Get Rich or Keep Tryin' Trajectories in dark net market vendor careers

Booij, Tim M. ; Verburgh, Thijmen; Falconieri, Federico ; van Wegberg, Rolf S.

DOI
10.1109/EuroSPW54576.2021.00028

Publication date
2021

Document Version
Submitted manuscript

Published in
Proceedings - 2021 IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2021

Accepted Author Manuscript. Link to published article (IEEE): https://doi.org/10.1109/EuroSPW54576.2021.00028

Get Rich or Keep Tryin' Trajectories in dark net market vendor careers

Tim M. Booij*, Thijmen Verburgh*, Federico Falconieri*, Rolf S. van Wegberg†
*Netherlands Organisation for Applied Scientific Research, TNO
†Delft University of Technology
{tim.booij, thijmen.verburgh, federico.falconieri}@tno.nl; r.s.vanwegberg@tudelft.nl

***Abstract*—Dark net markets are a competitive environment. As these anonymous markets enable criminals to trade illicit goods or services, this causes vendors to operate under pseudonyms, rather than real-world identities. The constant battle between market admins and law enforcement makes the typical lifespan of a market two years. When a market disappears, active vendors migrate to other markets with the intention to continue their business, or have already pro-actively done so in an effort to ensure business continuity. To secure their reputation across markets, they can try to obtain the same pseudonym on multiple markets, but other individuals could beat them to the punch. A much safer method therefore, is to generate a PGP-key and use the public key as identification across markets. This way, vendors signal their continued trustworthy and reputable service on markets to buyers.**

In this paper, we leverage the use of PGP-keys to map careers of dark net market vendors. We parse and analyze scraped data from over 90 dark net markets (2011-2015), and discern 2,925 unique careers. By employing group based trajectory modelling, a type of latent class analysis, we infer three different career trajectories - differentiating 'established', 'challenger' and 'failed' vendor careers. We show that these trajectories are heavily unbalanced in terms of longevity and success. We find that on average 80% of careers last just four months and generate very little sales. Only a small group (~2%) of highly successful vendors have a long and uninterrupted career that lasts years and spans multiple markets. This group is also responsible for at least 31% of the total revenue in our data.

***Index Terms*—Dark net markets, Vendor careers, PGP-keys, Cybercrime**

I. Introduction

Business continuity management is one of the paramount challenges for any entrepreneur. Running an anonymous, illegal business - e.g., selling illegal narcotics on dark net markets - however, requires the mechanisms found in the legal economy to ensure to stay in business, like trust and reputation, to be adapted. These dark net markets are commercial websites, operating through anonimization protocols such as Tor or I2P, designed to connect both vendors and buyers of illicit products. To prevent that anonymity turns into distrust, vendors on these markets are reviewed based on the buyer's satisfaction of the products sold and services provided. Over time, vendors build a reputation based on these reviews, providing potential buyers with a certain level of confidence in that specific vendor. As a byproduct, growing a reputation on these dark net markets, might attract increased attention of law enforcement. As resources are scarce, they tend to target vendors with high turnover - what they call 'the big fish'. Although dark net markets provide anonymity through technical means, one needs to take precautions as some elements of doing business - e.g., bitcoin payments, direct messaging of personal information or other sloppy mistakes - can still be used to attribute 'anonymous' activity to real-world identities. Here, vendors are confronted with an *identification dilemma* - work with a single pseudonym across markets, creating an identifiable *career* but risking more exposure, or working with multiple pseudonyms, providing more protection, but not allowing to build reputation over longer periods of time.

Next, vendors need to deal with identity management across multiple markets, as a vendor's pseudonyms can differ from market to market. In order to help buyers identify vendors across platforms, the community has adopted PGP-keys. These PGP-keys allow for encryption and decryption of messages and work separate from the marketplaces. If a message can be decrypted by multiple pseudonyms, it is very likely they are the same vendor. By using PGP-keys, it becomes possible to track dark net market vendors across multiple platforms, allowing us to gain insights into their career trajectories. Without linking different pseudonyms using PGP-keys, one can only study a 'career' on a single market.

Leveraging public PGP-keys in order to link pseudonyms across markets has been used in the past. However, these studies mainly focus on the effectiveness of PGP linkage [1] or provide generic insights into dark net market vendors [2]. Other researchers studied the differences of dark net market vendors and touched upon careers, but insights are limited to a single market [3]. An analysis specifically on criminal careers, spanning multiple dark net markets, is therefore still lacking.

In order to gain insights in dark net market vendor careers, we combine methodologies used for market analysis, such as sales activity based on feedbacks [4], with methods which are used within dark net market migration research [5]. Combining these methods have allowed us to analyse the careers of vendors within the dark market ecosystem and gain insights into their characteristics. Using group-based trajectory modeling, we have unravelled different groups vendors with similar trajectories. Additionally, by analyzing their sales over time, we have been able to construct an age-crime curve and survivability of these groups.

As part of the open-review model followed on WACCO this year, all the reviews for this paper are publicly available at https://github.com/wacco-workshop/WACCO

In this paper, we make the following contributions:

- We present the first comprehensive study into career trajectories of dark net market vendors, leveraging existing scrape data from over 90 dark net markets (2011-2015) comprising of 21,544 unique PGP-keys, to discern 2,925 unique careers who advertise 23,228 items with over 2,1 million approximated sales.
- We develop *PGPsucker* - a dedicated parser able to extract PGP-keys and corresponding metadata from dark net market and forum scrapes.
- We employ group-based trajectory modeling to infer three career trajectories of dark net market vendor. Next to a large portion of 'failing' careers (*n=2,368*), we find a large group so-called 'challengers' (*n=507*) who bear the same perseverance as 'established' vendors (*n=50*), but lack their dominance in sales.
- We show that these career paths are heavily unbalanced in terms of longevity and business success. We find that 80% of careers on average last just four months and generate very little turnover. Only a small group (~2%) of highly successful vendors have a long and uninterrupted career that lasts years and spans multiple markets. This group is also responsible for at least $50,805,700 in revenue - 31% of the total revenue in our data.

The remainder of this paper is structured as follows. Section II describes how dark net markets operate, what PGP-keys are and synthesises earlier work into dark net market careers. Section III describes our measurements methodology. In Section IV, we present our analysis of all PGP-keys found, followed by Section V that discusses in-depth the characteristics of three dark net market vendor career trajectories we develop. In Section VI, we discuss the limitations and public policy take-aways, where Section VII presents additional related work. Section VIII concludes.

II. Background

A. Dark markets

Dark net markets are commercial websites that operate through anonymization protocols, such as Tor or I2P [6]. Their popularity has steadily grown since the infamous Silk Road 1. These markets offer a broad range of illegal products and services such as drugs, credit card details and ransomware [2], [7]. Two constructs, anonymity and trust, contribute to the business model and the functionality of dark net markets [3], [8]–[13]. The most popular anonymization protocol, Tor, allows for both anonymous hosting of the dark net market and anonymous browsing, by either vendors or buyers [8]. The usage of cryptocurrencies as the mandatory payment method on dark net markets, provides an even higher level of anonymity. Finally, the anonymous delivery of physical products is achieved by (mis)using the postal services [8].

Although this anonymous business model might seem to provide rather obvious scamming opportunities, there are dedicated mechanics in place to create the required level of trust to stimulate 'honest' trading. The markets often provide escrow services for transactions, and act as a mediator and judge when disputes occur. This results in an ecosystem where vendors and buyers do not have to trust each other, they only need to trust the dark net market. Another mechanism that generates this trust, is the review system. Such a system allows buyers to evaluate vendors after a transaction, allowing actors to build a reputation on a market. The buyers can take all aspects of the purchase into account when providing feedback - information provided by the vendor, communication style, customer service, and shipping speed all contribute to a satisfactory rating.

Investing in a good reputation allows vendors to sell more in the long run, and charge higher prices for their products [10]. A bad reputation has a great impact on the sales and prices, as bad reputations are hard to repair. Furthermore, returning customers appear to have a main supplier for around 60% of their purchases [14]. On this, Décary-Hétu & Quessy-Doré [14] argue that one of the reasons a buyer might have for *not* being loyal to their main vendor, is to limit the dependence on that vendor and have multiple trusted back-ups available. This indicates that it is worthwhile to maintain a good reputation.

Migration patterns can be observed when markets shutdown, forcing actors to either quit or continue trading on a different platform [2], [5], [15], [16]. Law enforcement interventions have a huge impact on the ecosystem of dark net markets, however long term impacts are debated in earlier work [2], [15]. When studying the impact on the daily revenue of the entire dark net market ecosystem, high resilience to and fast recovery after take-downs and exit-scams can be observed [2].

B. PGP

Whilst migrating to a new dark net market, vendors encounter a challenge - verifying their previous identity. Using the same pseudonym as on previous platforms is not a strong verification, as this might be used by other vendors who registered faster. To prevent this, PGP-keys are used as a cross-platform identify verification method [8], [17]. PGP is a data encryption method that provides privacy, confidentiality and authentication through symmetric-key cryptography. The confidentiality aspect of PGP, is used to provide the possibility of identity verification – only one entity can access the encrypted content of the data or messages.

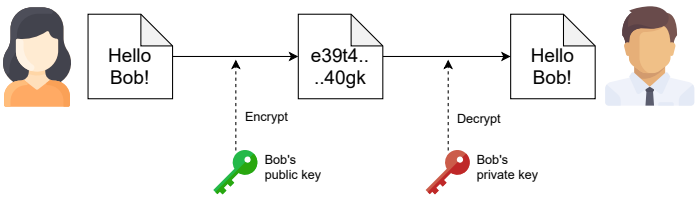

Fig. 1: Public key encryption example

Figure 1. provides a illustration of how PGP is used between Alice and Bob to send a message securely. By using the public key of Bob, Alice can encrypt data or a message, which only Bob - the owner of the corresponding private key - can decrypt in order to access the files or read the message. If Bob wants to reply to Alice, he will have to use the public key of Alice. A public key is derived from a private key and is distributed

by the owner of the private key. Listing 1 provides an example of the structure of such a public PGP-key.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: Keybase OpenPGP v1.0.0

xm8EX9eHqBMFK4EEACIDAwSbIEWff2bnJECZWpMPq
zpHEecPABJ6TO+B7VvIo4Otu4JS9QYgheknEZQG/u
y74qNxFR4qx5Ro8Vy5z9DATNFHRlc3QgPHRlc3RAd
Al/Xh6gCGy8DCwkHAxUKCAIeAQIXgAAKCRDpkPSW3
            <... more ...>
h/x+dCaoXoVY8cLAJwQYEwoADwUCX9eHqAUJDwmcA
BBkTCgAGBQJf14eoAAoJELRdeY4tnRtNAxgBAPy53
MNe5zwVSl05YPI8aAP4iaStTW2VnxD5XParH/lx8X
AYCBabiWZaGEhDzrNlIqeuUQ13sxyZPxwrbK3ieAt
xfwBfji7OJ/g+VYGtGbjUPfW89BIZVerpAT9PLHcX
2taP2A==
=569Z
-----END PGP PUBLIC KEY BLOCK-----
```

Listing 1: Example structure of a PGP-key

Vendors often have a public PGP-key available in their profile for this purpose, see Figure 2 for a currently active example. Soska & Christin [2] found that the usage of PGP-keys on Silk Road 1 by vendors was around 66% and increased to around 90% between 2013 and 2015 on other markets.

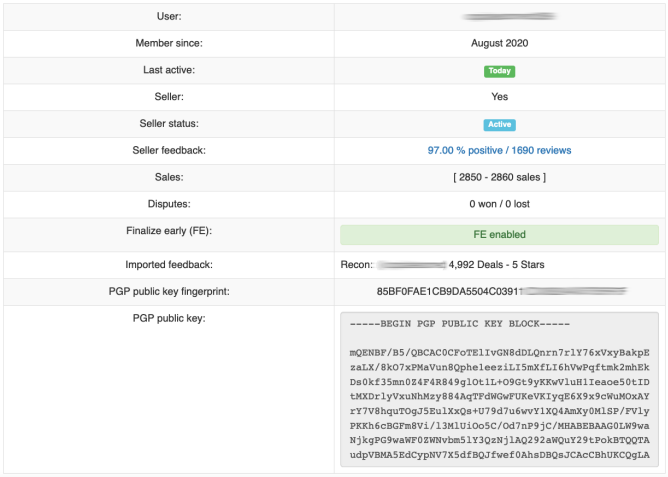

Fig. 2: Example of PGP usage on White House Market

C. Careers

Previous work on dark net market vendor careers is currently limited to observations on a single market. Paquet-Clouston et al. [18] differentiated three groups of vendors - low, mid and high level vendors. They observed that 90% of vendors on Alphabay were unsuccessful and most vendors have a market presence of less than six months.

Soska & Christin [2] have studied vendors across multiple dark net markets by associating the same pseudonyms. They observed that 50% of the vendors are present for 220 days or less. Over 10% of the vendors were active throughout the entire measurement interval, which spanned from 2013 to 2015. They concluded that ~25% of all vendors remain active for years on multiple platforms.

Migrating to new dark net markets, forced or voluntarily, can be regarded as defining events during a criminal career. As there is little research which provide insights on careers spanning across multiple markets, there is also not much known about the effects of interventions on vendor careers. Van Wegberg & Verburgh found that approximately 60% of the newly registered vendors on the Dream market forum stuck to the same identity, after Operation Gravesac and Operation Bayonet shut down the top tier market Alphabay and Hansa market [5]. Furthermore, they also found that of this 60%, only $2/3$, kept using the exact same pseudonym and PGP-key [5]. Others, however, found that most vendors did not move to other markets after a intervention [15]. This might be because successful vendors tend to migrate to new markets while keeping the same identity and therefore the transfer their reputation [16]. For unsuccessful vendors there seems little incentive to do the same.

III. Measurement Ethodology

To analyze careers on dark net markets, suitable datasets and methods are essential. In this section we first discuss the toolset we have designed to extract PGP-keys from dark net market scrapes, followed by the datasets we have used and integrated for the analyses in this paper.

A. Parsing vendor information

Dark net market research often starts with scraping, the collection of raw HTML directly from live markets [2], [19]. The raw HTML is not useful quite yet, in terms of criminal career analysis, and needs to be processed. Most commonly, some form of parsing is performed on the HTML documents to extract the features of interest. Whereas open source technology to perform automated web scraping exists and it is easily accessible, parsing technology is available only in elementary building blocks. An open source tool that performs out-of-the-box parsing of criminal career identifiers from raw HTML does not yet exist. For this reason, we have developed an open source, scalable, automated and modular parsing pipeline.

Here, our contribution is a Python package - 'PGP-sucker'. This small Python library provides functionality to index HTML documents in a PostgreSQL database, providing the ability to extract PGP-keys and usernames from dark net market HTML files. PGP-key extraction is quite straightforward. PGP public keys must all start and finish with the special strings `-----BEGIN PGP PUBLIC KEY BLOCK-----` and `-----END PGP PUBLIC KEY BLOCK-----` [20], allowing easy extraction using a regular expression. The PGPy Python library is then used to analyse the raw public key [21]. If the raw key is in fact a real key, PGPy will extract a rich set of metadata from the public key. Among others, metadata includes the key registration and expiration dates. We also carve out of the PGP public key the occasional `comment` or `version` attributes. Username extraction is performed with a collection of techniques tailored specifically to dark net market scrapes. The developed Python package consist of three specific Docker images, each designed to perform a specific task in the data acquisition - indexing, PGP-key parsing and username parsing. Figure 3 shows the high level architecture of the parsing pipeline.

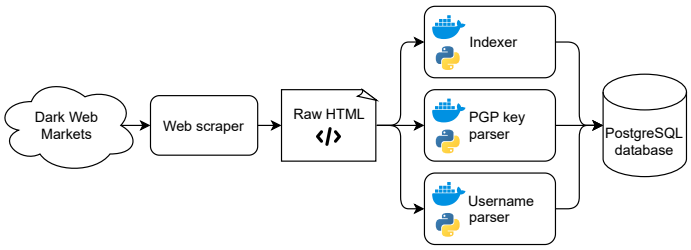

Fig. 3: High Level architecture of automated parsing pipeline

B. Aggregating multiple datasets

Multiple parsing efforts have typically been performed by researchers, all with different goals and using different data storage methods - ranging from relational databases to CSV files. Searching across multiple datasets can also be useful for law enforcement, as the datasets may augment each other. This can take quite some time, and is typically performed manually case by case.

To solve this problem we have designed a pipeline to automatically aggregate an heterogeneous body of datasets. For each available data source, our pipeline requires a Logstash configuration specific to that data source. Logstash takes care of ingesting data from the source and storing it in an aggregated Elasticsearch repository. Figure 4 shows the high level architecture of the aggregation pipeline.

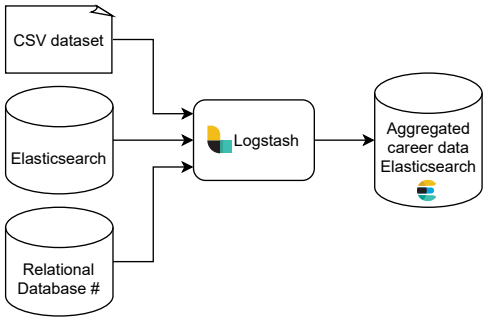

Fig. 4: Automated aggregation pipeline

C. Data

In this paper, we leverage two different datasets - the Dark Net Markets archive [22] and the parsed and analyzed dataset provided by Soska & Christin [2]. The Dark Net Markets (DNM) archive, is a collection of weekly or daily scrapes performed on all English dark net markets during the period 2011-2015. This collection covers 89 markets and 37 related forums. These raw HTML scrapes contain vendor pages, feedbacks on these vendors, related images, timestamps, and much more. For the purpose of this paper, we focus on the PGP public keys located on the vendor pages in these scrapes. To extract these PGP-keys, along with related metadata, we utilize our parsing pipeline as described in Section III-A. This resulted in a total of 21,544 unique PGP-keys found.

The DNM archives provide us with PGP-keys from specific vendor pseudonyms on a dark net market. In order to characterize these careers, we need data on the activity - i.e., sales - of these vendors over time. For this, we turn to the dataset created by Soska & Christin, which contains information about item listings and feedbacks on multiple prominent dark net markets as can be seen in Table I. For each of the listings posted by vendors on these markets, the dataset contains information as the title, descriptions, advertised prices, timestamps, and most importantly the feedbacks on each item. Previous research has shown that feedbacks have proven to be a good proxy for sales, and provide a structural lower bound of sales [2], [4], [7], [19].

TABLE I: Markets scraped by Soska & Christin [2]

Market	Listings	Vendors	Feedbacks
Agora	3,240	526	234,372
Black Market Reloaded	2,069	386	62,876
Evolution	9,551	1,002	464,146
Hydra	377	28	43,701
Pandora	1,204	169	89,065
Silk Road 1	4,053	645	605,744
Silk Road 2	2,734	441	662,497

Combining both datasets enables us to link numerous pseudonyms across multiple dark markets and aggregate careers through the proxy of PGP-keys. The intersection results in *pseudonym-PGP key* and *pseudonym-feedback* pairs. From this we can derive the pair *PGP key-feedback*, enabling us to follow PGP-keys over time - our definition of a vendor career. This combined dataset leaves us with unique 2,925 PGP keys with pseudonyms and feedback on their products.

IV. PGP Key Descriptives

This section will discuss the descriptive statistics of the extracted PGP-keys and a longitudinal analysis of key implementation in the dark net market ecosystem. As elaborated in Section III-C, we have obtained a total of 21,544 unique PGP keys from the DNM archives and therefore assume that a same amount of pseudonyms were active on dark markets between 2011 and 2015. Note however, that individuals might share PGP-keys or even use multiple different keys. This means, the total number of keys cannot be used to infer the amount of active vendors prior to matching them to vendor activity on markets.

Figure 5 shows the creation dates of the PGP-keys in the DNM archives from 2011, the approximate launch date of Silk Road 1, onward. A mere 27 keys were created prior to 2011. Curiously, the oldest created key dates back to November 1991. The PGP-keys we extracted on dark net markets seem to be created specifically for that purpose, as almost all keys were created after 2011. This is hypothesis is further supported by the median time between the creation date and the first seen date, which is 109 days. Within this time span, a dark net market vendor has to create their account on a dark market, publish their PGP-key and the scraper has to extract the key from the dark net market.

A sharp increase in the creation of PGP-keys can be seen after Operation Marco Polo, when Silk Road 1 was taken down. Before Operation Marco Polo, the use of PGP-keys was lower than after the operation [2]. We believe that this increase is due to the fact that after Silk Road 1 users were forced to migrate for the first time and encountered the problem

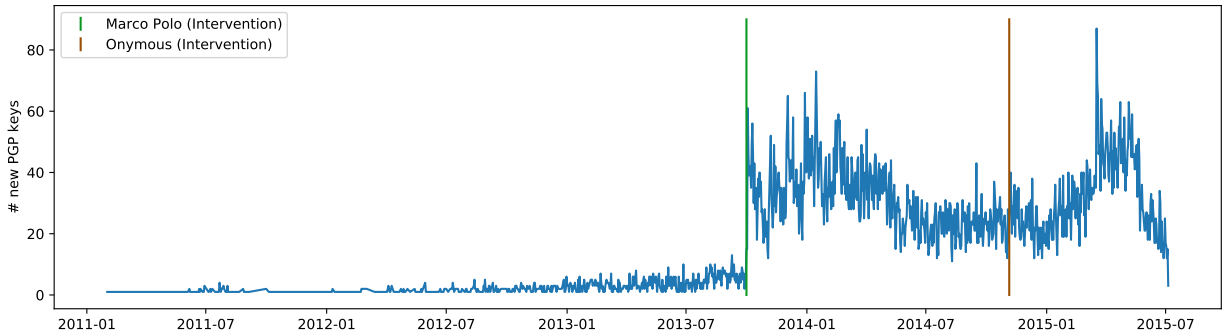

Fig. 5: Creation dates of new PGP-keys with major interventions

of transferring identity and reputation. After operation Marco Polo, PGP-keys seem to be integrated in the modus operandi of dark net market vendors. On top of this, a rise in popularity and coinciding influx of vendors can also contribute to the higher number of daily created PGP-keys.

In contrast, it seems that Operation Onymous might not have had a large direct effect on the influx of new PGP-keys, as can be seen in Figure 5. However, a steady increase starts around two months after Operation Onymous. We hypothesise that this can be explained by the ecosystem recovering from the operation slowly, and that the influx of new vendors consisted of both true 'new' vendors and those that discarded their previous identity [5].

V. Career Analysis

The previous section has elaborated on PGP-keys, where we have demonstrated how keys can used to track vendor activity over time. By taking this one step further, we can aggregate these insights into criminal careers with a great level of confidence. In this section we will combine scraped data on dark net market listings and feedbacks by Soska & Christin, with PGP-keys extracted from the DNM archives as explained in Section III-C. We will show how we utilize a latent profile analysis to distinguish between different careers trajectories.

A. Defining a career

Before unraveling the differences between careers of dark market vendors, it is paramount to grasp how such a career can be portrayed. As we have explained, we investigate the binding factor of PGP-keys as link for a career. Pseudonyms of vendors can be attributed to each other by their public key. Figure 6 depicts an example timeline of a career, which has been unraveled through this method. This timeline shows a couple of interesting details about this vendor. Throughout his or her career, multiple different pseudonyms have been used. Starting off with the same pseudonym, *Topdrugs*, for two different markets, following with three other pseudonyms for respectively *Evolution* and *Agora*. Interestingly, the pseudonym *rockstar35UK* generates significantly less revenue compared to the other pseudonym on Evolution, *superdrugz* - $33 compared to $21,889. It could be that the vendor was quite hesitant after Silk Road 2 was shut down. All these pseudonyms and activity can be associated with the same vendor - creating a career over time. This provides us with much more insights into the actual career vendors accumulate on dark net markets. By linking these pseudonym to one entity, we are able to track vendors over time.

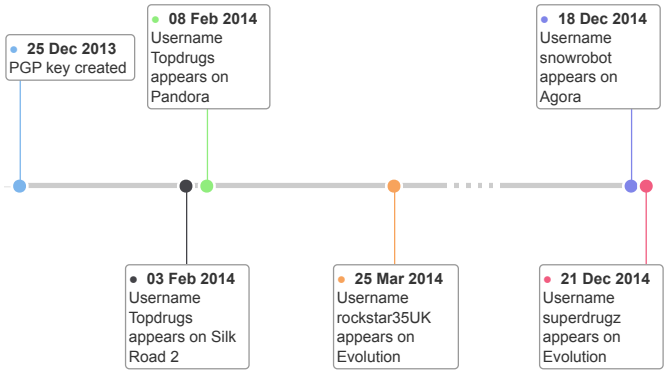

Fig. 6: Timeline of a career

B. Group-Based Trajectory Modeling

Criminals build their own career path - each with its own beginning and, most of the time, ending point. Prior research has been done on analyzing a broad spectrum of criminal career trajectories - ranging from burglars, to homicide offenders and even mafia organizations [23]–[27]. From earlier work we know that vendors have individual characteristics, which influence their success on dark net markets and ultimately determine the length and strength of their career [4].

We do not yet know if we can discern different career trajectories, however previous research suggests that latent groups of dark net market vendors can be found, differentiated by distinct characteristics, like their experience or activity [4]. In order to recognize patterns of activity, without assuming that specific groups exist, we consider group-based trajectory modeling (GBTM) - a model to identify clusters of individuals with similar activity over time.

Latent class analysis (LCA) is a subset of structural equation modeling, used to find groups or subtypes of cases in multivariate categorical data. GBTM is a type of LCA, aiming to reveal hidden groups without any prejudice about these possible groups. In contrast to the more static latent profile analysis, which is used to find groups based on a

complete picture of an individual as shown by Van Wegberg et al. [4], GBTM is more dynamic as it utilizes the *activity* over *time*. It is a statistical method, able to identify groups of distinctive trajectories. These are summarised by a definitive set of polynomial functions defined by time, as determined by a nonparametric maximum likelihood estimation. Turning to the field of criminology, Jennings et al. [28] elaborate on the fact that GBTM can be used to determine the age–crime curve of a particular criminal offending. They also explain that using GBTM an individual's criminal career can be depicted, without taking the structural elements of career dormancy, desistance, or onset into account. With GBTM, goodness of fit indicators like the Bayesian Information Criteria (BIC), the Akaike Information Criterion (AIC) and the log-likelihood (LL) can be used to determine model fit [29].

The particular nature of our data enables us to generate the variables required by GBTM. The activity of a vendor can be measured by the *amount of feedbacks* they receive on their sales. This also provides the time aspect, as we can measure feedbacks over time - which can be seen as the *experience* of a vendor.

Amount of feedbacks Vendors on dark markets provide listings with the products they sell. For each listing, the scrape data includes a lot of information on the product - title, description, advertised price, and a category classification. Besides these static variables, buyers can also leave a feedback on a listing, regarding the product and vendor. As we have discussed in Section III-C, previous research has shown that feedback is a reasonable proxy for sales. In contrast, using revenue skews towards activity captured in monetary value and not in transaction activity.

Experience Each vendor on the dark web has a certain amount of experience selling products. This can range from very experienced vendors, shipping large amounts of their products all over the world, to vendors with little to non-existing activity. Each feedback provided for a listing has a timestamp. The resolution for these timestamps is *per day*. A lower resolution was not feasible in our data and higher sampling lead to diverging models. To measure experience we use this specific characteristic of all listings belonging to a specific vendor's PGP-key. Consequently we can laterally follow the activity of all pseudonyms belonging to that specific PGP-key. To establish a baseline of uniformity, we set the day of the first feedback as starting point for a career. Accordingly, the ending point corresponds to the last day of activity. Days without any feedbacks, or a period of desistance, are taken into account as experience only *if* the vendor resumes activity afterwards.

TABLE II: GBTM output - 1 to 5 groups

	BIC	**AIC**	**LL**
1 Group	7198907	7198853	-3599422
2 Groups	4745907	4745786	-2372884
3 Groups	**4006577**	**4006766**	**-2003275**
4 Groups	3656106	3655850	-1827906
5 Groups	3482416	3482093	-1741022

Different GBTM models were created using the *crimCV* package in R, version 0.9.6 [30]. Table II shows the final results of the five models produced by the GBTM with an input of 2,925 careers. More groups could be created, however to maintain a good sense of clarity in the results, we chose to limit the emerging groups to five [24], [25]. To evaluate these results, the BIC, AIC and LL are depicted in the table, allowing us to compare the models with each other. An ideal model solution minimizes the BIC and AIC values [24]. Consequently, the values in Table II would point to a model with five groups, as the BIC and AIC are the lowest. However, in order to maintain a sense of interoperability, we added the requirement that a group should at least represent 1% of the total population [4]. When taking this into account, the model with three groups emerges as the best fitting model to our data, as the model with four groups drops significantly below this threshold (0,67%).

C. Defining the groups

In order to grasp a fundamental understanding of these three groups - i.e., career trajectories - we need to elaborate on their distinct characteristics. Tables III to V depict these characteristics and show the differences between five measured variables. Two of these variables have been used by the GBTM to create the model - the amount of feedbacks and the experience. The three other variables, the amount of *listings*, the *diversity* in product portfolio and *revenue* also provide useful insights into the intrinsic nature of our groups. For each group, all five characteristics are described by the mean, median, and the min/max values.

Listings We report the amount of listings based on the given feedbacks. The amount unique listings of all feedbacks for a certain vendor in a groups is taken into account. This amount gives insights into the amount of differentiation vendors have in a group in terms of products.

Diversity In addition to the diversification the amount of listings a vendor has, the product category says something about the diversity of a vendor's product portfolio. Our data provides a product category for each listing. To capture the diversity amongst the products a vendor offers, we attribute each vendor with a boolean diversity score. If a vendor has feedbacks covering multiple product categories - i.e., illegal narcotics and stolen credit cards - we classify this vendor as divers and provide it with a diversity of 1.

Multihoming Similar to the possibility of measuring product diversity, vendors can also have presence on multiple markets - this is called multihoming. For each vendor we measure this multihoming, again with a boolean score. When a vendor has made at least one sale on more than one dark market, we classify this multihoming score as 1.

Revenue Finally we report on the amount of revenue a vendor has accumulated during their career. This is again based on the sales proxied by each feedback times the price of the listing transacted. As one is not required to provide a feedback after the purchase, we can see this value as a lower bound of the earnings a vendor has made during their career.

The first group depicts the top hitting vendors - 'the big fish'. Overall they have grossed the highest amount of revenue, have the most listings, and feedbacks per day. We have named this group the 'established' group. These vendors are the most successful throughout their career and can be seen as professional vendors. The second group we encounter is a group which experience is even higher compared to the 'established' group. Interestingly, this group has less feedbacks per day. Also, the mean and median amount of revenue and listings are not on the same level as the top tier vendors. Due to these observations, we call this the 'challenger' group - persisting vendors who have long careers, despite the lack of major turnover. Finally, the third group consists of vendors who have 'failed' during their career. All characteristics are inferior compared both other groups. Their careers bleed out after a short stint on the market and the amount of feedbacks they receive is also very small.

TABLE III: Established group (*n=50*)

	Mean	**Median**	**Min**	**Max**
Feedbacks	18	10	0	1,036
Experience	526	434	65	1,733
Listings	182	183	8	498
Diversity	0.94	1	1	0
Multihoming	0.84	1	1	0
Revenue	$1,019,144	$568,018	$16,590	$5,293,392

TABLE IV: Challenger group (*n=507*)

	Mean	**Median**	**Min**	**Max**
Feedbacks	3	1	0	318
Experience	539	513	60	1,286
Listings	95	93	2	1,669
Diversity	0.82	1	1	0
Multihoming	0.88	1	1	0
Revenue	$214,235	$102,476	$26	$5,525,967

TABLE V: Failed group (*n=2,368*)

	Mean	**Median**	**Min**	**Max**
Feedbacks	1	0	0	314
Experience	121	81	1	829
Listings	16	10	1	199
Diversity	0.59	1	1	0
Multihoming	0.31	1	1	0
Revenue	$15,811	$3,018	$0	$358,486

As a result of the dynamic nature of GBTM, these groups give unique insights into the diversity amongst different vendor career trajectories on dark net markets. The characteristics of these three groups might suggest an inherit balance amongst them. Just 50 professional vendors make up the 'established' group. The vendors in this group have clearly 'made-it', looking merely at the mean gross sales this group has realized. A certain level of proficiency can be hypothesized when looking at specific vendors within this group, like *HumboldtFarms* and *GreenLeafLabs* - after having made a name for themselves on dark net markets, legalized companies with these names arose during their career prime. It is clear, that to become an established vendor on the dark net markets, it is essential to have a long lasting career with steady sales during this time.

The 'challenger' group is however a bit more diversified in terms of vendors. Table IV shows this group has similar experience to the 'established' group and the revenue is not bad either, but the amount of feedbacks is significantly less. This group contains vendors with high amounts of sales during a short period of time, and vice versa, vendors with low amounts of sales spread out over a significant lengthy career. We hypothesise this as a possible explanation for the significant amount of multihoming seen in this group. An example is the vendor *Shiny-Flakes*, who's career could be deemed established as a lot of revenue was made during his career but is placed in the 'challengers' group by our model. He was apprehended by law enforcement at his peak, bringing the length of his career down to less then three quarters of a year whilst grossing more than $5.5 million during this period. Interestingly, if activity was measured in revenue, this vendor would have been lost in the 'established' group, not allowing us to differentiate disrupted careers. If his career persisted, Shiny-Flakes would have made it into the established group. In contrast, the far less notorious *BooMstick* can also be found in the 'challenger' group - grossing a little north of $5,000 during a career which lasted over three years. Anyone aspiring to achieve anything on dark net markets, or vendors looking for an extra source of income, can be found in the 'challenger' group.

Finally, the remaining 80% of the vendors are found in the 'failed' group - these vendors have definitely not made it. Overall they have little revenue, low diversity amongst their listings and a short career. Most vendors in this group quit briefly after their first sale, which is also indicated by the rather low multihoming score. Examining the characteristics of all groups as defined by the GBTM provides a brief insight into their (dis)similarities. However, further exploration is required in order to say something about the persistence and survivability of vendors in these groups.

D. Crime curve

The age-crime curve is an observation on the timeliness of criminal behavior - a descriptive on the micro-level relationship between age and predisposition to offend. Throughout developmental criminology, a relationship between age and crime is believed to be one of the most consistent findings [31]. A lot of prior research has been done on these age-crime curves - most of them pointing to the conclusion that criminal behavior increases in adolescence and decreases in adulthood [32]. Jennings & Meade have made it clear that group-based trajectory models have changed the landscape of age-crime curve criminology research and argue that merely the surface has been scratched on this area [28]. We built upon this suggestion, by creating an age-crime curve for the careers of dark net market vendors in our data. In our case, we are not dealing with the actual ages of these vendors, but use the age of a career as a proxy for this.

Figure 7 shows the result of plotting the average feedbacks per day, for each of our three groups - thus creating an age-

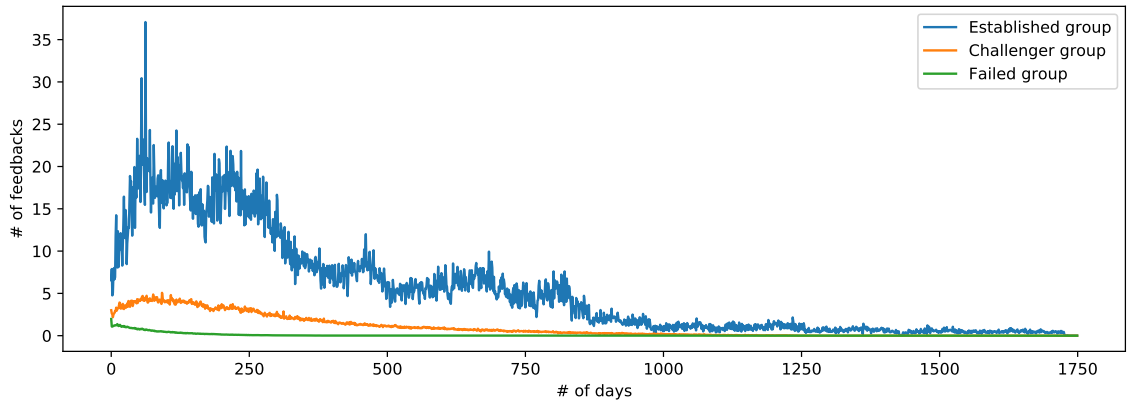

Fig. 7: Number of feedbacks per day from the beginning of a career

crime curve for vendors on dark net markets. The 'established' group stands out as the most prominent group. With only 50 careers, or 1.7% of the total, the dominance of this group can be observed distinctively. The 'established' and 'challenger' groups prolong a lasting career, both declining around 250 days. The 'failed' group is clearly not having the best career prosperity. Interestingly, a certain sense of 'adolescence' can be seen in the graph, with an increase in crime after the initial period and a decrease in 'adulthood'.

E. Survival of the fittest

As hinted in Figure 7, careers with more feedbacks, and higher revenue, stay active significantly longer. To complement this finding, we perform a survival analysis. For this we have used the Kaplan-Meier estimator [2], [33], which estimates the survival function $S(t)$ on lifetime data and is given by the following equation:

$$\widehat{S}(t) = \prod_{i:\ t_i \leq t} \left(1 - \frac{d_i}{n_i}\right) \tag{1}$$

where t_i is a day when at least one feedback was given, d_i the number of feedbacks given on a day, and n_i the number of careers up to day t_i. Figure 8 illustrates the survivability for each of the groups, or the probability a vendor in each group is still active after a certain amount of days. Immediately we can see that most vendors in the 'failed' group quit after half a year, which is in line with our previous observations. This graph however also illustrates that both the established and challenger groups follow the same career timeline in terms of longevity. After around 500 days, half of the vendors have stopped and almost all of them after about 3.5 years. Rather counter intuitively, this means that the vendors in the 'challenger' group have the same level of persistence as the 'established' vendors. Even though the 'challenger' group is not as successful as the 'established' group it seems that there is enough incentive to continue their career and refrain from starting over with a new career. A potential explanation can be that the 'challenger' group includes part-time vendors that have another, legal or illegal, source of income that they supplement with a career as a dark market vendor.

VI. Discussion

In this section, we first discuss the limitations inherent to our measurement methodology and the implications on our results. Second, we will touch upon the public policy take-aways of our findings.

A. Limitations of methodology

We will next discuss the limitations of our study within three main areas. First, we will cover data processing limitations, second, the arguably unobtrusive behavior of dark net market vendors, and three, the extrapolation of our findings.

When conducting scientific analyses, validation is an important aspect. Scraped data is prone to biases or mistakes made in the crawler implementation. Beside this, operators of dark net markets do not provide usage statistics of their platforms - proving it difficult to have a sense of ground-truth.

Another limitation relates to several behavioural components of dark net market vendors, which might have influenced the results. A dark net market vendor needs to have a public PGP-key published in order to be scraped. The proportion of vendors publishing a public PGP-key grew from 66% to around 90% between 2012 and 2015 according to Soska & Christin [2], therefore we argue that this impact is limited. Second, we note that that 'copy-cat' vendors have been active, who publish not there own public PGP-keys on their profile - causing false connections. Doing this would however not make much sense, as these copy-cats will not be able read the encrypted messages - as they are not in possession of the private key. Additionally, vendors might change PGP-keys, whilst still providing a proof of transfer. This can be done by creating a so-called *clearsigned message* including the new public PGP-key. A downside of this method is that, once the source location of the clearsigned message is unavailable, the proof of transfer is rendered useless. No prior research has been done on the frequency of copy-cat vendors and clearsigned PGP-key transfers, but due to their downsides it is highly likely to be a small number.

The final limitation of this study, is to tread carefully when extrapolating our results beyond the time frame in this paper.

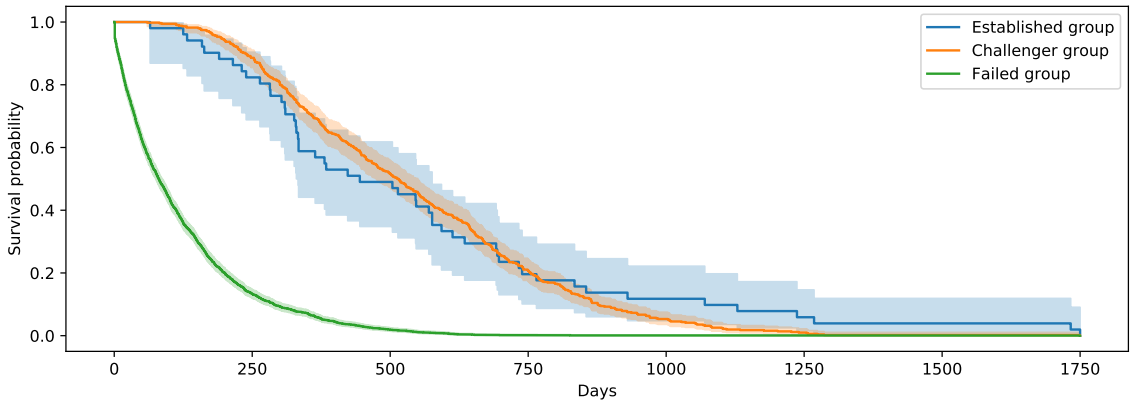

Fig. 8: Probability a given vendor in each group is still active after a certain period

The dark net market ecosystem is volatile and constantly changing [34] - and our analyses have been performed on data spanning 2011-2015. However, this study focuses on gaining insights on careers, not on quantifiable results about specific numbers. We argue that our high-level insights are tenable and not constrained by time.

B. Public policy takeaways

Our findings suggest that the majority of discovered PGP-keys in our data, are created for a special purpose - i.e., serving as an attribute for dark net market vendors. Not only do we find the creation dates of keys to be close to early activity of vendors, we see an intriguing pattern wherein events - like take-downs or exit-scams - coincide with influxes in key creation. After Operation Marco Polo (2013) we witness a sharp increase in key registrations. A similar increase is apparent after Operation Onymous (2015). These findings indicate that vendors create PGP-keys with the special purpose of linking them to their dark net market activity. This also means that it is unlikely to stumble across these keys in another setting - e.g., a key used for e-mail or other mainstream activity. In turn, a special purpose PGP-key therefore can be used to identify careers and attribute activity to real-world entities.

Leveraging PGP-keys to reconstruct careers, we find that dark net markets careers are hard to make – and break. We witness only a small group (~2%) of highly successful vendors (*n=50*) with a long career that lasts years. Interestingly, after a short period of peaking sales, the 'established' vendors seem to transact steadily for the remainder of their career. Not surprisingly, we see that ~80% of all vendors seem to 'fail' and as a consequence quit after just four months. Curiously, the group in between - the 'challengers' - seem to enjoy the same longevity in their careers, without reaching the same sales figures as the 'established' vendors. Note however, that this group also holds vendors, like the infamous vendor Shiny-Flakes, who's careers are interrupted due to law enforcement operations but did manage to generate generous revenue figures in their tenure on the market.

Based on these insights, authorities might differentiate interventions to target 'established' vendors. It seems that only this small group of vendors is able to be active for years and generate significant revenue. Given the limited resources of law enforcement, and their ambition to maximize impact of operations, it seems more efficient to focus on these careers. In reverse, we now also know what happens if law enforcement does not break a career. Our results show, that 80% of careers seem to generate little revenue - i.e., only a couple thousand dollars, and on average end after just four months. One could argue, that interventions aimed at the entire market population therefore are of little use. Since 80% of the actors on these markets are likely to last only four month either way. To put taxpayer money to best use, one could advocate to mainly target the other 20% by means of infiltration, pseudo-buys or other means at law enforcement's disposal.

VII. Related work

Parts of our paper build on or advance recent work on a number of topics. First, our work relates to earlier, criminological work into criminal careers. Second, our work can be tied to measurements of the nature, size and volume of trade on dark net markets. Third and last, we identify similar analyses as our group based trajectory modelling in studies into 'criminal performance' on underground markets. In this section, we discuss related work on these three topics.

Criminal careers First, our work relates to the extensive body of criminological work into criminal careers [31], [35], [36]. Since the early 1930's, research efforts have focused on mapping and understanding careers in the criminal enterprise[32]. Making use of official criminal records, most researchers reconstructed criminal careers of repeat offenders in an organized crime setting - ranging from burglars [26] to homocides [27]. Later, others investigated mafia careers and pathways in networks or terrorist organizations [23].

Like earlier work, we take frequency of activity - in our case transactions on an underground market - over time as features for an age-crime curve wherein we depict different pathways in doing business on dark net markets. In contrast,

we make use of measurements in the underground economy to best capture criminal activity. This way, we circumvent the bias in official criminal records, wherein only caught criminals are registered and their activity is based on sentenced offences.

Measurements on dark net markets Next, we leverage and build on longitudinal studies into the nature and size of dark net markets [1], [2], [7], [19], [37]–[40]. Prominent work by Soska & Christin maps sales numbers and vendor activity over time and across multiple markets [1], [2], [19]. Most studies include, or even focus on, drugs and physical goods, which make up a large proportion of the product portfolio [37], [38]. Others, like Van Wegberg et al. [7] investigate the trade of cybercrime commodities on these markets. Our work uses these measurements to derive and differentiate criminal careers.

Criminal performance on underground markets Finally, our insights advance the body of work on the 'criminal performance' of actors on underground markets [18], [41], [42]. Earlier work looked at the performance of actors based on what and how they sell, or their intrinsic characteristics - like experience. Earlier work by Decary-Hetu & Leppanen [41] and Holt et al. [42] predicted criminal performance on carding forums. They find that vendor experience and certain product features, like customer support options, predict the performance of carders. Similar to our work, Paquet-Clouston et al. [18] and investigate 'vendor trajectories' on AlphaBay using group-based trajectory modeling in vendor market share. Recent work by Van Wegberg et al. [4] unravelled latent profiles of vendors active in the cybercrime segment on AlphaBay.

VIII. Conclusions

In this paper, we present a comprehensive study into criminal career trajectories of dark net market vendors. We lever the fact that vendors use public PGP-keys to link pseudonyms across markets. In turn this allows us to discern careers.

In order to map vendors across markets using their public PGP-key, we developed a dedicated PGP parser, able to extract PGP-keys and corresponding metadata from dark net market scrapes. By leveraging two existing datasets, we capture 21,544 unique PGP-keys. By matching these PGP-keys to vendor activity across markets, we discern 2,925 unique careers. We have shown how a vendor can adopt many different pseudonyms, and combinations of these converge into a single career. In total, all identified careers combined advertise 23,228 items, generating at least 2,1 million approximated sales.

To unravel the differences between careers on dark net markets, we have employed group-based trajectory modeling - enabling us to identify clusters of vendors with similar activity over time. From this, we find career trajectories - the 'established', 'challenger' and 'failed' vendors. By applying an age-crime curve lens, we find that 80% of vendors have a career lifespan just short of four months, from which we argue that aiming interventions at marketplaces might have limited effects. Only a small group (~2%) of highly successful vendors is responsible for at least $50,805,700 in revenue - at least 31% of the total revenue in our data. Interestingly, the last group, the so-called 'challengers' (*n=507*) bear the same perseverance as these successful vendors, but lack their dominance in terms of sales - grossing not more than a modal legal income.

Many questions remain regarding the careers of vendors on dark net markets - such as migration patterns and the impact of interventions on individual careers. Here, we can see a clear added value of GBTM and its predictive capabilities studying the impact of interventions. Although these questions still remain, we have demonstrated that applying an age-crime lens on dark net markets allows us to gain a deeper understanding of the different career trajectories and can provide relevant insights towards evidence-based policing.

References

[1] X. H. Tai, K. Soska, and N. Christin, "Adversarial matching of dark net market vendor accounts," in *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 2019, pp. 1871–1880.

[2] K. Soska and N. Christin, "Measuring the longitudinal evolution of the online anonymous marketplace ecosystem," in *24th USENIX Security Symposium, USENIX Security 15, Washington, D.C., USA, August 12-14, 2015*, J. Jung and T. Holz, Eds. USENIX Association, 2015, pp. 33–48. [Online]. Available: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/soska

[3] J. Cox, "Staying in the shadows: the use of bitcoin and encryption in cryptomarkets," *The Internet and drug markets*, pp. 41–48, 2016.

[4] R. van Wegberg, F. Miedema, U. Akyazi, A. Noroozian, B. Klievink, and M. van Eeten, "Go see a specialist? predicting cybercrime sales on online anonymous markets from vendor and product characteristics," in *WWW '20: The Web Conference 2020, Taipei, Taiwan, April 20-24, 2020*, Y. Huang, I. King, T. Liu, and M. van Steen, Eds. ACM / IW3C2, 2020, pp. 816–826. [Online]. Available: https://doi.org/10.1145/3366423.3380162

[5] R. van Wegberg and T. Verburgh, "Lost in the dream? measuring the effects of operation bayonet on vendors migrating to dream market," in *Proceedings of the Evolution of the Darknet Workshop*, 2018, pp. 1–5.

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

[7] R. van Wegberg, S. Tajalizadehkhoob, K. Soska, U. Akyazi, C. H. Gañán, B. Klievink, N. Christin, and M. van Eeten, "Plug and prey? measuring the commoditization of cybercrime via online anonymous markets," in *27th USENIX Security Symposium, USENIX Security 2018, Baltimore, MD, USA, August 15-17, 2018*, W. Enck and A. P. Felt, Eds. USENIX Association, 2018, pp. 1009–1026. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/van-wegberg

[8] T. Verburgh, E. Smits, and R. van Wegberg, "Uit de schaduw," *Justitiele Verkenningen*, vol. 44, no. 5, 2018.

[9] M. C. Van Hout and T. Bingham, "'surfing the silk road': A study of users' experiences," *International Journal of Drug Policy*, vol. 24, no. 6, pp. 524–529, 2013.

[10] W. Przepiorka, L. Norbutas, and R. Corten, "Order without law: Reputation promotes cooperation in a cryptomarket for illegal drugs," *European Sociological Review*, vol. 33, no. 6, pp. 752–764, 2017.

[11] J. Mounteney, A. Oteo, and P. Griffiths, "The internet and drug markets: Shining a light on these complex and dynamic systems," *The Internet and drug markets*, pp. 127–133, 2016.

[12] M. Tzanetakis, G. Kamphausen, B. Werse, and R. von Laufenberg, "The transparency paradox. building trust, resolving disputes and optimising logistics on conventional and online drugs markets," *International Journal of Drug Policy*, vol. 35, pp. 58–68, 2016.

[13] D. Décary-Hétu and B. Dupont, "Reputation in a dark network of online criminals," *Global Crime*, vol. 14, no. 2-3, pp. 175–196, 2013.

[14] D. Décary-Hétu and O. Quessy-Doré, "Are repeat buyers in cryptomarkets loyal customers? repeat business between dyads of cryptomarket vendors and users," *American Behavioral Scientist*, vol. 61, no. 11, pp. 1341–1357, 2017.

[15] D. Décary-Hétu and L. Giommoni, "Do police crackdowns disrupt drug cryptomarkets? a longitudinal analysis of the effects of operation onymous," *Crime, Law and Social Change*, vol. 67, no. 1, pp. 55–75, 2017.

[16] L. Norbutas, S. Ruiter, and R. Corten, "Reputation transferability across contexts: Maintaining cooperation among anonymous cryptomarket actors when moving between markets," *International Journal of Drug Policy*, vol. 76, p. 102635, 2020.

[17] A. Afilipoaie and P. Shortis, "From dealer to doorstep–how drugs are sold on the dark net," *GDPO Situation Analysis. Swansea University: Global Drugs Policy Observatory*, 2015.

[18] M. Paquet-Clouston, D. Décary-Hétu, and C. Morselli, "Assessing market competition and vendors' size and scope on alphabay," *International Journal of Drug Policy*, vol. 54, pp. 87–98, 2018.

[19] N. Christin, "Traveling the silk road: A measurement analysis of a large anonymous online marketplace," *CoRR*, vol. abs/1207.7139, 2012. [Online]. Available: http://arxiv.org/abs/1207.7139

[20] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer, "RFC 4880 - OpenPGP Message Format ," 2007, https://tools.ietf.org/html/rfc4880.

[21] M. Green, "Pretty Good Privacy for Python," 2020. [Online]. Available: https://github.com/SecurityInnovation/PGPy

[22] G. Branwen, N. Christin, D. Décary-Hétu, R. M. Andersen, StExo, E. Presidente, Anonymous, D. Lau, D. K. Sohhlz, V. Cakic, V. Buskirk, Whom, M. McKenna, and S. Goode, "Dark net market archives, 2011-2015," July 2015, accessed: 2020-11-01. [Online]. Available: https://www.gwern.net/DNM-archives

[23] G. M. Campedelli, F. Calderoni, T. Comunale, and C. Meneghini, "Life-course criminal trajectories of mafia members," *Crime & Delinquency*, p. 0011128719860834, 2019.

[24] N. Deslauriers-Varin and E. Beauregard, "Victims' routine activities and sex offenders' target selection scripts: A latent class analysis," *Sexual Abuse*, vol. 22, no. 3, pp. 315–342, 2010.

[25] B. H. Fox and D. P. Farrington, "Creating burglary profiles using latent class analysis: A new approach to offender profiling," *Criminal Justice and Behavior*, vol. 39, no. 12, pp. 1582–1611, 2012.

[26] M. G. Vaughn, M. DeLisi, K. M. Beaver, and M. O. Howard, "Toward a quantitative typology of burglars: A latent profile analysis of career offenders," *Journal of Forensic Sciences*, vol. 53, no. 6, pp. 1387–1392, 2008.

[27] M. G. Vaughn, M. DeLisi, K. M. Beaver, and M. O. Howard, "Multiple murder and criminal careers: A latent class analysis of multiple homicide offenders," *Forensic Science International*, vol. 183, no. 1-3, pp. 67–73, 2009.

[28] W. G. Jennings and C. Meade, "Group-based trajectory modeling," *Oxford handbooks online in criminology and criminal justice*, pp. 183–198, 2016.

[29] K. P. Burnham and D. R. Anderson, "Multimodel inference: understanding AIC and BIC in model selection," *Sociological methods & research*, vol. 33, no. 2, pp. 261–304, 2004.

[30] J. D. Nielsen, J. S. Rosenthal, Y. Sun, D. M. Day, I. Bevc, and T. Duchesne, "Group-based criminal trajectory analysis using cross-validation criteria," *Communications in Statistics-Theory and Methods*, vol. 43, no. 20, pp. 4337–4356, 2014.

[31] E. P. Shulman, L. D. Steinberg, and A. R. Piquero, "The age–crime curve in adolescence and early adulthood is not due to age differences in economic status," *Journal of Youth and Adolescence*, vol. 42, no. 6, pp. 848–860, 2013.

[32] S. Glueck and E. Glueck, "Later criminal careers," *Commonwealth fund*, 1937.

[33] E. L. Kaplan and P. Meier, "Nonparametric estimation from incomplete observations," *Journal of the American statistical association*, vol. 53, no. 282, pp. 457–481, 1958.

[34] IOCTA, "Internet organised crime threat assessment (iocta) 2019," *Europol*, October 2019. [Online]. Available: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

[35] D. P. Farrington, "Age and crime," *Crime and justice*, vol. 7, pp. 189–250, 1986.

[36] M. V. Van Koppen, C. J. De Poot, E. R. Kleemans, and P. Nieuwbeerta, "Criminal trajectories in organized crime," *The British Journal of Criminology*, vol. 50, no. 1, pp. 102–123, 2010.

[37] J. Aldridge and D. Decary-Hetu, "Not an 'Ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation," *SSRN Electronic Journal*, vol. 564, no. October, 2014. [Online]. Available: http://www.ssrn.com/abstract=2436643http://papers.ssrn.com/abstract=2436643

[38] J. Aldridge and D. Décary-Hétu, "Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets," *International Journal of Drug Policy*, 2016.

[39] D. Décary-Hétu and L. Giommoni, "Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous," *Crime, Law and Social Change*, vol. 67, no. 1, pp. 55–75, feb 2017. [Online]. Available: http://dx.doi.org/10.1007/s10611-016-9644-4http://link.springer.com/10.1007/s10611-016-9644-4

[40] K. Kruithof, J. Aldridge, D. Décary-Hétu, M. Sim, E. Dujso, and S. Hoorens, "Internet-facilitated drugs trade," *RAND Corporation*, vol. 2016, pp. 21–32, 2016.

[41] D. Décary-Hétu and A. Leppänen, "Criminals and signals: An assessment of criminal performance in the carding underworld," *Security Journal*, vol. 29, no. 3, pp. 442–460, 2016.

[42] T. J. Holt, O. Smirnova, and A. Hutchings, "Examining signals of trust in criminal markets online," *Journal of Cybersecurity*, 2016.