BAYES BUSINESS SCHOOL

MASTERS THESIS

The effects of cybersecurity campaigns on the darknet

Author: Yong Shih, Leong

Supervisor: Simone Santoni

This report is submitted as part of the requirements for the award of the MSc in Business Analytics

September, 2022

BAYES BUSINESS SCHOOL

Abstract

Business Analytics

The effects of cybersecurity campaigns on the darknet

by Yong Shih, Leong

The topic of this study is the effects of cybersecurity campaigns on darknet markets. This study was achieved using the Gwern Branwen dataset with a focus on Operation Onymous and the 14 dark net markets and forums. Time-series plots, topic modelling and sentiment analysis were carried out using Python as the main programming language. Following the study, the main conclusion was that cybersecurity campaigns are not effective in lowering activity in the darknet market for more than 2 weeks. Within a month, activity levels and size of darknet markets would reach to peaks higher than before the intervention. Some levels of innovation and competitiveness can also be seen in the dark net markets after the intervention.

Acknowledgements

Firstly, I could not have done this research without the help of my teammates Benedict Zhou and Terry Tang. I'm also extremely grateful to our lecturer Simone Santoni for all the guidance given within and outside the scope of this project.

Secondly, words cannot express my gratitude to my family and my girlfriend. Their trust and beliefs in me has kept me motivated throughout my time in Bayes Business School and this research project.

Lastly, I'd like to acknowledge the 2021-22 Business Analytics cohort members that have supported me throughout my Masters at Bayes Business School.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivations and objectives of the study

The Dark Net Markets (DNM) are online anonymous platforms that allow the trade of mainly illegal goods. The main product sold in these markets are drugs (Christin, 2012). Other items such as weapons, counterfeit items, credit card information and hacking services could be found on those platforms. They connect buyers and sellers worldwide and the main currency traded on the platform is cryptocurrencies such as Bitcoin (Bradley, 2019).

The most famous and first successful online DNM is Silk Road which opened in February 2011 (Soska & Christin, 2015). As estimated by Soska & Christin (2015), Silk Road's sales volumes can reach up to $650,000 a day but generally stay around the $300,000 to $500,000 mark. It was claimed that the owner Ross Ulbricht was making $20,000 a day in commissions and has amassed a total of $80 million (Olson, 2013). In October 2013, Silk Road market was taken down by law enforcement due to its high profile nature (Rushe 2014; BBC, 2015). Soon after its take-down, some buyers and sellers moved to ex-competitors such as Sheep Marketplace and Black Market Reloaded while others started their own marketplaces such as "Silk Road 2.0" which came online a month after Silk Road's closure (Soska & Christin, 2015). During Ross Ulbricht's sentencing, the judge expressed that his sentence would show copycats of the consequences of hosting DNMs (BBC, 2015; Olson, 2013).

As technology is constantly improving, participants in the illegal markets will use this to their advantage to evade law enforcers. Therefore understanding questions such as "Do cybersecurity campaigns effectively lower illegal activities in the DNM ecosystem?" and "Do cybersecurity campaigns foster innovation and competition?" is key in tackling these DNMs. A number of explanatory data analysis is employed to determine the best campaign and market to study. In addition to that, time-series plots as well as topic modelling and sentiment analysis would be carried out. The following chapters will consist of literature review, data and methods, analysis and results, discussion of results and finally the conclusion.

Chapter 2

Literature Review

2.1 Literature review

The research area of whether cybersecurity campaigns effectively shut down DNMs and its vendors has been a hot topic over the recent years as law enforcement and policy makers are trying to be a step ahead of emerging DNMs.

2.1.1 Effects of enforcement on traditional drug markets

Although the crackdown on DNMs is fairly new with the first publicised takedown in 2013 when police arrested Ross Ulbricht for hosting Silk Road (BBC, 2015). We can take a look at police crackdowns on the traditional drug market as a framework on how to assess the effectiveness of drug enforcement strategies and understand how the DNM ecosystem is affected. Early studies by Reuter and Kleinman (1986) associate price as an indicator of effectiveness in drug enforcement strategies. Price is determined by both demand and supply, in this case can both be targeted by law enforcement to lower consumption and ultimately supply of drugs.

Demand control programs tackle the issue by reducing the consumption of drugs on a user level. These programs can take the form of educating people on the dangers of drugs in school. More importantly, supply side programs affect the consumption of drugs by directly targeting the ease of access to these illicit drugs (Decary-Hetu & Giommoni, 2017). One type of supply side disruptions is crackdowns on marketplaces or geographical areas. However Mazerolle et al. (2006) found that a one-size-fits-all police crackdown is not as effective as reducing drug problems than community or multi-agency partnerships. Although crackdowns are effective at seizing the drugs and drug runners, there are very little evidence to show that these crackdowns have any significant influence on the drug user or supplier in the long run (Kerr et al., 2005; Decary-Hetu & Giommoni, 2017; Wood et al., 2004). If any, the impact is short term and market participants adapt quickly by displacement techniques.

One such displacement technique is tactical displacement. As a result of risk of law enforcements, markets would turn from “open” to “closed” even if options of drugs are lesser for buyers and a limited access to the number of buyers for the sellers (Edmunds et al., 1996).

2.1.2 Darknet Markets (DNM)

As seen from the effects of enforcement on traditional drug markets, one of the major disadvantages is that there are high risks in participating within the market. If participants do take part, it is within a "closed" setting. The invention of cryptomarkets or DNM revolutionised the trade of drugs and other illegal items. Allowing the trade of drugs in the best available setting for both buyer and seller. A combination of technologies allows for a high level of anonymity. Firstly, the IP addresses of both the host of the market and the participants are hidden through the use of the Onion Router (Tor) network. Secondly, participants trade in cryptocurrency such as Bitcoin which further hides their identity as these digital currencies cannot be traced or identified. This allows for the trade of illegal substances and services within a "closed" market setting without having the disadvantages of options of drugs or a limited access to buyers.

To date, there are only a few known police operations that have targeted the DNM. Two of the more well known operations are Marco Polo and Onymous which were executed in October 2013 and November 2014 respectively (Heindenreich & Westbrooks, 2017; Europol, n.d.). Operation Marco Polo was targeted at taking down the DNM "Silk Road", which led to 173,991 bitcoins being seized which is worth $33.6 million at the time of writing of the article (FBI, 2013). Following operation Marco Polo many of the participants moved to other DNMs such as Agora, Evolution, Diabolus and Silk Road 2 to name a few. However, just after a short period of time, agencies from Europol, the FBI, ICE, HIS and Eurojust launched another operation which led to the arrest of 17 administrators and vendors (Europol, n.d.).

2.1.3 Effects of enforcement on DNMs

Taking a closer look at Operations Marco Polo and Onymous tells us a clearer picture of the effects of enforcement on the DNMs. Following Operation Marco Polo, there was a 100% and 460% increase of vendors in other DNMs such as Black Market Reloaded (BMR) and Sheep Marketplace over a 6-week period respectively (Buskirk et al., 2014). The closure of Silk Road did not deter participants from re-entering into other DNMs or lead participants to lose confidence in the technologies that shroud their identities. A similar picture can be painted when taking a look at Operation Onymous. Soska and Christin (2015) found that the DNM ecosystem is quite resilient to takedowns as aggregate sales volumes were back to more than half of what they were within a few weeks after the operation.

One of the more interesting aspects of the effects of enforcement on DNMs are the technological innovations that take place after the operation. There is research to suggest that these operations incentivise innovation within the DNM (Buxton & Bingham, 2015; Buskirk et al., 2014). Two factor authentication features as well as clever marketing campaigns for communicating with buyers started to take place in these DNMs as a result of Operation Marco Polo. Buxton and Bingham (2015) reports that in light of Operation Onymous, new decentralised markets (Open Bazaar & Dark Market) started gaining its popularity. Decentralised markets are one of the innovations that emerged in a response to the operations. These decentralised markets are

not controlled by any single entity, which means there aren't any fees. Another innovation that can be seen as a result is Grams, it was termed the Google of the DNM (Stone, 2017). This was the first of its kind, a search engine that could compare prices and reviews of DNMs.

2.1.4 Data

As there aren't many ways of collecting data for DNMs, all of the studies that have used data from the DNM have directly scraped from the Dark Net (Soska & Christin, 2015; Christin, 2012; Aldridge & Decary-Hetu, 2015; Decary-Hetu & Giommoni, 2016; Bradley, 2019). Some papers implemented their own scraping frameworks when these DNMs were still online (Soska & Christin, 2015; Christin, 2012; Aldridge & Decary-Hetu, 2015). Meanwhile other studies relied on using the dataset collected by Gwern Branwen (Decary-Hetu & Giommoni, 2016; Bradley, 2019). The dataset consists of snapshots of 89 DNMs through a period of 2013-2015 (Branwen et al., n.d.). As the dataset is only a daily or weekly snapshot, it may not contain every single item and vendor information. Bradley (2019) also pointed that the scrapes were not done on regular intervals across all markets hence there may be time discrepancies between different markets. The Gwern dataset is also severely restricted and any conclusion made from the analysis must be made cautiously. Tedious work to clean and pre-process the data must also be done prior to any analysis as the data comes from different DNMs which all have different layouts and different storage of data.

Chapter 3

Data and Methods

3.1 Gwern Branwen Dataset

The dataset that we have chosen to analyse comes from the Gwern Branwen dataset it was scraped on a weekly or daily basis throughout 2013-2015. This large dataset consists of 89 DNMs and 37+ related forums which the file size is about 1.6TB uncompressed (Branwen et al. 2015). As seen from previous literature, this dataset has a few issues of its own. Mainly the information stored is not in consistent intervals hence there might be some missing data. Next, there may be differences in the layouts of each DNM. In the upcoming subsections, the information that will be extracted and the methods as to how these issues are overcome are laid out below.

3.1.1 Extracted information: Markets

Information	Description
Item	Name of the item
Item category	Category of the item
Price	Price of the item
Price unit	Unit of the price (eg. Dollar, Bitcoin)
Vendor of the item	Name of the vendor
Description	A short description of the item
Image	Image of the item (image path)
The from location of the item	Where the item will be delivered from
The to location of the item	Where the item can be delivered to
Feedback	Feedback of the item and/or vendor below the item description
Username	The username who wrote the feedback
Date	The date of the feedback
Feedback rating	The rating of the feedback out of a certain number

TABLE 3.1: Information that would be extracted from each DNM

3.1.2 Extracted information: Forums

Information	Description
Topic	The main topic of the post
Post timestamp	The date the post was created
Content of post	The content category of the post
Author	The username that created the post
Reply username	The username that replies
Reply content	The content of the reply
Reply timestamp	The time the reply was made

TABLE 3.2: Information that would be extracted from each darknet forum

Tables 3.1 and 3.2 shows the information that will be extracted from the darknet markets and forums. There are 13 variables that will be extracted from the DNM while 7 variables for the darknet forums to be analysed. Appendix A displays the structure in which the data has been collected and saved in a json file.

3.1.3 Issues

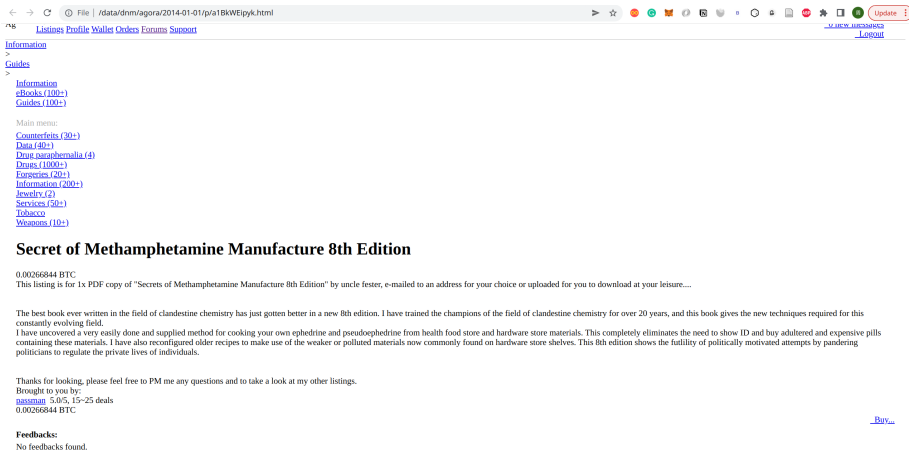

FIGURE 3.1: Agora landing page 2014

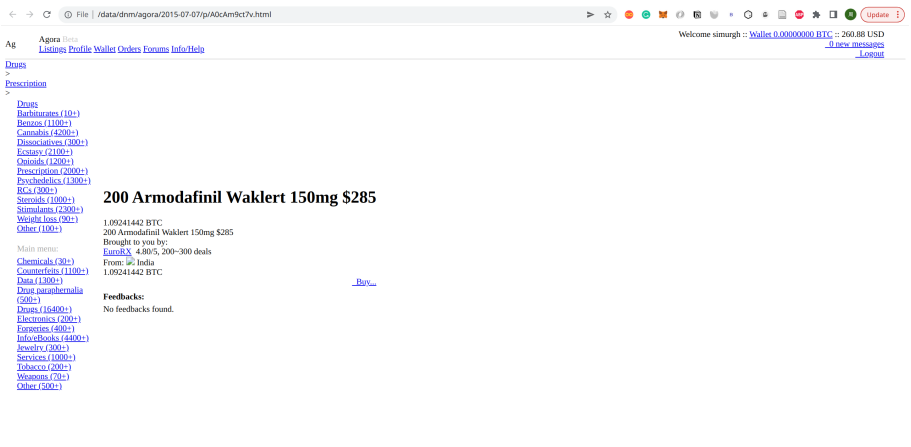

FIGURE 3.2: Agora landing page 2015

As these DNMs are ever changing, a common theme or pattern must be found for each element along all the markets. Figures 3.1 and 3.2 shows how the *Agora* DNM has changed over a year, there are more information and categories in 2015 than there was in 2014. Firstly, to extract the elements that we want, we use *CSS* to extract information that we want. We also use a 'Regular expression' also known as *regex* to extract information that has a specific pattern. A combination of these methods are sometimes deployed to obtain clean data. An example is shown below as to how these two methods can be used to extract the price out of an object.

```
price = soup.find('div', class_='col-sm-4 col-lg-4 text-right')
number = float(re.search(r'\d+.?\d+', price.text).group(0))
```

3.1.4 Parser

The following unified modeling language (UML) of figure 3.3 below lays out clearly the forum, item and vendor parser as well as the file type of each information and the markets and forums that will be targeted for this research based on the reasoning's of section 3.2 and table 3.4 below. To avoid the issue of re-running the parser everytime it is interrupted, data is temporarily stored in a *tmp* file. This saves time as the program can continue to run from where it last got interrupted from.

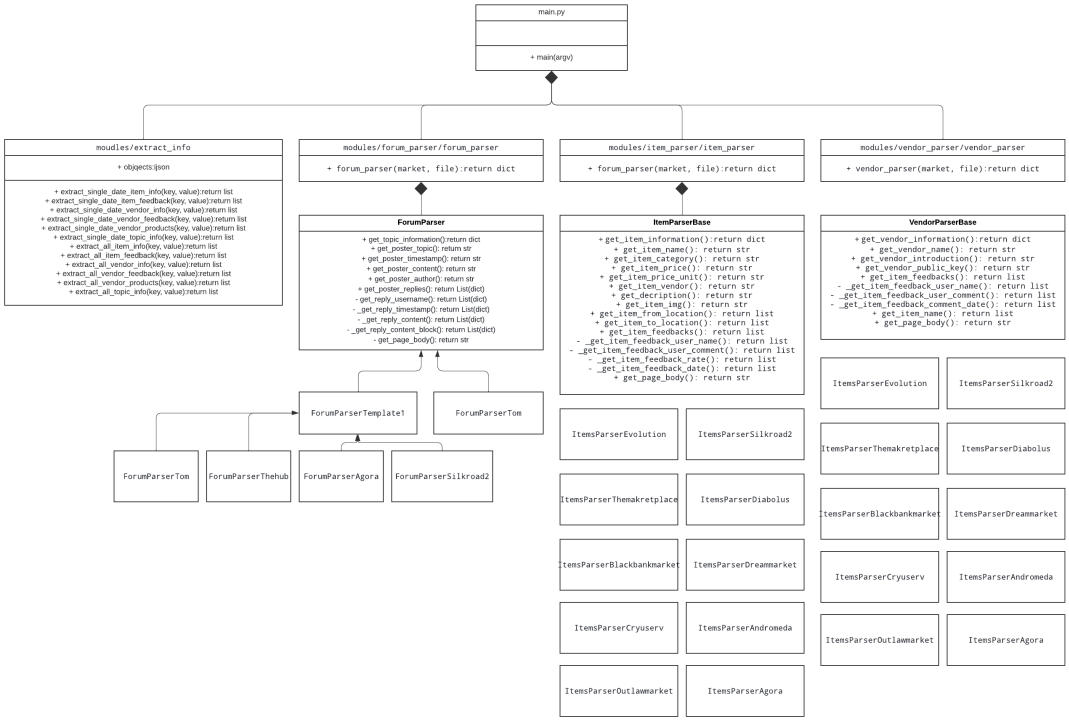

FIGURE 3.3: UML diagram

3.2 Explaratory Data Analysis

After cleaning and pre-processing, we produce some plots for explanatory data analysis (EDA). This would give us a clearer picture on what markets and operations we should focus on based on the facts of the EDA. Below we will have 2 figures that will lead us to conclude our findings on which combinations of operations and markets would best fit the study.

3.2.1 Influence of campaigns on markets

Figure 3.4 shows the influence of campaigns on the different DNMs. This graph was produced solely based on the timeline of operations as well length of DNMs operating. On the x-axis we have years of operation and y-axis the names of the individual DNMs. A pink rectangle covers the time taken for each operation while a blue bar chart shows the time from when a DNM goes online till it is taken down either by law enforcement, exit scams or simply a closure by its administrators. At first glance, we can see that the only operation that does not have any overlaps with other operations is Marco Polo which shut down Silk Road 1.0. This indicates that there will be difficulty in analysing the impact of each operation on different DNMs as there are many timeline overlaps for the campaigns. Operation Commodore and Onymous have the shortest campaign times but seems to be highly effective in shutting down DNMs as there are a number of markets that stopped operating after the campaign has ended. The length of these operations can be found in appendix B

3.2.2 Accumulative market change

To take a closer look, we use the size of the folder as a proxy to size of each market. This method would allow us to measure the size of change of each market over a time period. Figure 3.5 shows the cumulative size change of each market during each operation while table 3.3 shows the different scenarios that could take place.

Scenarios	Description	Accumulative change
1	The duration of the market doesn't overlap with the campaign	0%
2	The duration of market is totally in the campaign period	-100%
3	The market started before the campaign but ended during the campaign duration	-100%
4	The market started before the campaign but ended after the campaign duration	Change of the first data after the end of the campaign and the last data before the start of the campaign
5	The market started during the campaign but ended after the campaign duration	Change of the first data after the end of the campaign and the first market size

TABLE 3.3: Different scenarios of time overlap between campaign and darknet markets/forums

On the right of the matrix in figure 3.5, we have a colour gradient to indicate the accumulative change of size of market (file size). On the opposite sides of the spectrum, we have a grey cell which indicates a change of up to -100% (0 in the colour spectrum), indicating the closure of a market (scenarios 2 or 3). While a darker orange or red indicates a change of up to 100% (<1.0 in the colour spectrum) indicating the emergence or growth of a market (scenarios 4 or 5). A light orange indicates that the operation does not affect the campaign (0% change or =1 in the colour spectrum, scenario 1).

We can see that operations Shrouded Horizon, Babylon and Darknode has a number of grey cells which indicate that these operations are not useful in our study as it would be difficult to link the DNMs closure to the impact of the operation. This would be the same for operations Marco Polo and Hyperion as they only consist of light orange cells and thus these operations have no effect on a large account of the DNM. Lastly, we have operation Onymous, Commodore and Pacifier of which Operation Pacifier has the least DNM closures (2 closures) than Onymous and Commodore (6 closures each). These two operations (Onymous & Commodore) are the best options to research as they provide adequate evidence to prove the research question. However, due to the time constraint of this research it was decided that Operation Onymous was a better candidate for the research as there was more information available online than its counterpart.

3.2.3 Chosen market sample

As discussed earlier, Operation Onymous is the best operation to be studied for the purposes of this research. It affected 17 different dark net markets and forums of which we study 14 of them (7 markets and 7 forums) and is summarised in table 3.2.4 below. The markets that were dropped are *Andromeda*, *Cryuserv* and *Outlawmarket*. The main reason of dropping these markets (*Andromeda*) is that they have incomplete data which would lead to inaccurate conclusions. Specifically, *Cryuserv* and *Outlawmarket* has incompatible file system (*ngix file type*) and

ddos protection on some profiles respectively. The selected 14 markets are listed in table 3.4 below while the full market and forum list that Operation Onymous affected is listed in appendix C.

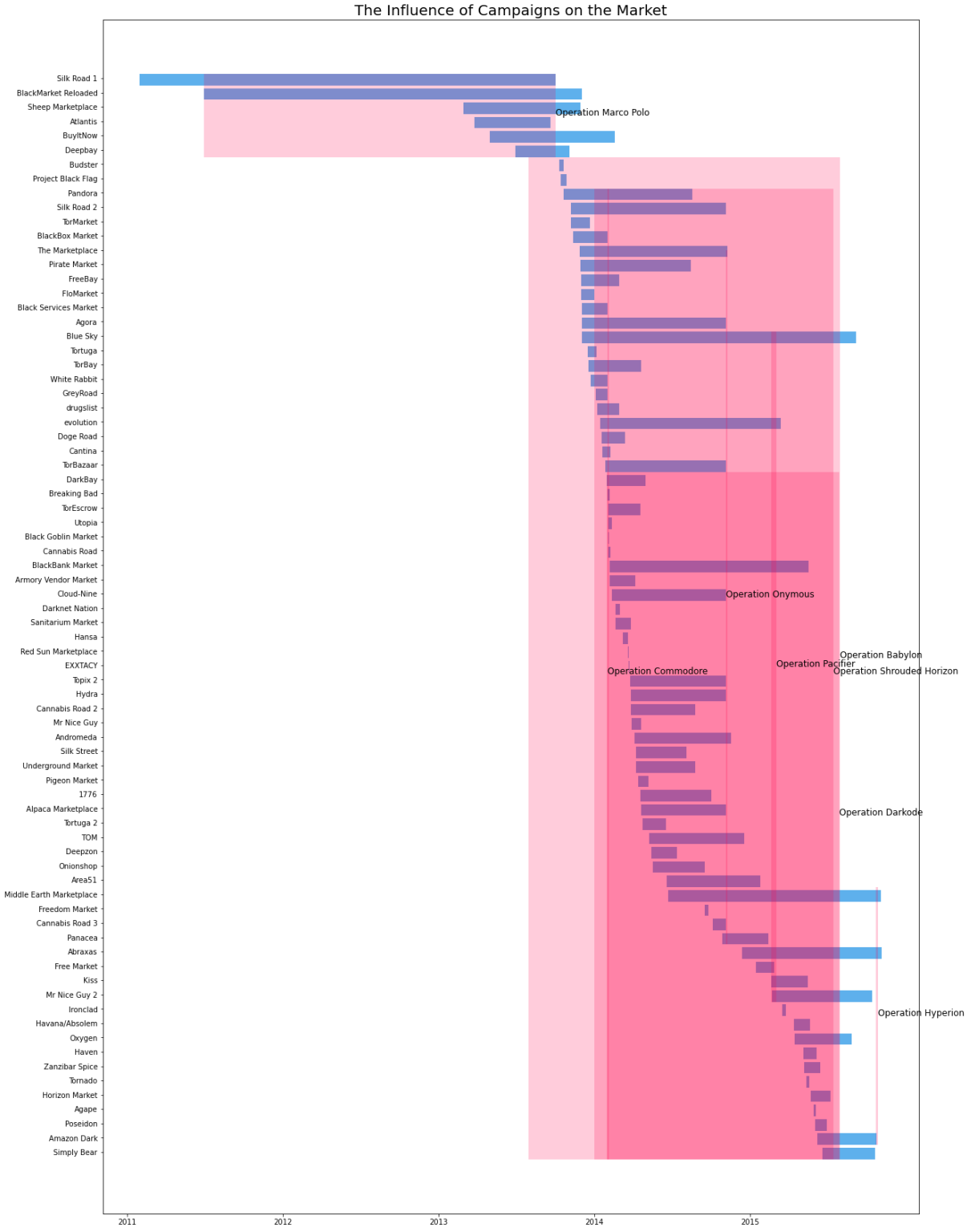

FIGURE 3.4: Influence of campaigns on each market

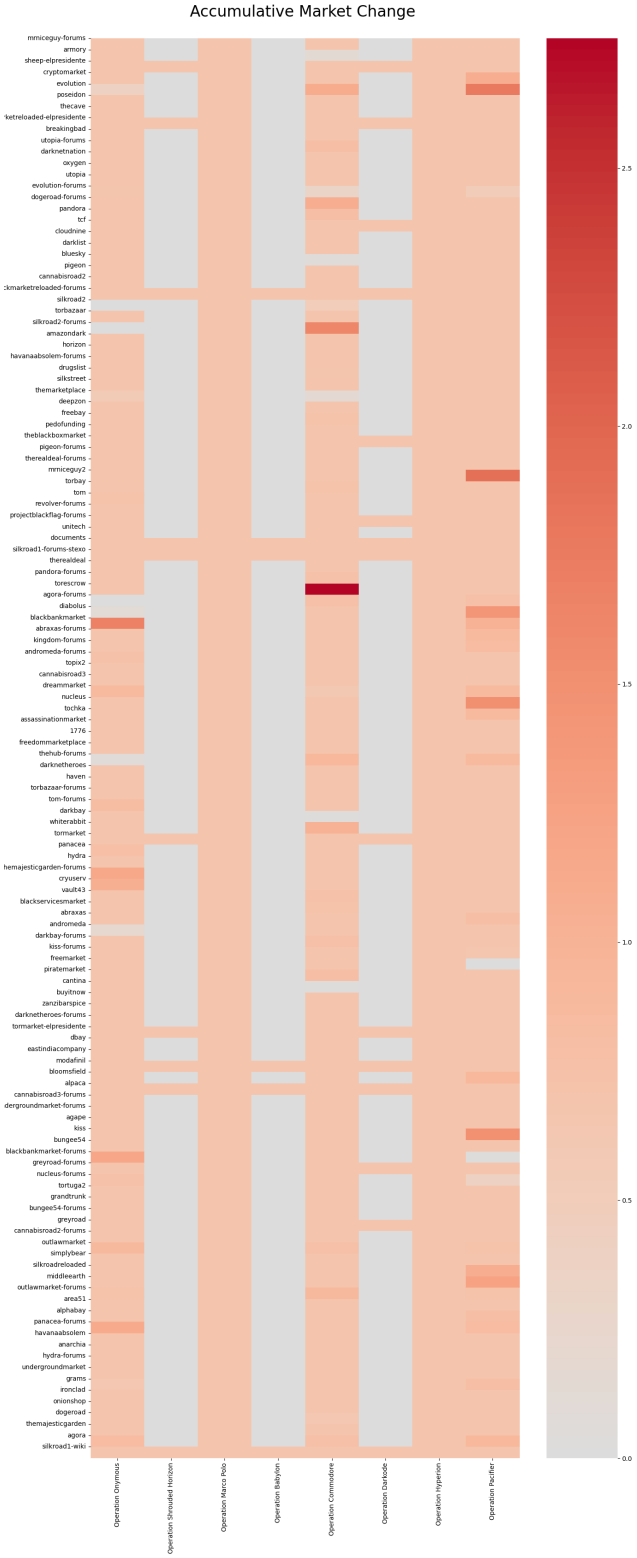

FIGURE 3.5: Accumulative market change

Darknet market	Type
Agora	Market
Blackbankmarket	Market
Dreammarket	Market
Diabolus	Market
Evolution	Market
Silkroad2	Market
Themarketplace	Market
Agora-forums	Forum
Blackbankmarket-forums	Forum
Panacea-forums	Forum
Silkroad2-forums	Forum
Thehub-forums	Forum
themajesticgarden-forums	Forum
tom-forums	Forum

TABLE 3.4: Summary of darknet markets and forums that were chosen

Chapter 4

Analysis and results

4.1 Market Analysis

Four EDA will be carried out in the following sections which are regarding the overall DNM, feedback, forum and transactional data. By looking at these EDA it will give us an idea of the influence of Operation Onymous leading up to and after the campaign on each of the DNMs that were taken down.

4.1.1 Items trend

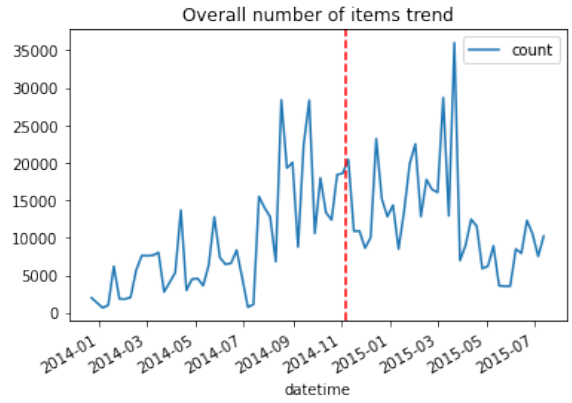

FIGURE 4.1: Overall items trend

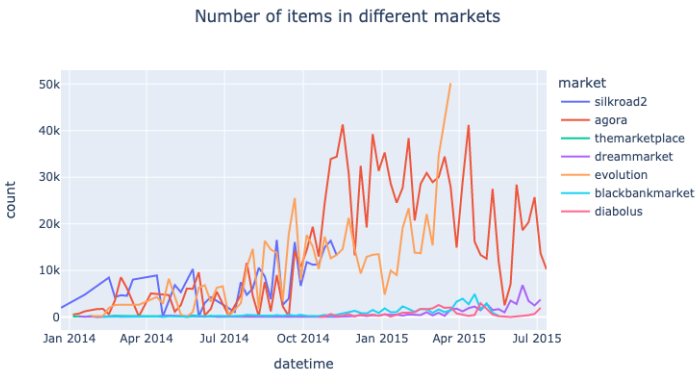

FIGURE 4.2: Items trend on specific markets

Figures 4.1 and 4.2 are time series graph that show the overall average number of items over a 1.5 year period. The red dotted line shown in figure 4.1 is where Operation Onymous was carried out. We can see overall in the market there was a significant drop in the overall average number of items from 20,000 to 10,000 about a 50% decline in less than 3 months. Taking a closer look at the number of items in specific DNM, *Agora* and *Evolution* both had a decline when *Silkroad2* was shut although *Evolution's* decline was later than *Agoras*.

4.1.2 Vendors trend

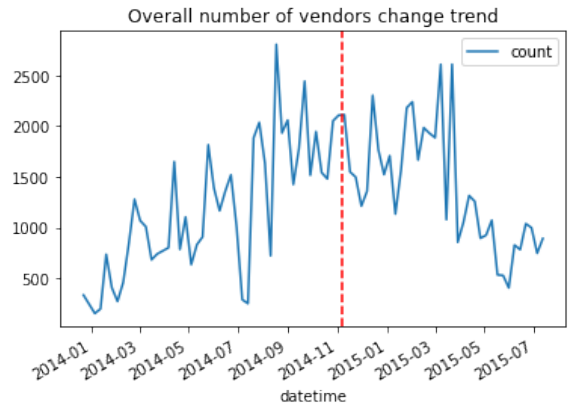

FIGURE 4.3: Overall vendors trend

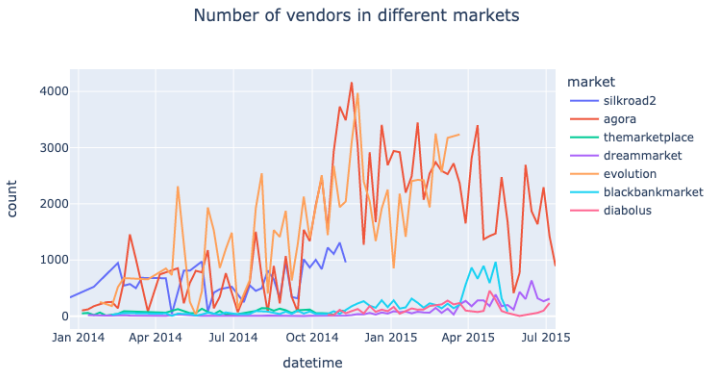

FIGURE 4.4: Vendors trend on specific markets

Similar to the item trends section above, figures 4.3 and 4.4 are time series graph that show the overall average number of vendors and a comparison within different markets. Figure 4.3 has a similar trajectory to that of the items trend whereby immediately after the take-down of *Silkroad2* a significant portion of vendors exit the market. Within a month these vendors re-enter the market, but there is an even higher peak than before Operation Onymous. The DNM comparison in figure 4.4 displays a decrease in number of vendors for the two largest markets after the closure of *Silkroad2*. Looking closer at the other markets, we can see a disturbance in the ecosystem as the number of vendors in markets such as *blackbankmarket*, *diabolus* and *dreammarket* become volatile.

4.1.3 Correlation matrix between markets

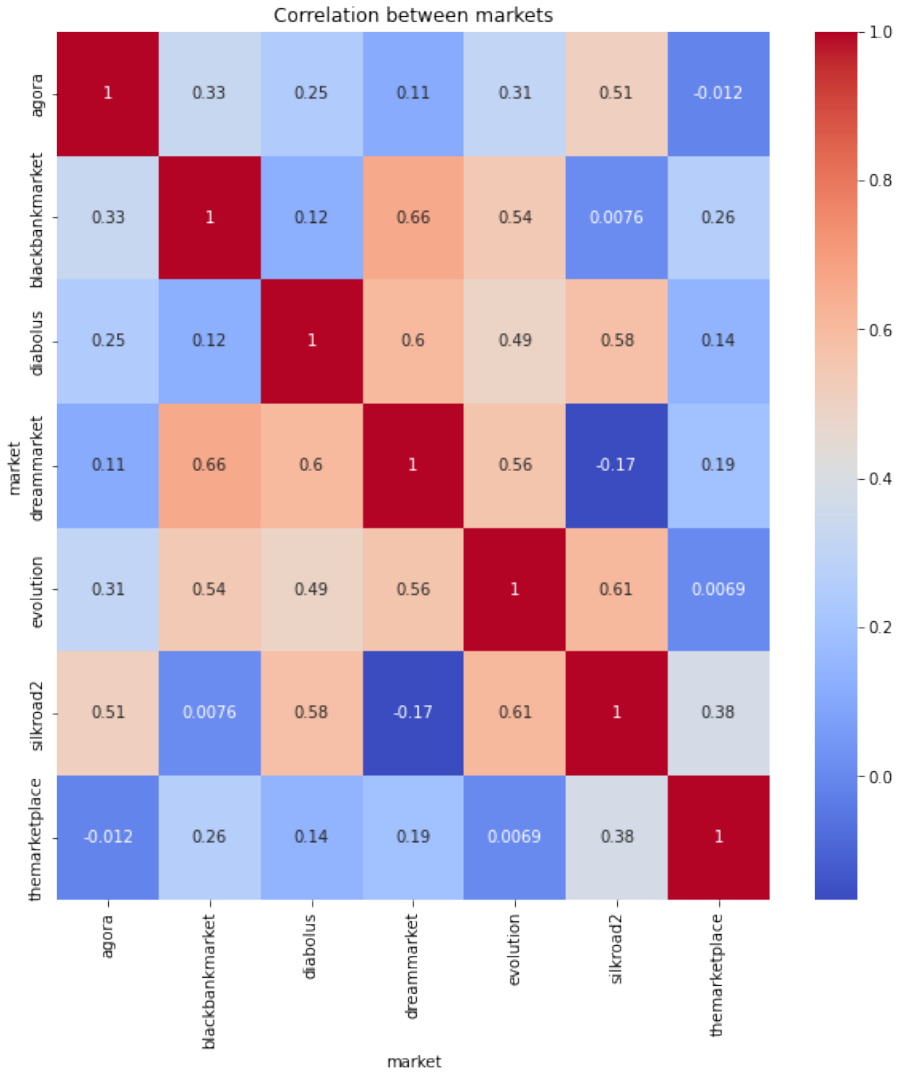

FIGURE 4.5: Correlation matrix of markets (items in markets)

Figure 4.5 above shows the correlations between the number of items in markets that were affected by Operation Onymous. The DNMs which has the highest correlation is *dreammarket* and *blackbankmarket* followed by *silkroad2* and *evolution* with correlation scores of 0.66 and 0.61 respectively. The DNM with little to no correlations are *themarketplace* and *evolution* as well as *silkroad2* and *blackbankmarket* at 0.0069 and 0.0076 respectively.

4.1.4 Categories trend

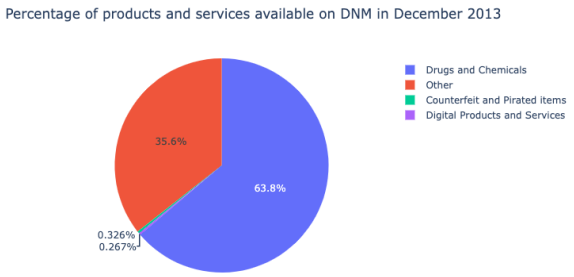

FIGURE 4.6: Percentage of products and services in December 2013

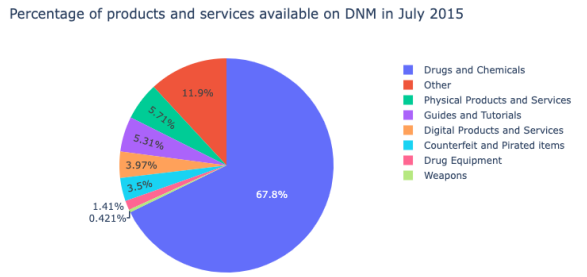

FIGURE 4.7: Percentage of products and services in July 2015

Taking a look at figure 4.6 and 4.7 we can clearly see that the category *drugs and chemicals* dominate the DNMs at over 60% in both 2013 and 2015. Taking a look at the difference in categories between early and later stages of the DNM we can see that more categories have emerged in later years. The emergence of new categories may be due to the DNM diversifying as more participants and vendors enter the market.

4.1.5 Overall market size change over time by item count

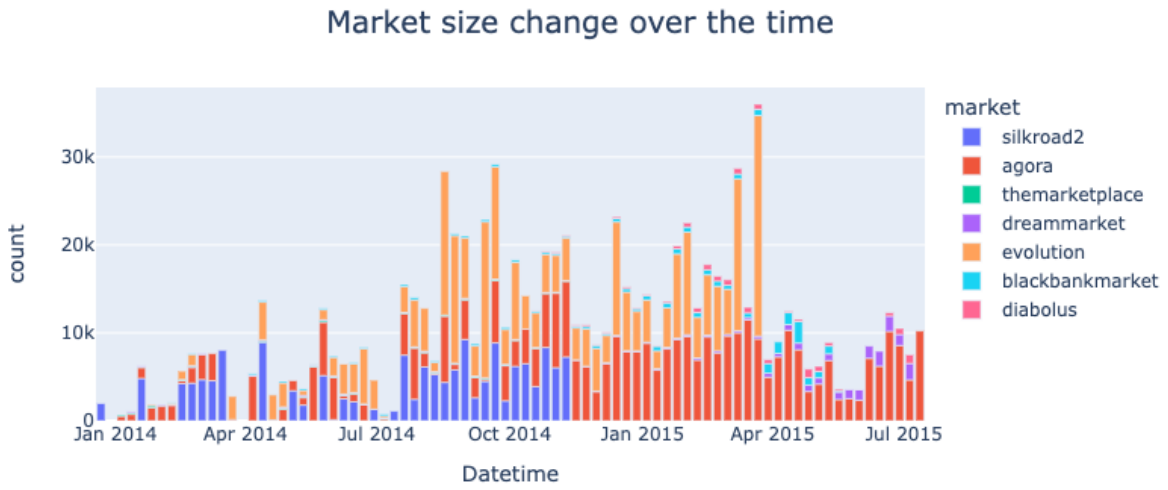

FIGURE 4.8: Overall size of specific DNM over time

A stacked bar chart is plotted to visualise the change in size of market over time, in this case size of market is determined as the number of items in each market. We can clearly see where Operation Onymous took place when the blue bar of *Silkroad2* is erased from figure 4.8. We

can also see a significant increase in market size of the DNM *Evolution*, a few weeks after Operation Onymous. It can also be noted that at the peak of *Evolution* was in early 2015, when the DNM was at its largest market size before it closed down. *Agora* although not by much has also seemed to grow in market size following the operation. Meanwhile the other DNMs stayed relatively similar in size before and after the operation.

4.1.6 Category comparison by darknet markets

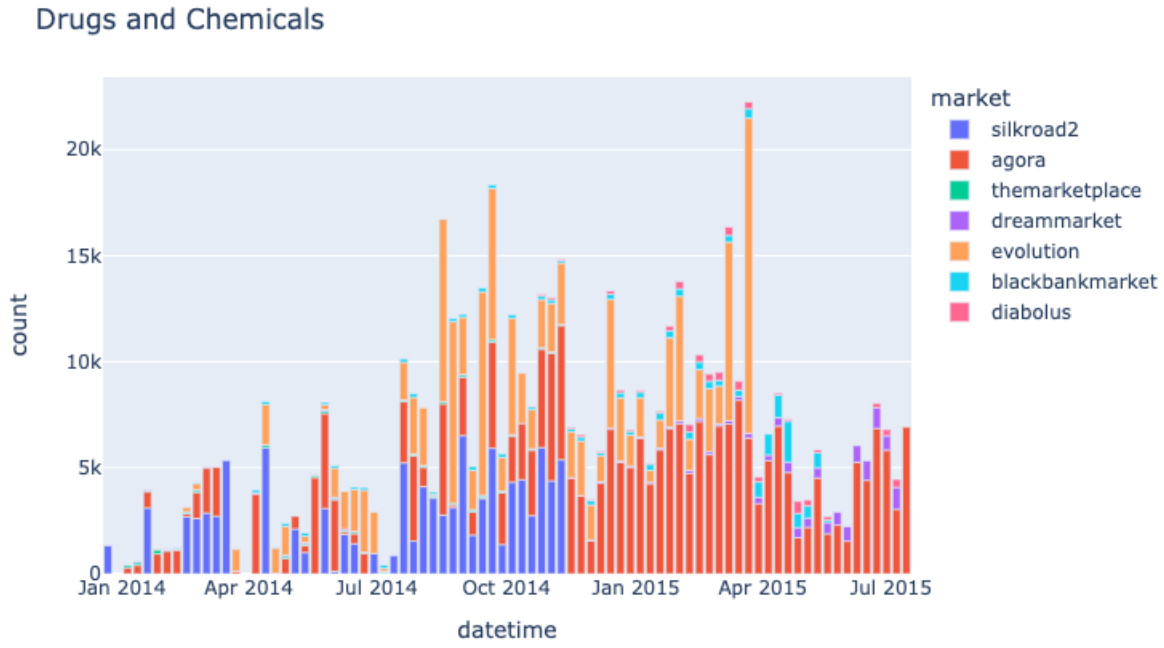

FIGURE 4.9: Drug and chemicals count over time

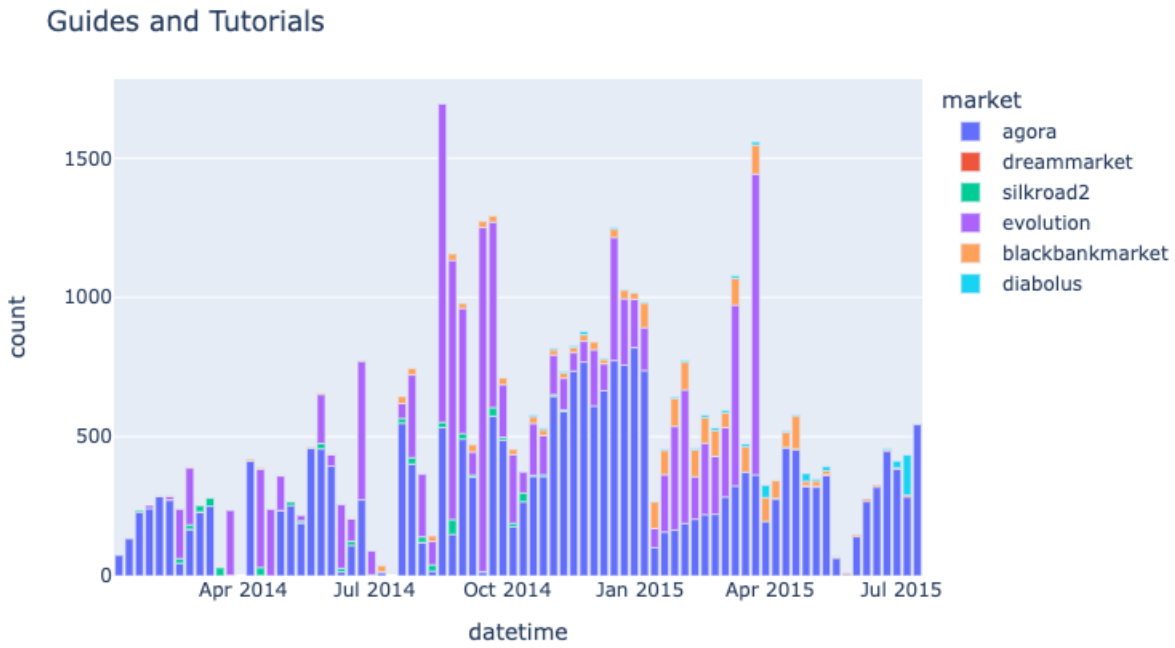

FIGURE 4.10: Guides and tutorials count over time

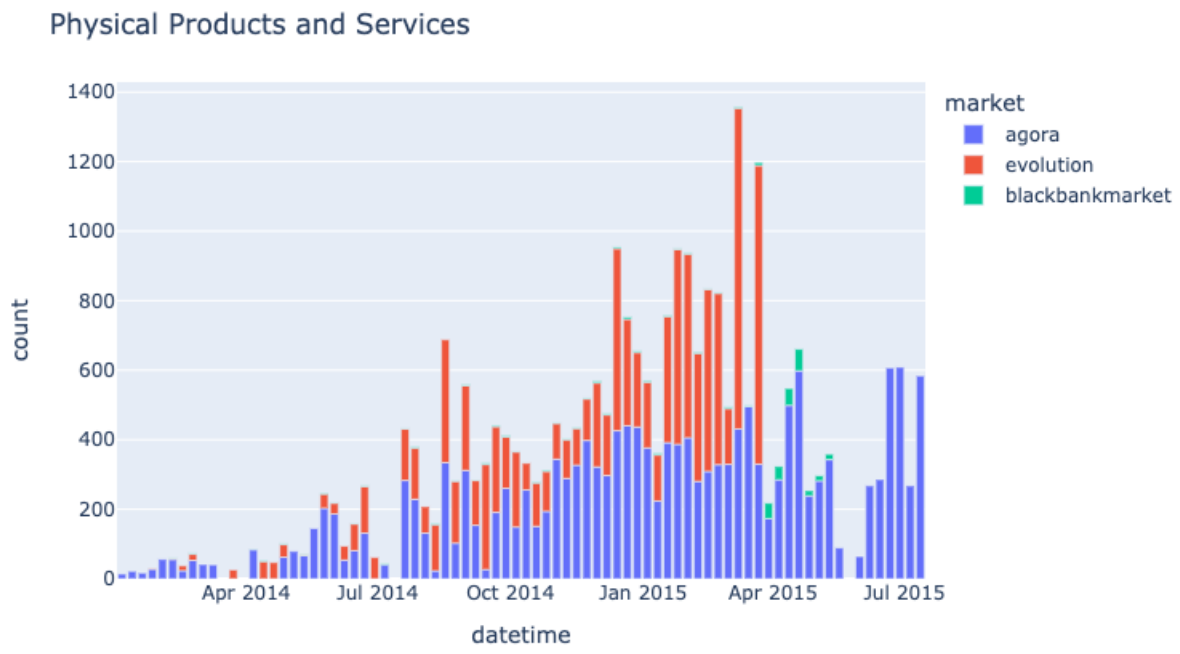

FIGURE 4.11: Physical products and services count over time

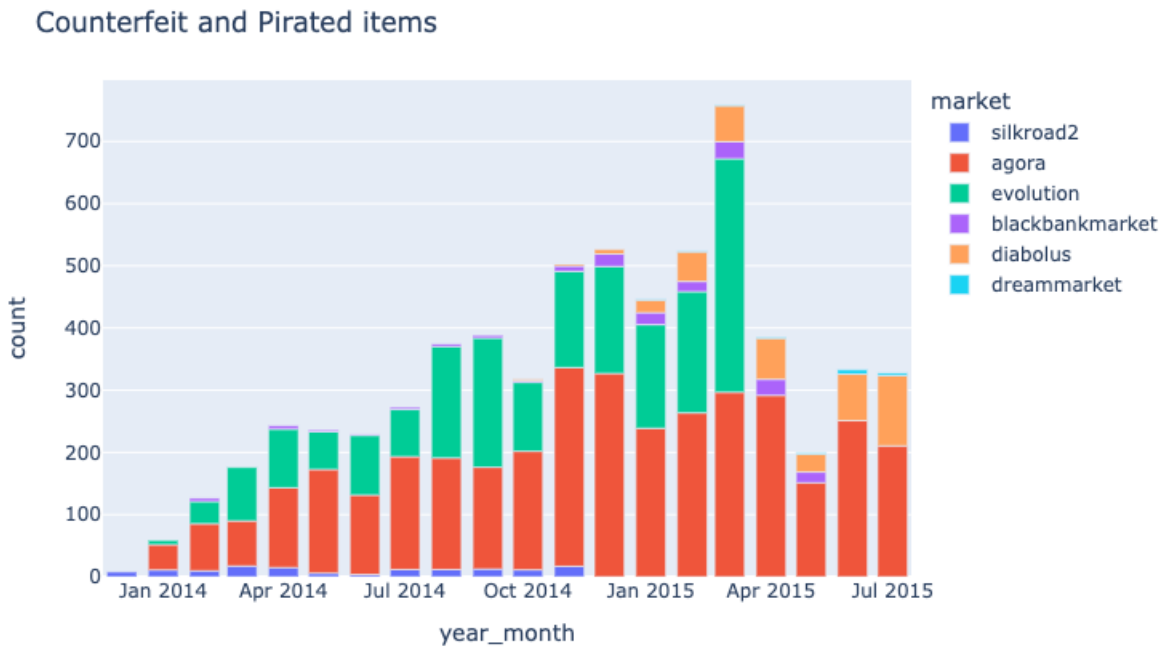

FIGURE 4.12: Counterfeit and pirated items count over time

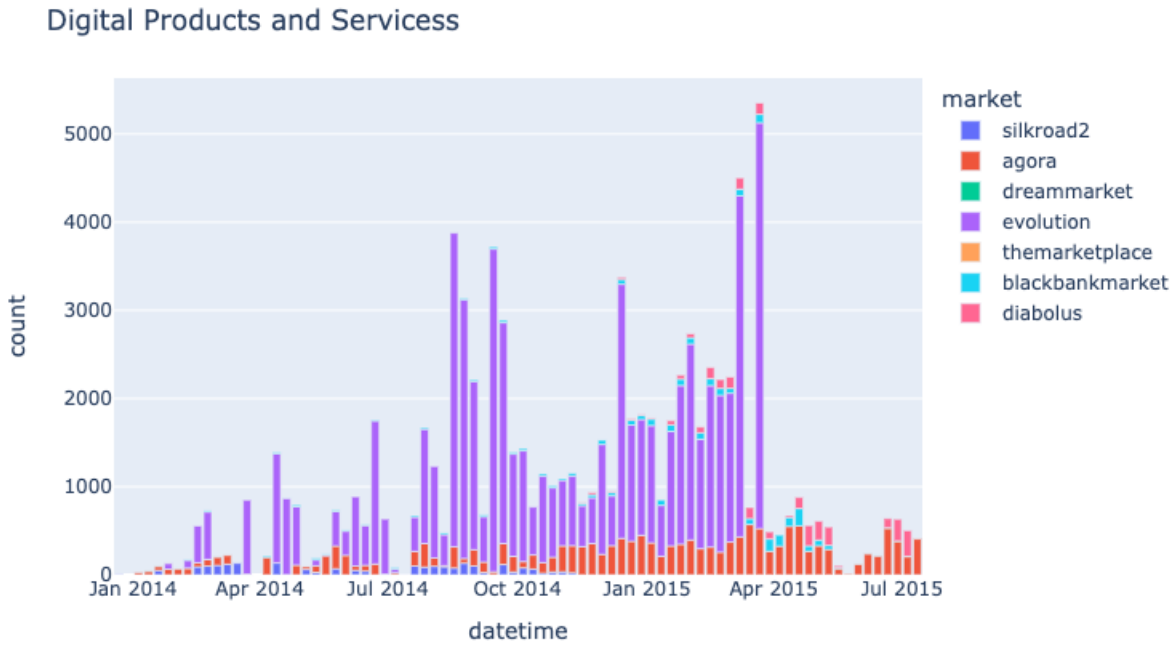

FIGURE 4.13: Digital products and services count over time

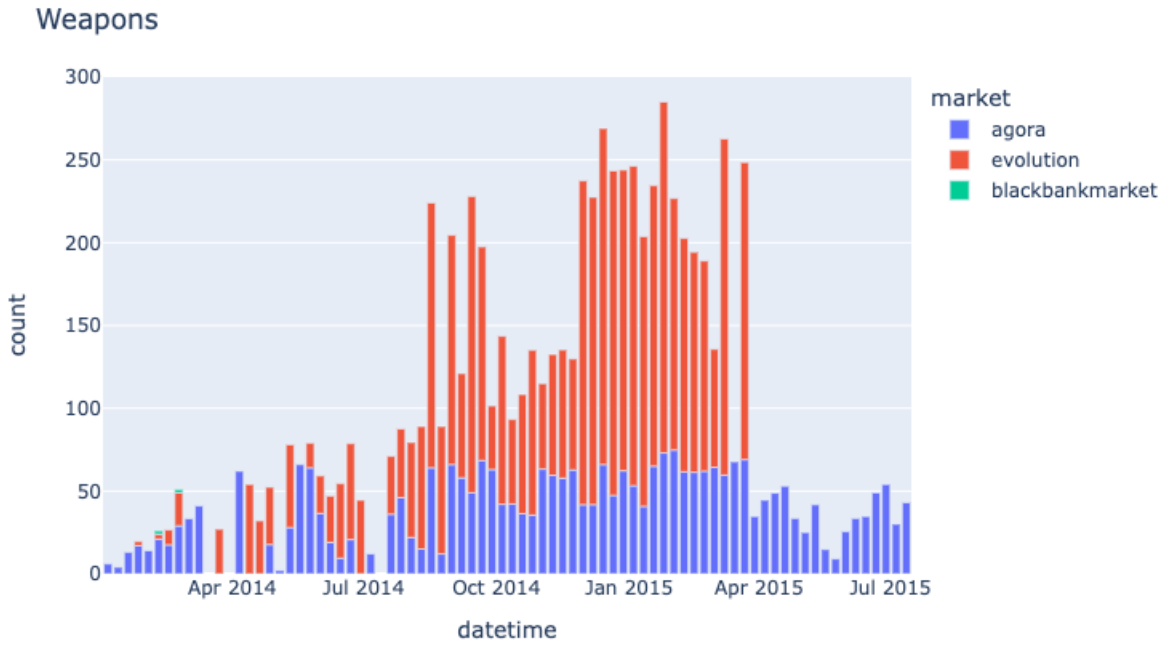

FIGURE 4.14: Weapons count over time

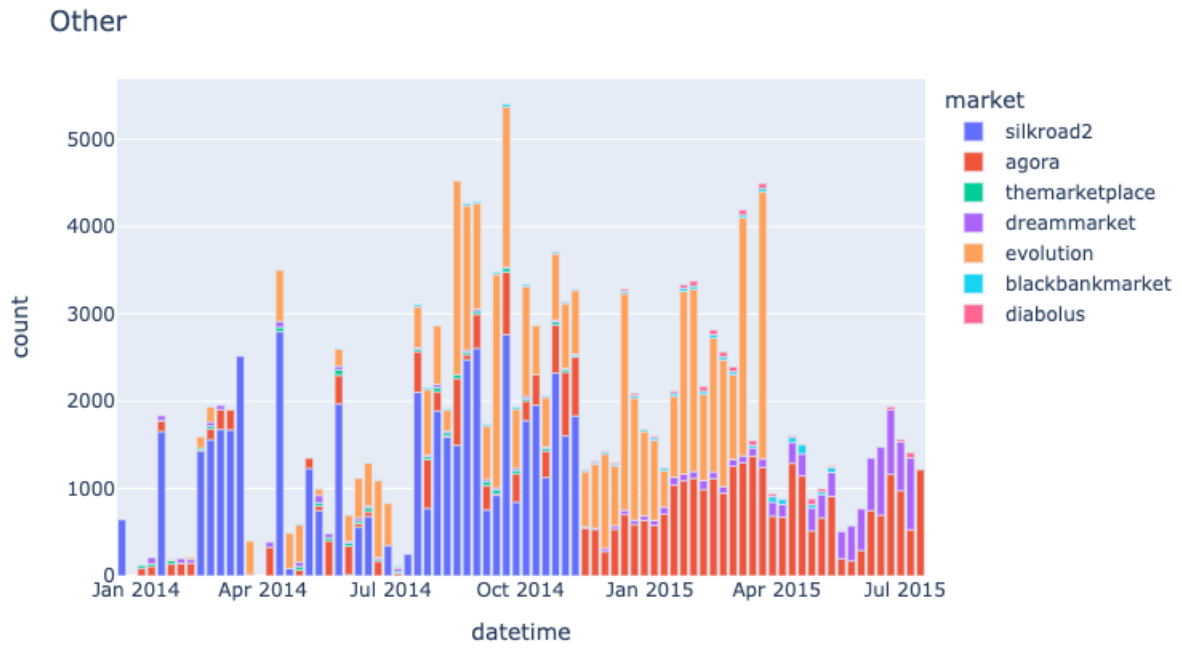

FIGURE 4.15: Others count over time

Figures 4.9- 4.15 above show how the specific categories in the DNM were affected by Operation Onymous. Starting with the category that has the most items is *Drugs and Chemicals* in figure 4.9. Before the campaign we can see that *Silkroad2*, *Agora* and *Evolution* had the biggest share within the group of DNMs. A week or two after Operation Onymous, we can see that the combined count of *drugs and chemicals* fall below 5000, this can be attributed to vendors staying low to avoid law enforcement. But just a month later, number of *drugs and chemicals* rise back up to pre-campaign levels with *Agora* and *Evolution* absorbing the vendors from *Silkroad2*. For the category *Guides and Tutorials*, we find that *Agora* and *Evolution* dominate the market as seen in figure 4.10. Likewise, a dip can be seen in the number of *Guides and Tutorials* in the DNM ecosystem after Operation Onymous and a rebound of the market after 2 months. There are only 3 DNM in our selection that offers physical products and services. As the same as before *Agora* and *Evolution* has a large influence in this category looking at figure 4.11. Astoundingly the *Counterfeit and Pirated items* category in figure 4.12 doesn't seem to be affected by the operation by much as we see a very small dip, most likely due to *Silkroad2* exiting the market and then a growth up till March of 2015. Unlike the previous few figures, figure 4.13 seems to be monopolised by *Evolution*. It doesn't seem like there is much of a change until after Operation Onymous in late 2014 where we see a sudden growth of more than 200% in count of *digital products and services*. Lastly we have the categories *weapons* and *other*, these two categories are more difficult to interpret as there aren't as much data on them. A glance at figure 4.14 would show that there aren't many markets that have the category *weapons* this is because most DNMs ban the trade of this specific category. Nevertheless, DNM like *Evolution* and *Agora* still carry these items albeit having less than 300 total count for the combined DNMs. Even though the category *other* would be harder to interpret due to the category's nature, we can still look at the

overall picture to see the effects of Operation Onymous on the market. Similar to the findings above, large DNM such as *Agora* and *Evolution* were not affected by much from the campaign. If anything, after the campaign, *Evolution* can be seen having a growth and smaller DNM like *Dreammarket* can be seen growing steadily 6 months after the campaign in May 2015.

4.2 Vendor analysis

It would be interesting to take a look at whether vendors jump-ship to different DNM when the one they are previously on has been taken down by Operation Onymous.

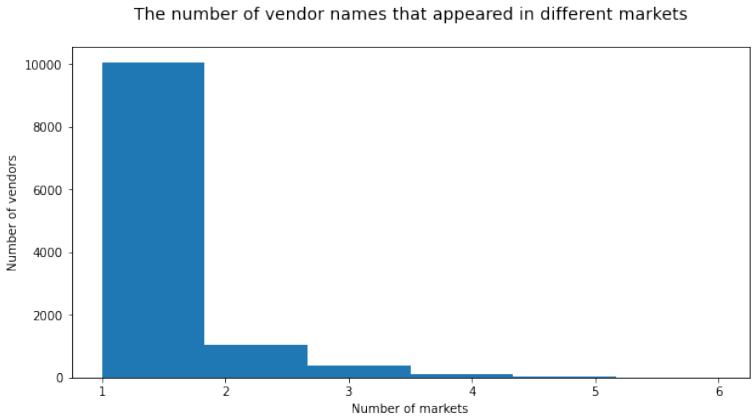

FIGURE 4.16: Number of markets that the same vendor name appears

Figure 4.16 shows a highly skewed bar chart, with most vendors only being in one of the market while about 800 vendors can be seen having the same usernames in 2 markets and only 100-200 vendors use the same name in 3 markets. However this does not show that vendors are not in multiple markets as they may use a different username.

4.2.1 Vendors that moved from *Silkroad2* to other markets

Vendor	Market	Count
DutchComfort	3	1508
theOCguy	3	102
PharmaPhil	3	538
Sun-tzu	3	178
sodawater	3	50
dubntuff	3	1085
bedia06	2	19
Fent4You	2	170
Kaskade	2	16
spartanlabsoz	2	1064
CptnHayata	2	102
diondibra	2	144
ozmetics	2	282

TABLE 4.1: Vendors with 2 or 3 appearances in different markets and items sold

Table 4.1 tries to understand if vendors that appear in more markets are also vendors that have the highest sale count. Vendors in more markets do have a higher sale count with the exception of vendor *sodawater* and *spartanlabsoz* with appearances in 3 and 2 markets but a sale count of 50 and 1064 respectively. In other words, after the intervention, vendors do seek for alternative DNM to sell on despite being at risk of law enforcement.

4.3 Feedback analysis

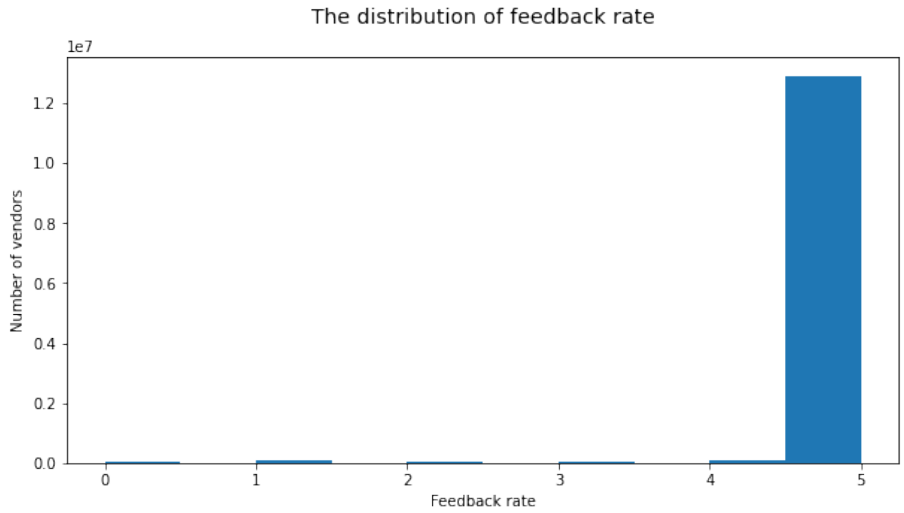

FIGURE 4.17: Distribution of feedback

Market	Feedback rate
Silkroad2	4.957
Agora	4.914
Blackbankmarket	4.831
Diabolus	4.788
Themarketplace	4.616

TABLE 4.2: Average feedback rate for each market

By merging the data from the feedback information and markets table, we can get an average feedback rating for each market. Figure 4.17 tells us that most feedback and reviews of items are positive. Either one or two possibility comes from this, vendors only receive feedback when customers are happy and would be repeat customers. Vendors that have lower quality product or service are driven out of the DNM which explains why there aren't many negative feedback. Table 4.2 shows the average feedback rate, we can see that *Silkroad2* has the highest feedback rate followed by *Agora* and *Blackbankmarket*. It may be one of the reasons why *Agora* became popular after Operation Onymous when *Silkroad2* was shut. *Evolution* did not have its own feedback system, however we can still research about the market by searching topics that relate to *Evolution* in the forums.

4.4 Forum analysis

4.4.1 Topics related to *Evolution*

ID	Forum	Date	Topic
0	agora	2014-03-19	AuthorTopic: Evolution hacked [many vendor+adm...
1	agora	2014-03-19	AuthorTopic: evolution market?? looks alot lik...
2	agora	2014-04-16	AuthorTopic: Anyone looking for us can find us...
...	...	...	...
270	themajesticgarden	2015-03-23	AuthorTopic: SunWu on Evolution?
271	themajesticgarden	2015-03-29	AuthorTopic: Alexandra from Evolution
272	themajesticgarden	2015-05-03	AuthorTopic: Evolution Guides

TABLE 4.3: Forums that consist the word *Evolution*

Table 4.3 shows a summary of the topics related to *Evolution* in different forums. There seems to be quite a lot of marketing regarding *Evolution* after the intervention. Topics such as "Is vendor x on Evolution?" and "Lets go to Evolution, 3-4% commisions, 2000+ drug listings" can be seen.

4.4.2 Sentiment analysis

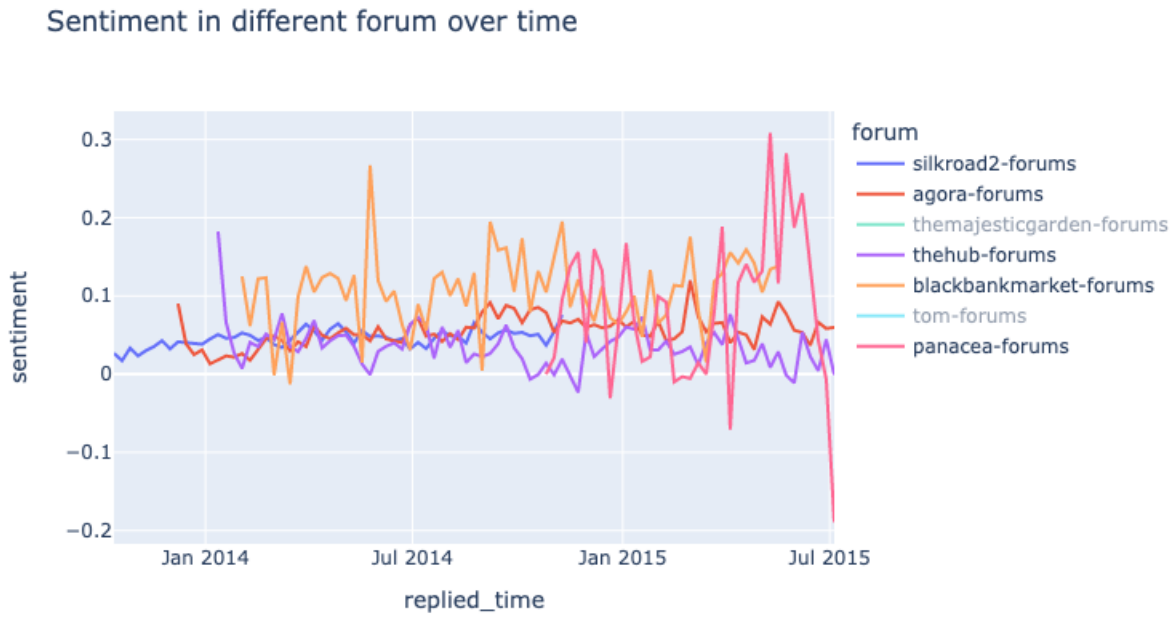

FIGURE 4.18: Sentiment of forums over time

Figure 4.18 depicts the sentiment of darknet forums over time, for easier visualisation we have removed *themajesticgarden-forums* and *tom-forums* from this figure as those forums have highly volatile data. Post intervention, the only forum that seems to have a lower sentiment is *pancea-forums* the other forums stayed relatively neutral. In mid-2015 *pancea-forums* seems to have a huge drop in sentiment value. A reasoning behind a neutral stance in darknet forums is that vendors and users may be afraid of law enforcers getting a hold of their information if they have a strong opinion on the market or they are under the law enforcers radar.

4.5 Price analysis

4.5.1 Bitcoin analysis

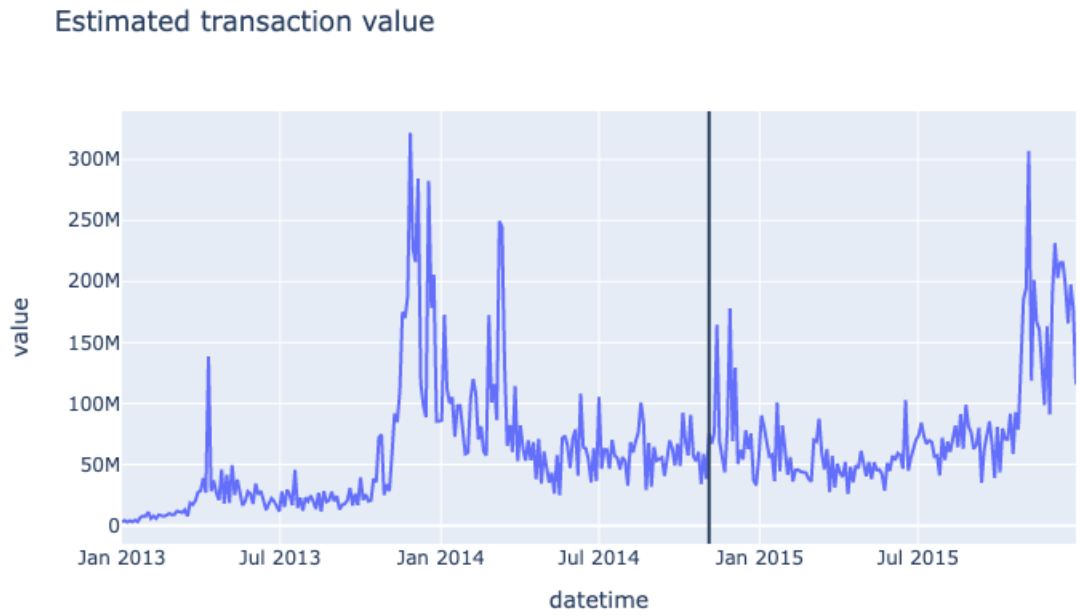

FIGURE 4.19: Bitcoin transactional value over time

Figure 4.19 plots the estimated transaction value over time to see the effects of Operation Onymous on the Bitcoin transaction value in darknet markets. The black line shows when Operation Onymous was carried out, it can be seen following the intervention a change of $100 million was wiped off instead of the $1million that was reported (Europol, 2014). Participants of the market may have withdrawn their bitcoins out of these DNM which may contribute to the change of $100 million decrease in bitcoin transaction value.

Chapter 5

Discussions of results

5.1 The effect of cybersecurity campaigns on DNM

Based on our analysis and findings, there is sufficient evidence from the data to suggest that cybersecurity campaigns are not effective at deterring participants from re-entering DNMs in the short run. The item and vendor trends show us that just a month after the intervention, the overall number of items and vendors in the market rebounds to pre-operation numbers. This is in line with previous study from Soska and Christin (2015) where they found that sales volume climbed back within a few weeks after the intervention. Furthermore, the correlation matrix between some DNM like *Silkroad2* and *Evolution* suggests that vendors are selling in multiple markets. This would mean that if an operation targets one of the two markets, vendors would be unaffected. The overall market size change also conveyed the same idea as *Evolution* grew in size in the short run after the intervention due to displacement of vendors from *Silkroad2*. This result is similar to studies found on effects of supply side enforcement on traditional drug markets (Kerr et al, 2005; Decary-Hetu & Giommoni, 2017). Overall, in the smaller DNMs there seems to be more traffic in both items and vendors after the operation as participants look for a new DNM to carry out their activities.

The vendor analysis further proves that there are indeed vendors that are involved with multiple DNMs. However, one limitation is that vendors can easily change their username and this would cause bias to our results. Feedback analysis and sentiment analysis does not seem to show any negativity within markets and forums even after the intervention. However, this may be because participants are afraid of law enforcers hence they do not want to attract any attention to themselves. Even though the sentiment analysis does not show much negative sentiment after the intervention, we can clearly see that participants are afraid of their Bitcoins being seized by the authorities.

5.1.1 Innovation in the dark net markets

Technical innovations in the dark net market are hard to spot and harder to quantify especially when these DNMs are constantly under surveillance. One such innovation is marketing campaigns for communicating with buyers as seen in the forum analysis. Marketing campaigns would start right after intervention to invite customers to a different DNM. Law enforcement's

are giving free publicity which in turns creates more competition and innovation within the DNMs (Decary-Hetu & Giommoni, 2017).

5.1.2 Recommendations

Law enforcers and policymakers may want to shift strategies and instead of having long costly operations, to have short operations that take down one DNM at a time. This would put fear into market participants as to when and where the next take-down will be and deter them from depositing any Bitcoins into the markets. Another strategy that could be implemented is targeting their mode of communications (forums) before intervening on markets. As seen from the analysis, most participants rely on forums to advertise and communicate their next move after the intervention. On the other hand, demand side programs such as spending on education of the dangers of drugs could be more cost effective than supply side programs.

Chapter 6

Conclusion

6.1 Concluding remarks and future studies

The main objective of this research is to study the evaluate the impact of cybersecurity campaigns on darknet markets. We found that in the short run, Operation Onymous was only effective at lowering activity within the darknet market for one or two weeks. In the long run these surviving DNMs tend to grow to even larger sizes prior to the intervention. Interestingly, an observation on increased innovation and competitiveness within the dark net markets and forums can be seen. Lastly, we were not able to investigate the impact of operations on the emergence of new darknet markets due to the limited dataset that we have. As this research only covers the impact of one operation on a group of DNMs, the effect of multiple operations within a same timeline is unknown. Further studies could be made to study the effects of multiple operations on DNMs. Additionally, a focus on the 3 largest DNM during the time was emphasised in this study therefore effects on smaller DNMs may be neglected. Another study that could be done is the effect of interventions on a network of smaller DNMs.

Bibliography

BBC (2015) "Silk Road drug website founder Ross Ulbricht jailed". Available at: https://www.bbc.co.uk/news/world-us-canada-32941060 (Accessed: 31 August 2022).

Bradley, C. (2019) *On the Resilience of the Dark Net Market Ecosystem to Law Enforcement Intervention*. PhD. University College London.

Branwen, G. (n.d.) *Darknet Market Archives (2013–2015), Gwern.net*. Available at: https://www.gwern.net/DNM-archives (Accessed: 31 August 2022).

Buxton, J. and Bingham, T. (2015) *The rise and challenge of dark net drug markets.*. Swansea: Global Drug Policy Observatory. Available at: http://www.drugsandalcohol.ie/23274/1/Darknet%20Markets.pdf (Accessed: 31 August 2022).

Christin, N. (2013) "Traveling the silk road", *Proceedings of the 22nd international conference on World Wide Web - WWW '13*. doi: 10.1145/2488388.2488408.

Federal Bureau of Investigation (FBI) (2022) *Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of "Silk Road" Website*. Available at: https://archives.fbi.gov/archives/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website (Accessed: 31 August 2022).

Heidenreich, S. and Westbrooks, D. (2017) "Darknet Markets: A Modern Day Enigma for Law Enforcement and the Intelligence Community", *American Intelligence Journal*, 34(1), pp. 38-44. Available at: https://www.jstor.org/stable/26497115 (Accessed: 31 August 2022).

Kerr, T., Small, W. and Wood, E. (2005) "The public health and social impacts of drug market enforcement: A review of the evidence", *International Journal of Drug Policy*, 16(4), pp. 210-220. doi: 10.1016/j.drugpo.2005.04.005.

Mazerolle, L., Soole, D. and Rombouts, S. (2006) "Street-level drug law enforcement: A meta-analytical review", *Journal of Experimental Criminology*, 2(4), pp. 409-435. doi: 10.1007/s11292-006-9017-6.

Olson, P. (2013) "The man behind Silk Road – the internet's biggest market for illegal drugs", *The Guardian*. Available at: https://www.theguardian.com/technology/2013/nov/10/silk-road-internet-market-illegal-drugs-ross-ulbricht (Accessed: 31 August 2022).

Operation Onymous (n.d.) *Europol*. Available at: https://www.europol.europa.eu/operations-services-and-innovation/operations/operation-onymous (Accessed: 31 August 2022).

Reuter, P. (1986) "Risks and Prices: An Economic Analysis of Drug Enforcement", *Crime and Justice*, 7, pp. 289-340. doi: 10.1086/449116.

Rushe, D. (2014) "Silk Road 2.0's alleged owner arrested as drugs website shuttered by FBI", *The Guardian*. Available at: https://www.theguardian.com/technology/2014/nov/06/silk-road-20-owner-arrested-drugs-website-fbi (Accessed: 31 August 2022).

Soska, K. and Christin, N. (2015) 'Measuring the longitudinal evolution of the online anonymous marketplace ecosystem', in, pp. 33–48. Available at: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/soska (Accessed: 31 August 2022).

Stone, Z. (2017) "Grams, The Google Of The Dark Web Has Shuttered Operations", *Forbes*. Available at: https://www.forbes.com/sites/zarastone/2017/12/16/grams-the-google-of-the-dark-web-has-shuttered-operations/?sh=56dc6ed37624 (Accessed: 31 August 2022).

Ursani, Z., Peersman, C., Edwards, M., Chen, C. and Rashid, A. (2021) "The Impact of Adverse Events in Darknet Markets: an Anomaly Detection Approach", *2021 IEEE European Symposium on Security and Privacy Workshops* (EuroSamp;PW). doi: 10.1109/eurospw54576.2021.00 030.

Van Buskirk, J., Roxburgh, A., Farrell, M. and Burns, L. (2014) "The closure of the Silk Road: what has this meant for online drug trading?", *Addiction*, 109(4), pp. 517-518. doi: 10.1111/add.12422.

Appendix A

Data collection structure

A.1 Market Data Structure

```
eg.
{"2013-01-13":{'items':[{'item_name': 'xxxxx',
                         'file_path': 'xxxxx',
                         'category': 'xxxxxx',
                         'vendor': 'xxxxx',
                         'item_description': 'xxxxxxx',
                         'item_img': './xxx/xxx/xxx',
                         'price': '0.0013',
                         'price_unit': 'btc',
                         'location': ['worldwide','India'],
                         'feedbacks': [
                                      {'user_name': 'xxxxx',
                                       'comment': 'xxxxxx'},
                                      {'user_name': 'xxxxx',
                                       'comment': 'xxxxxx'}],
                         'page_body':'xxxxxxxxxxxx'
                          },
                        {'item_name': 'xxxxx',
                         'file_path': 'xxxxx',
                         'category': 'xxxxxx',
                         'vendor': 'xxxxx',
                         'item_description': 'xxxxxxx',
                         'item_img': './xxx/xxx/xxx',
                         'price': '0.0013',
                         'price_unit': 'btc',
                         'location': ['worldwide','India'],
                         'feedbacks': [
                                      {'user_name': 'xxxxx',
                                       'comment': 'xxxxxx'},
                                      {'user_name': 'xxxxx',
                                       'comment': 'xxxxxx'}],
                          'page_body':'xxxxxxxxxxxx'
                          },

               'vendors': [{'vendor_name': 'xxxxx',
                            'file_path': 'xxxxx',
                            'vendor_introduction': 'xxxxxx',# Include everything
```

```
                              'vendor_public_key': 'xxxx'
                              'feedbacks': [
                                        {'user_name': 'xxxxx',
                                         'date': 'xxxxx',
                                         'comment': 'xxxxxx'},
                                        {'user_name': 'xxxxx',
                                         'date': 'xxxxx',
                                         'comment': 'xxxxxx'}],
                               'item_name': [
                                         'xxxxx',
                                         'xxxxx',
                                                ]
                               }
                                                                ]
}
```

A.2 Forum Data Structure

```
eg.
{"2013-01-13":{'poster_topic':{
                              'poster_timetamp':'xxxx-xx-xx',
                              'poster_author':'xxxxx',
                              'poster_content': 'xxxxx',
                              'replies' :[
                                        {'user_name':'xxxx',
                                         'content':'xxxxxx',
                                         'date':'xxxxxxx',
                                         'content_block_text':'xxxx'},
                                        {'user_name':'xxxx',
                                         'content':'xxxxxx',
                                         'date':'xxxxxxx',
                                         'content_block_text':'xxxx'},
                              'file_path':'xxxxxx',
                              'page_body':'xxxxxxxxxxx'},

  "2013-01-13":{'poster_topic':{
                              'poster_timetamp':'xxxx-xx-xx',
                              'poster_author':'xxxxx',
                              'replies' :[
                                        {'user_name':'xxxx',
                                         'content':'xxxxxx',
                                         'date':'xxxxxxx',
                                         'content_block_text':'xxxx'},
                                        {'user_name':'xxxx',
                                         'content':'xxxxxx',
                                         'date':'xxxxxxx',
                                         'content_block_text':'xxxx'},
                              'file_path':'xxxxxx',
                              'page_body':'xxxxxxxxxxx'},
```

Appendix B

Timeline of Operations

Campaign	Start	End	ExactTime
Operation Onymous	2014-11-05	2014-11-06	TRUE
Operation Shrouded Horizon	2014-01-01	2015-07-15	TRUE
Operation Marco Polo	2011-07-01	2013-10-02	TRUE
Operation Babylon	2013-07-31	2015-07-31	FALSE
Operation Commodore	2014-02-01	2014-02-01	FALSE
Operation Darkode	2014-01-29	2015-07-29	FALSE
Operation Hyperion	2015-10-22	2015-10-28	FALSE
Operation Pacifier	2015-02-19	2015-03-04	TRUE

TABLE B.1: Operation start and end date

Appendix C

Dark net markets and forums that Operation Onymous affected

Darknet market	Type
Agora	Market
Andromeda	Market
Blackbankmarket	Market
Cryuserv	Market
Dreammarket	Market
Diabolus	Market
Evolution	Market
Silkroad2	Market
Outlawmarket	Market
Themarketplace	Market
Agora-forums	Forum
Blackbankmarket-forums	Forum
Panacea-forums	Forum
Silkroad2-forums	Forum
Thehub-forums	Forum
themajesticgarden-forums	Forum
tom-forums	Forum

TABLE C.1: Summary of darknet markets and forums that were affected