) related listings. The *Malware/Tools* was the second category with with a total of $8,442$ (23.3%) listings, while the third place belonged to listings associated with *Hacking* amounting to $4,702$ (13%). Figure 2 showcases how all of the listings are distributed over the 13 categories.

Lastly, after we established links between the segments of the botnet *Value Chain Model* (see Section IV-B), we took an interest in uncovering how our dataset of $36,314$ listings can

be mapped on the model. We correlated *Monetization* with the biggest part of the dataset (86.6%) at 31,446 listings , and *Technology* with a total of 27,926 listings, which refers to 76.9% of the entries. *Firm Infrastructure* could be associated with 68.4% of the listings, while *Assimilation* came in last with 58.5%. We present an overview of the results on Table II.

Marketplaces	Listing count	Percentage
Market 1	10390	28.61 %
Market 2	5799	15.97%
Market 3	5132	14.13%
Market 4	4295	11.83%
Market 5	2060	5.67%
Market 6	1913	5.27%
Market 7	1753	4.83%
Market 8	1311	3.61%
Market 9	911	2.51%
Market 10	695	1.91%
Market 11	440	1.21%
Market 12	239	0.66%
Market 13	191	0.53%
Market 14	188	0.52%
Market 15	173	0.48%
Market 16	167	0.46%
Market 17	158	0.44%
Market 18	123	0.34%
Market 19	121	0.33%
Market 20	78	0.21%
Market 21	65	0.18%
Market 22	38	0.10%
Market 23	26	0.07%
Market 24	22	0.06%
Market 25	19	0.05%
Market 26	7	0.02%

Table III: Listing concentration on the 26 marketplaces

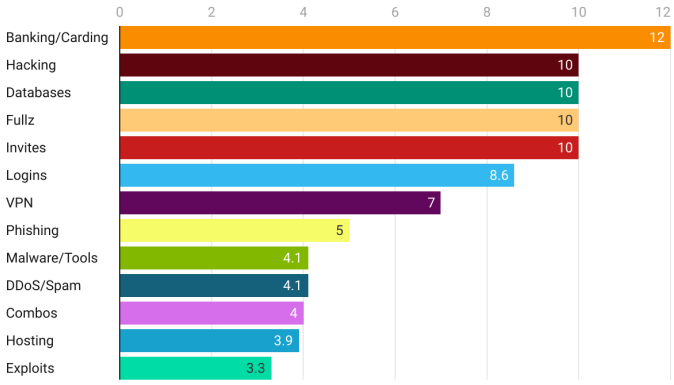

Figure 4: Median price values for all listing categories in USD.

2) Pricing: In order to get a good estimation of how expensive botnet-related products and services are, we calculated the median value for the listings of each category. The most expensive category overall, was the *Banking/Carding* category, with a median of 12 USD. The category following was not a single one, but rather a tie between 4 separate categories, namely *Hacking, Databases, Fullz*, and *Invites* all at a median of 10 USD. *Account Logins* listings came was the third most expensive, presenting a median of 8.6 USD. Interestingly, *Exploits* were the cheapest and most accessible products, available at a median of just 3.3 USD. The median price values for all categories are illustrated on Figure 4.

Getting an overview of how the pricing of the listings fluctuates between the different segments provides insight on both the cost of setting up a botnet, as well as the potential revenue that can be achieved by a botmaster. The products and services in the *Monetization* segment presented the highest price median, at 7.9$, with *Firm Infrastructure* following close behind at 7$. *Technology* came in third with a 5.1$ median , almost tying with *Assimilation* at 5$.

D. Vendors

This section is dedicated to the analysis performed on the vendors of the botnet-related listings.

1) Vendor concentration: As discussed in Section III-C3, out of the initial unique 7,178 vendor entries, we found that 1,163 were providing services or products that could be utilized by an already established or potential botmaster. In regard to vendor concentration, we found that 5 of the marketplaces accounted for 58.4% (679) of the vendors, while 79.8% (929) were spread among the top 10 platforms. Lastly, the largest marketplace at the time we conducted our crawls, was hosting 21.6% of the vendors. For a more detailed overview, see Appendix A.

In regard to the listing categories, *Banking/Carding* was yet again found to be the most populated, with 63.3% (736) of the vendors providing related listings (see Section II). *Malware/Tools* was found to be the second richest in terms of vendor availability, coming at 49.8% (579), while *Account Logins* came in third with 376 (32.3%) vendors (see Table IV).

2) Reputation & sales: Out of the 1,163 vendors, 559 (48.1%) had positive feedback scores on their profiles, 469 (40.3%) had trust ratings, and 797 (68.5%) had been assigned a level based on sales. This indicates that these vendors are indeed active, with listings that have resonated with clients enough to purchase and evaluate the vendors' services.

In terms of the actual reputation status of the vendors, after normalizing the reputation values (see Section III-C6), we calculated the positive feedback scores at an average of 61.5%, while the average trust rating and sale level came in at 4.3/5 and 1.9/10 respectively. The numbers suggest that although the vendors are trusted and evaluated as quality sellers, it appears that the number of sales carried out is quite low on average.

To verify this, we decided to also calculate how many vendors had sales histories, as well as the median value of the transactions these vendors had completed. We found that 674 (58%) of the vendors had already carried out sales by the time we deployed our crawlers, while the median value for all vendor sales was only 7. Additionally, 272 vendors (23.4%)

claimed to have carried out sales on multiple platforms, many of which had not been operational for years.

3) Cross-platform tracking: Good reputation, along with the resulting trust are vital for the success of a vendor in the darkweb. One factor to establishing trust in the darkweb trading ecosystem is maintaining a respectable status across multiple marketplaces [3]. For that reason, we decided to track vendor activity throughout the 26 marketplaces, using their usernames and PGP keys, to investigate how many of the vendors utilize more than one platforms to carry out their business transactions.

By initially using the vendor usernames, we came across 145 instances of cross-platform use, which is equal to 12.5% of the entire vendor pool. Approximately half of these instances (51%) referred to use on two platforms, while there were two extreme cases of vendors seemingly operating on 13 marketplaces.

In the case of PGP keys, we found that 1064 out of the 1,163 opted for the use of the protocol, and included the keys on their profiles, which translates into 91.5% of the total. However, our results indicate that out of these vendors only 151, meaning 14.2% (or 13% of the grand total), could be potentially linked to activity on more than one platforms. Additionally, we found that there were also two cases of PGP keys located on 9 marketplaces. What we can notice in these

Listing Type	Vendor count	Percentage
Banking/Carding	736	63.3%
Malware/Tools	579	49.8%
Logins	376	32.3%
Hacking	334	28.7%
Databases	268	23.0%
VPN	253	21.8%
Invites	243	20.9%
"Fullz"	222	19.1%
Exploits	202	17.4%
DDoS/Spam	194	16.7%
Hosting	157	13.5%
Combos	116	10.0%
Phishing	93	8.0%
Total	**1,163**	**100%**

Table IV: Vendor distribution over the 13 categories.

results is a disparity between the percentages of usernames and PGP keys located on more than one platforms. Since cross-platform PGP key use is higher that username use, our understanding of this number disparity is that there are vendors who use the same PGP keys across platforms, but decide on using a different alias. However, we also observe a gap between the maximum platforms that vendors seemed to be operating on at the same time, with the PGP key maximum at 9 platforms, and the username maximum at 13. This suggests that there are also vendors that follow the reverse approach, meaning that they will use the same username, but a different PGP key, which could also indicate impersonation attempts by users other that the original vendors. (for more details see Table V).

Platform count	By username	By PGP
2	74 (51.0%)	88 (58.3%)
3	22 (15.2%)	22 (14.6%)
4	19 (13.1%)	23 (15.2%)
5	17 (11.7%)	11 (7.3%)
6	13 (9.0%)	7 (4.6%)
Total	145 (100%)	151 (100%)

Table V: count of vendors tracked by their usernames and PGP keys on multiple marketplaces.

E. Discussion: Interpreting the results by segment

After carrying out our analysis of the dataset, a few things stand out. The fact that the *Firm Infrastructure* segment is associated with 68.4% of the listings can be translated into botmasters having a lot of options when it comes to money laundering services and associated products (e.g. bank-drops, cash-outs, stolen cryptocurrency wallet accounts). This holds great significance due to the risks associated with this specific part of this type of business, such as being tracked by law enforcement. Moreover, cost-wise, the listings in this segment seem quite accessible, since the price median was to 7$.

All of the model segments appear populated by listings to a degree that any potential botmaster would have adequate options for all of the stages associated with establishing their infrastructure. For example, in regards to the *Monetization* block, and in combination with the *Banking/Carding*, *Databases*, *"Fullz"*, and *Account Logins* categories amounting to 17,045 listings (46.9% of the total), there seems to be potential profit for established botmasters in the sale of harvested credentials (e.g. bank credentials, user logs, accounts, and private information). The same thinking applies to *Malware/Tools* and *Exploit* listings, since botmasters can utilize both to upgrade their infrastructure, boost their impact, and consequently achieve increased profit.

Lastly, with 76.9% of the dataset being related to the *Technology* segment, and *Assimilation* being associated with 21,249 listings, botmasters are offered a variety of methods they could deploy to start recruiting their first bots, as well as bolster the ranks of an existing network and maintain its effectiveness (e.g. phishing, spamming campaigns through mailing lists). The Technology block is also associated with obfuscation mechanisms (e.g. VPNs, hosting, and proxies), which can be utilized to augment the botnet operations with improved stealth. Additionally, both of these two segments present low median price values of approximately 5, which translates into low setup and maintenance costs for the botmasters.

V. Related Work

In section we go over previous research related to our work. Gathering intelligence from darkweb marketplaces has been attempted in many cases in the past, both through qualitative and quantitative methods, namely through the use of crawlers. One of the most notable works involving use of crawlers, is that of *Nicolas Christin* [16]. The target was the

Silk Road marketplace, the first[1] and most infamous darkweb marketplace. The study was carried out in 2011-2012, with crawlers being deployed on a daily basis. The outcome was an understanding of the platform's operation and insight on the associated components such as products, vendors, clients, payment, and currency.

Soska and *Christin* [17] investigate how the darkweb market shifted to a new status quo after *Silk Road*, the most dominant marketplace at the time, was taken down in 2013. They deployed crawlers on 16 marketplaces, in an effort to document the impact Silk Road's shutdown had to darkweb illegal trading up until the year 2015.

Nunes et al. [22] follow a similar approach to ours, by utilizing a crawler, parser, and classifier to harvest cyber threat intelligence from 17 marketplaces and 21 forums. In their analysis they zoom in on the sale of zero-day exploits, and investigate the vendors' interaction and availability in both types of platforms.

More recently, *Georgoulias et al.* [19] perform a quantitative analysis of cybercrime products by crawling 8 darkweb marketplaces. They find the particular category of products is quite inexpensive to acquire, and they also explore the presence of vendors throughout the different platforms. Additionally, they present preliminary findings by also using crawler to harvest data from the Invisible Internet Project (I2P) mirrors of the sites, which could be useful for future research efforts.

Although similar to the aforementioned works, in our effort we focus specifically in the botnet market, and how the components of the botnet business model can be correlated to the listings available on darkweb marketplaces. We gravitate much more towards the aspect of running a botnet as a business, composed of various elements, each contributing towards a successful and profitable organization.

Apart from quantitative research focusing on the darkweb market, there are also efforts that dive into the cybercrime taking place on clearweb sites, and particularly forums. *Pastrana et al.* [23] turn their attention towards 4 popular cybercrime forums, and manage to harvest a total of 48m posts created by 1m accounts, dated from 2005 to 2018. This was made possible through the use of *CrimeBot*, a crawler developed by the research team for the purposes of this work, which they utilized over the span of 9 months. The resulting dataset was the foundation for the *CrimeBB* database, the analysis of which offered insight on the properties and operation of these forums, such as currency and payment. Additionally, they investigate how new actors can potentially be lured into joining in cybercrime activities.

Qualitative approaches have also been employed over the years to study the darkweb market. *Georgoulias et al.* [3] document the elements and properties of 41 darkweb marketplaces and 35 vendor shops, along with 3 popular darkweb forums, in and effort to understand the components that contribute to the successful and profitable operation of these platforms.

Specific product categories have also drawn the interest of researchers in the past, both through qualitative and quantitative methods. These works aim to map the characteristics of various subcategories of cybercrime, with the goal of contributing towards gaining a better grasp on cybercrime as a whole. Drugs [24], firearms [25], and stolen data [26], are a few examples, with more recently, due to the COVID-19 pandemic, efforts on vaccines and vaccination certificates available on cybercrime platforms [27], [28].

Botnets have always been a research topic that allowed for approaches with different focal points, due to the variety they offer in terms of characteristics. Some examples are architectures, detection and defense [29], [30], [31], analysis on specific botnets [32], focus on botnet takedowns [33], as well as works that dive more into the business/economic aspect of running a botnet.

Bottazzi and Me [34] use their own model composed of 4 different blocks in order to illustrate how a botnet can generate profit for a botmaster. Each block represent a link in the supply chain of a botnet.

Levchenko et al. [4], through a more practical approach, investigate the specific market of botnet spam services. Through data harvested over the span of three months from a variety of sources (e.g. data from botnets that had been taken over in the past), in combination with purchases from sites offering such services, they attempt to understand the business aspect that lies behind spam attacks.

Karami et al. [5] employ a combination of approaches with the end goal of disrupting botnet operations, and specifically that of booters/DDoS service providers. Firstly, They utilized crawlers to gather account data from booters that relied on the *PayPal* platform to receive payment from their clients. Then, after establishing a collaboration with PayPal, they managed to take these accounts down, which put a serious dent in their services, effectively disrupting the operation of their business.

Putman et al. [35], use the *Business Model Canvas* to analyze the operation of a botnet, and using four case studies, they study the relation between the revenue and costs that are associated with running and maintaining a botnet.

Lastly, the work of *Georgoulias et al.* [6], which serves as the main inspiration for this paper, illustrates how the various components that when combined form the infrastructure of a botnet, can be mapped onto their adapted implementations of the *Business Model Canvas* and the *Value Chain Model*. Additionally, they document the details of notable takedown attempts against 28 botnets, from the year 2008 until 2021, and how the methods implemented by the takedown actors can be correlated to the adapted business models.

Taking into account all of the different approaches applied by researchers over the years and discussed above, in this work we decide to employ a combination of methods. While, we opt for the use of crawlers, parsers, and classification models, and hence a more technically oriented approach, the business

[1]Technically the *Farmer's Market* (2010) was the first darkweb marketplace, but *Silk Road* (2011) marks the beginning of a new era and new breed of marketplaces, much more similar to the ones that exist today, due to its greater popularity and impact

aspect of botnets lies at the center of our methodology and analysis.

VI. Conclusion

Darkweb marketplaces are a stepping stone for malicious individuals who wish to enter the cybercrime world. They offer an array of options for botmasters who wish to establish their infrastructure, maintain or update it. They can also utilize marketplaces to provide their services to clients to achieve profit, while remaining anonymous thanks to the obfuscation mechanisms implemented by the platforms and the Tor network itself.

In this paper, we crawl the products, services, and vendor profiles of 26 darkweb marketplaces with focus on the botnet-related listings, resulting in a final dataset of $36,314$ listings and $1,163$ vendors. Our main purpose is to uncover how the segments of the botnet *Value Chain Model*, are reflected upon the listings available on these platforms, and how this correlation can be interpreted in terms of botnet setup, maintenance, and revenue. Our results indicate that botmasters have a wide variety of options on all of these three types of activities, which also come in prices that make them very accessible. We also present the aggregated details of these listings and the sellers providing them, such as pricing, type, and vendor reputation. We find 76.2% of the listings to be located on 5 of the marketplaces, with the category of *Banking/Carding* accounting for 29.3% of the listings and 63.3% of the vendors. Additionally, *Monetization* is the model segment with the most associated listings at 86.6% of the data. The largest marketplaces at the time of our crawls, is found to be hosting around 21.6% of the vendor pool and 28.6% of the listings. In an effort to track vendor activity across the 26 marketplaces, we use their usernames and PGP keys. Our results suggest that only 145 (12.5%) vendors use the same username and 151 (13%) the same PGP key across multiple platforms. Lastly, since we would like to contribute as much as we can in future works by other researchers, we also elaborate on our architecture and methodology applied, and plan to release the dataset after the acceptance of the paper.

References

[1] eSentire. 2022 official cybercrime report. [Online]. Available: https://www.esentire.com/resources/library/2022-official-cybercrime-report

[2] S. Morgan. Cybercrime to cost the world 8 trillion annually in 2023. [Online]. Available: https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

[3] D. Georgoulias, J. M. Pedersen, M. Falch, and E. Vasilomanolakis, "A qualitative mapping of darkweb marketplaces," in *2021 APWG Symposium on Electronic Crime Research (eCrime)*. Boston, MA, USA: IEEE, 2021, pp. 1–15.

[4] K. Levchenko, A. Pitsillidis, N. Chachra, B. Enright, M. Félegyházi, C. Grier, T. Halvorson, C. Kanich, C. Kreibich, H. Liu, D. McCoy, N. Weaver, V. Paxson, G. M. Voelker, and S. Savage, "Click trajectories: End-to-end analysis of the spam value chain," in *Proceedings of the 2011 IEEE Symposium on Security and Privacy*, ser. SP '11. USA: IEEE Computer Society, 2011, p. 431–446. [Online]. Available: https://doi.org/10.1109/SP.2011.24

[5] M. Karami, Y. Park, and D. McCoy, "Stress testing the booters: Understanding and undermining the business of ddos services," in *Proceedings of the 25th International Conference on World Wide Web*, ser. WWW '16. Republic and Canton of Geneva, CHE: International World Wide Web Conferences Steering Committee, 2016, p. 1033–1043. [Online]. Available: https://doi.org/10.1145/2872427.2883004

[6] D. Georgoulias, J. M. Pedersen, M. Falch, and E. Vasilomanolakis, "Botnet business models, takedown attempts, and the darkweb market: A survey," *ACM Comput. Surv.*, vol. 55, no. 11, feb 2023. [Online]. Available: https://doi.org/10.1145/3575808

[7] F. I. Team. (2017) Threat actors discuss circumvention techniques against "bank drop" detection. [Online]. Available: https://flashpoint.io/blog/bank-drop-techniques/

[8] Swift. (2020) How cyber attackers 'cash out' following large-scale heists. [Online]. Available: https://www.swift.com/news-events/news/how-cyber-attackers-cash-out-following-large-scale-heists

[9] P. Paganini. (2013) An interesting post by brian krebs is food for thought on the business behind a cashout service for cybercriminals. [Online]. Available: https://securityaffairs.com/14907/cyber-crime/the-business-behind-a-cashout-service-for-cybercriminals.html

[10] J. Martin and N. Christin, "Ethics in cryptomarket research," *International Journal of Drug Policy*, vol. 35, pp. 84–91, 2016.

[11] J. Martin, *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs*. Springer, 2014.

[12] J. Martin, "Lost on the silk road: Online drug distribution and the 'cryptomarket'," *Criminology & Criminal Justice*, vol. 14, no. 3, pp. 351–367, 2014.

[13] D. Décary-Hétu and J. Aldridge, "Sifting through the net: Monitoring of online offenders by researchers," *European Review of Organised Crime*, vol. 2, no. 2, pp. 122–141, 2015.

[14] M. J. Barratt, S. Lenton, and M. Allen, "Internet content regulation, public drug websites and the growth in hidden internet services," *Drugs: education, prevention and policy*, vol. 20, no. 3, pp. 195–202, 2013.

[15] J. Buxton and T. Bingham, "The rise and challenge of dark net drug markets," *Policy brief*, vol. 7, pp. 1–24, 2015.

[16] 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*, 2013, pp. 213–224.

[17] 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.

[18] A. Cuevas, F. Miedema, K. Soska, N. Christin, and R. van Wegberg, "Measurement by proxy: On the accuracy of online marketplace measurements," in *31st USENIX Security Symposium (USENIX Security 22)*. Boston, MA: USENIX Association, Aug. 2022, pp. 2153–2170. [Online]. Available: https://www.usenix.org/conference/usenixsecurity22/presentation/cuevas

[19] D. Georgoulias, R. Yaben, and E. Vasilomanolakis, "Cheaper than you thought? a dive into the darkweb market of cyber-crime products," in *Proceedings of The 18th International Conference on Availability, Reliability and Security (ARES 2023)*. ACM, 2023, 12th International Workshop on Cyber Crime, IWCC.

[20] Monero. (2017) The merits of monero: Why monero vs bitcoin. [Online]. Available: https://www.monero.how/why-monero-vs-bitcoin

[21] Z. Albeniz. (2019) A europol officer confessed that they could not track monero (xmr) transactions. [Online]. Available: https://medium.com/@ziyahanalbeniz/a-europol-officer-confessed-that-they-could-not-track-monero-xmr-transactions-dbd568f02922

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

[23] 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*, 2018, pp. 1845–1854.

[24] J. Demant, R. Munksgaard, and E. Houborg, "Personal use, social supply or redistribution? cryptomarket demand on silk road 2 and agora," *Trends in Organized Crime*, vol. 21, no. 1, pp. 42–61, 2018.

[25] G. P. Paoli, J. Aldridge, R. Nathan, and R. Warnes, "Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web," 2017.

[26] A. Hutchings and T. J. Holt, "A crime script analysis of the online stolen data market," *British Journal of Criminology*, vol. 55, no. 3, pp. 596–614, 2015.
[27] A. Bracci, M. Nadini, M. Aliapoulios, D. McCoy, I. Gray, A. Teytelboym, A. Gallo, and A. Baronchelli, "Vaccines and more: The response of dark web marketplaces to the ongoing covid-19 pandemic," *PloS one*, vol. 17, no. 11, p. e0275288, 2022.
[28] D. Georgoulias, J. M. Pedersen, M. Falch, and E. Vasilomanolakis, "Covid-19 vaccination certificates in the darkweb," New York, NY, USA, apr 2022. [Online]. Available: https://doi.org/10.1145/3530877
[29] S. S. Silva, R. M. Silva, R. C. Pinto, and R. M. Salles, "Botnets: A survey," *Computer Networks*, vol. 57, no. 2, pp. 378 – 403, 2013, botnet Activity: Analysis, Detection and Shutdown. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128612003568
[30] S. Khattak, N. R. Ramay, K. R. Khan, A. A. Syed, and S. A. Khayam, "A taxonomy of botnet behavior, detection, and defense," *IEEE Communications Surveys Tutorials*, vol. 16, no. 2, pp. 898–924, 2014.
[31] K. Alieyan, A. ALmomani, A. Manasrah, and M. M. Kadhum, "A survey of botnet detection based on dns," *Neural Computing and Applications*, vol. 28, no. 7, pp. 1541–1558, 2017.
[32] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis *et al.*, "Understanding the mirai botnet," in *26th USENIX security symposium (USENIX Security 17)*. USA: USENIX Association, 2017, pp. 1093–1110.
[33] D. Dittrich, "So you want to take over a botnet," in *Proceedings of the 5th USENIX Conference on Large-Scale Exploits and Emergent Threats*, ser. LEET'12. USA: USENIX Association, 2012, p. 6.
[34] G. Bottazzi and G. Me, "The botnet revenue model," in *Proceedings of the 7th International Conference on Security of Information and Networks*, ser. SIN '14. New York, NY, USA: Association for Computing Machinery, 2014, p. 459–465. [Online]. Available: https://doi.org/10.1145/2659651.2659673
[35] C. G. J. Putman, Abhishta, and L. J. M. Nieuwenhuis, "Business model of a botnet," in *2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)*. USA: IEEE, 2018, pp. 441–445.

APPENDIX

A. Parsing value types

In this section we present the entirety of the value types targeted by the crawler and parser applications of our system. For more context on each individual type, see *Georgoulias et al.* [3].

Listings	Vendors
Listing link	Source listing
Listing title	Profile link
Description	Name
Vendor	PGP key
Price	Description
Currency	Member since
Sold	Vendor since
Rating	Feedback entries
Reviews	Overall feedback
Shipping from	Rating/Trust level
Shipping to	Vendor level (based on sales)
Shipping method	Finalize early
Payment type	Disputes won
Stock	Disputes lost
Product subcategory	Total disputes
Product category	Sold
Featured/promoted listing	Sales on other marketplaces
	Other marketplaces
	Total sales

Table VI: Value types parsed from the HTML files.

B. Listing & vendor concentration tables

In this section we present the listing and vendor concentration throughout the marketplaces. The name of the platforms are provided only for the reviewers, and will be anonymized after the acceptance of the paper.

Marketplaces	Vendor count	Percentage
Market 1	251	21.58%
Market 2	125	10.75%
Market 3	108	9.29%
Market 11	99	8.51%
Market 5	96	8.25%
Market 4	68	5.85%
Market 6	59	5.07%
Market 8	44	3.78%
Market 9	42	3.61%
Market 7	37	3.18%
Market 14	30	2.58%
Market 19	23	1.98%
Market 13	19	1.63%
Market 17	18	1.55%
Market 16	17	1.46%
Market 15	16	1.38%
Market 12	16	1.38%
Market 23	16	1.38%
Market 18	16	1.38%
Market 24	16	1.38%
Market 10	13	1.12%
Market 21	12	1.03%
Market 25	8	0.69%
Market 20	7	0.60%
Market 22	4	0.34%
Market 26	3	0.26%

Table VII: Vendor concentration on the 26 marketplaces

C. Botnet value chain model

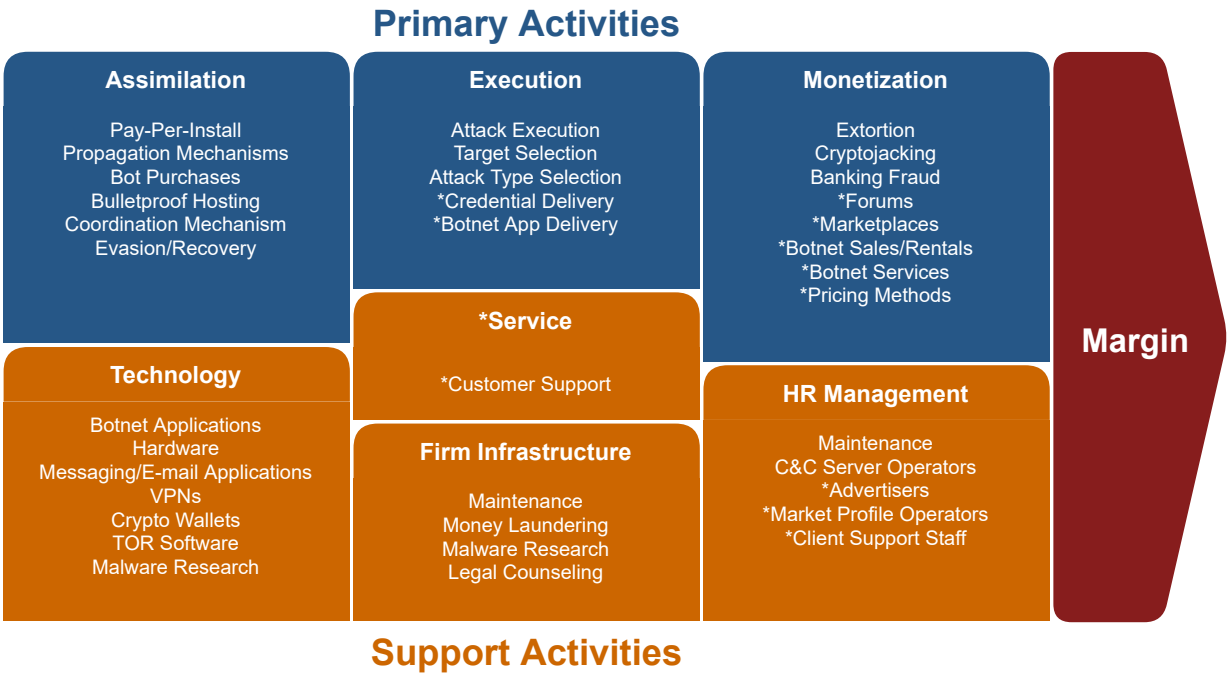

Figure 5: Botnet value chain model [6].