Underground Markets: Security Metrics

WM0824TU Economics of Cyber Security - Group 16
September 23, 2019

EUR/USD - 1,35379 - 00:00:00 14 giu (EEST)
EUR/USD (Bid), Ticks, # 300 / 300
Gold, spot - 1.276,820 - 23:00:00 13 giu (CEST)
Gold, spot (Bid), 1 minute, # 159 / 300, Logarithmic, Heikin Ashi
Settings
Quote List [2]
World Markets
Dow Jones Comp.

Name	Student Number
Veroniek Binkhorst	4276620
Rowdy Chotkan	4570243
Björn Ho	4320867
Swaathi Vetrivel	4900863

Table of Contents

Table of Contents 1

1. Introduction 2

2. A framework for analysing the costs of cybercrime 4

3. What security issue does the data speak to? 5

3.1 Whose security? 5

3.1.1 Law enforcement agency 5

3.1.2 Security vendors and users 5

3.1.3 Software companies 6

3.1.4 Internet service provider 6

3.2 Security of which values? 6

3.2.1 Online safety 6

3.2.2 Privacy 6

3.3 Security from which threats? 6

3.4 Incentives 7

4. Ideal metrics for security decision makers 8

5. What are the metrics that exist in practice? 9

6. Metrics designed from the data set 11

7. Evaluation of the designed metrics 13

7.1 Total turnover per marketplace per month 13

7.2 Total turnover per category per month 14

7.3 Percentage of total turnover per category per marketplace 17

7.4 Proportion of items in the marketplace as a function of the number of sellers 18

8. Conclusion 22

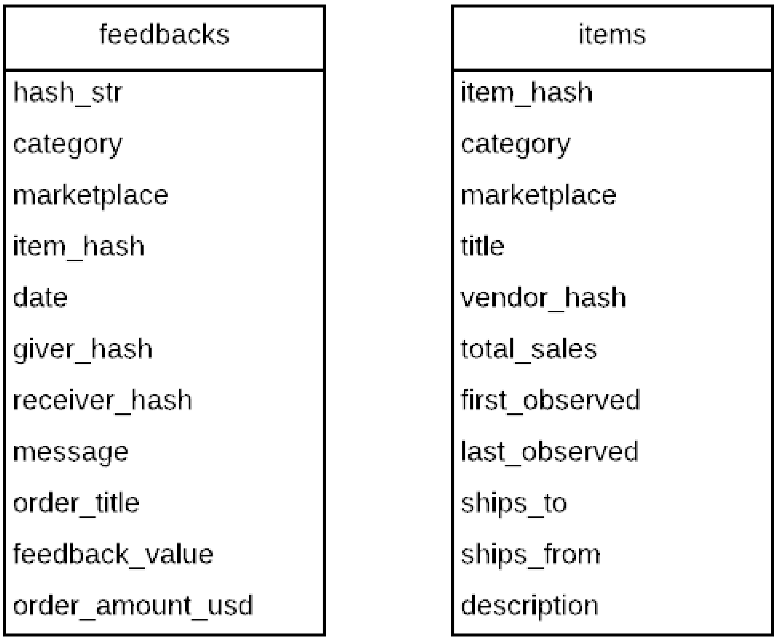
References 23

1. Introduction

During the lectures we have learned the importance of measuring cyber security and the difficulties to determine the right metric. Security metrics are used to illustrate how security activities affect security goals and help make the right security decisions. This report examines data on underground markets from the data set *16_underground_markets* and develops security metrics to deal with the security threats posed by these markets.

Cybercrime has become highly professionalized and various “underground”, i.e., illegal, markets have risen. These that supply various services required for a cyber attack (Franklin et al., 2007). This results in the phenomenon of cybercrime-as-a-service, making it possible to buy, for example, DDoS-services or fake credit card credentials in underground markets. In these markets there are sellers and buyers and moreover they are online, and hence can be defined as a multi-sided e-commerce platform (Asghari et al., 2016).

The data set on underground markets used for this project is a SQLite[1] database file, consisting of two tables, namely: `*feedback*` and `*items*`. Their decomposition can be seen in Figure 1.



feedbacks
hash_str
category
marketplace
item_hash
date
giver_hash
receiver_hash
message
order_title
feedback_value
order_amount_usd

items
item_hash
category
marketplace
title
vendor_hash
total_sales
first_observed
last_observed
ships_to
ships_from
description

Figure 1: Dataset decomposition

[1] https://www.sqlite.org/index.html

The item table consists of the listings offered and the feedback table consists of feedback given after a purchase including the receiver and giver hashes. Since these marketplaces usually require a mandatory feedback, the amount of feedback has been proven to be a good proxy for the minimum number of sales (Soska & Christin, 2015).
There also exist relations between the columns. For example, each feedback entry can be linked back to an items listing via the field `*item_hash*`. The relations also allow for the tracking of vendors across marketplaces (via the unique `*vendor_hash*` field).

These underground markets that facilitate cybercrime have a significant economic and social impact on society. An example is the ransomware WannaCry, which infected an enormous amount of computers all over the world and has a vast socio-economic impact (van Voorst, 2017). In order to develop security metrics to deal with these impacts and the overarching security issue associated with it, we first examine the costs associated with cybercrime. Thus, a framework for analysing the costs of cybercrime will be discussed section 2 followed by an introduction into the security issue associated with the dataset in section 3. In section 4, we suggest ideal metrics that would aid security decision makers to better defend against the issue and in section 5 we discuss metrics that exist in practice. The metrics designed from the data will be presented in section 6 followed by an evaluation in section 7. We conclude the report in section 8 with a brief note about the metrics discussed.

2. A framework for analysing the costs of cybercrime

The costs of cybercrime has been analyzed by Anderson et al. (2012) and they propose a framework where the total social cost of cybercrime is the sum of direct losses, indirect losses, and defence costs. Direct loss is the value of losses, damage, or other suffering felt by the victims as a consequence of a cybercrime. Part of the direct losses is the criminal revenue, which Anderson et al. (2012) defined as the gross receipts from crime. Indirect loss is the value of the losses and opportunity costs imposed on society by an act of cybercrime. Defence costs measure prevention efforts. The framework can be seen in figure 2.

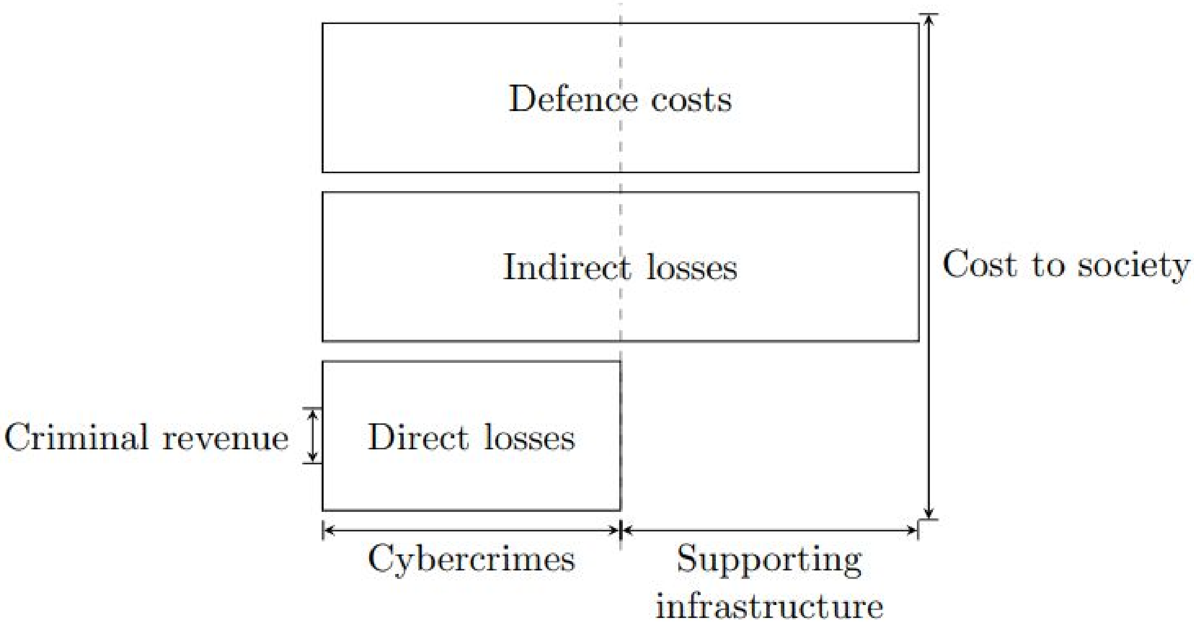


Figure 2: A framework for analysing the costs of cybercrime (Anderson et al., 2012, pp. 5).

3. What security issue does the data speak to?

The socio-economic impact on society caused by underground markets that facilitate cybercrime is the security issue that is analyzed in this report. The data indicates that there are 44578 unique items being offered by 5585 vendors across eight marketplaces worldwide. The items can be grouped into 17 unique categories of items ranging from pirated software to malware and botnets.

These underground market transactions go under the radar and result in negative externalities, the costs of which are borne by society. For instance, the costs of educating the public on best practices to defend against threats like malware is a negative externality. The cost of this externality falls to the government, law enforcement agencies, or the individual vendors of software that offers protection against malware. Hence, it would be in the best interest of all these actors and the general public to mitigate these transactions and curb the underground market activity.

In order to analyze the impact of these markets, we first need to understand the main actors involved in this security issue.

3.1 Whose security?

The global security of society as a whole is threatened by the existence of these underground markets since their operations and its consequences are not restricted by geographical boundaries. There are various actors involved in dealing with the security issues caused by these markets. In some cases the actors involved are also in turn, a victim of cybercrime. This section describes the actors and their costs and losses.

3.1.1 Law enforcement agency

Underground markets are used to facilitate cybercrime by trading illegal items and services for money. The law enforcement agency (LEA) wants to stop underground markets from operating because of violation of the law and the impact it has on society. The costs for the LEA is an element of defence costs in the framework introduced in section 2. These costs are made by the LEA to prevent cybercrime transactions and to stop the underground markets.

3.1.2 Security vendors and users

Within the data set a lot of different categories can be identified, one of them being malware. Users become victims from cybercrime because of the malware spread into the digital world. Victims suffer from direct losses because of the damage on their computer systems. Security vendors have to use effort to repair the damage caused by malware, these are indirect losses for security vendors.

3.1.3 Software companies

Piracy is very common in underground markets, this is also one of the categories inside the given data set. Software companies are making losses because they missed potential customers that might have bought a genuine copy instead of acquiring a pirated version. Pirated versions of their software is sold via underground markets. This victim wants to be protected against these indirect losses.

3.1.4 Internet service provider

Users are accessing the underground market websites via the internet service provider (ISP). So the ISP is also related to the cybercrime security issue. They do not want to block websites because this indirect loss causes bad reputation for the provider. However, the LEA could try to pressure the ISP to ban such websites from being accessed by users.

3.2 Security of which values?

This section describes the values that need to be protected from cybercrime in underground markets.

3.2.1 Online safety

Cyber attacks can be purchased from underground markets, such as DDoS attacks and malware. These attacks can cause downtime on websites which results in reputation damage to the website owners as well as possible financial losses. Victims of malware attacks also suffer from economic loss in order to repair the damage to computers. Thus the online safety of victims needs to be protected from cybercrime in underground markets.

3.2.2 Privacy

Cybercrime hackers obtain databases in order to sell personal information like credit cards and ATM cards for money. Criminals can use this information to make illegal purchases. This brings huge inconvenience to the victims, as they need to have their cards blocked and might suffer from economic losses. Thus the privacy of (possible) victims needs to be protected from cybercrime in underground markets.

3.3 Security from which threats?

The threats are the actors that are participating in the cybercrime activities in underground markets. The website owner is a threat because this actor facilitates cybercrime activities. The interest of this person is to keep the cybercrime business up for as long as possible. The other threat are all users that are utilizing the underground markets for cybercrime. For example sellers that are selling personal info on the website or buyers that want to buy cyber attacks to achieve their goal.

3.4 Incentives

Underground markets incentivize sellers because of the high amount of buyers and without the need of getting directly in contact with the buyers (Van Wegberg et al., 2018). The buyers and sellers can be anonymous and have a good accessibility, hence the underground market is suited for cybercrime. The LEA has the incentive to protect the values from the threats and to increase online safety for the victims. The effect of malware from cybercrime also incentivize ISPs to deal with it. They have increased their efforts to deal with malware because of various reasons, like costs for customer support whenever a security incident occurs on users, or to prevent brand damage since ISPs would like to provide a secure service for their clients (van Eeten & Bauer, 2009).

4. Ideal metrics for security decision makers

The primary security decision maker that is considered is the Law Enforcement Agency (LEA), which, as discussed in section 3.1.1, wants to mitigate the socio-economic impact of underground markets that facilitate cybercrime. An ideal set of metrics ought to help the LEA understand the optimal allocation of its resources to obtain maximal security benefit. Hence, the ideal metrics should measure the direct, indirect and defence costs associated with cybercrime activity as discussed in section 2. Further, since the items in the dataset are grouped by categories based on the corresponding cybercrime activity, our proposed ideal metric captures these costs associated with a cybercrime activity for each dollar spent on these categories in the underground markets. Thus, our ideal metrics would be the following.

- Direct losses incurred per category for every dollar spent
- Indirect losses incurred per category for every dollar spent
- Defence costs for each category for every dollar spent
- The loss of revenue from taxes for every dollar spent
- Damages to society for every dollar spent

These would aid the LEA in arriving at a holistic understanding of which category of items in the underground market contribute the most to losses and damage incurred by the society. This understanding would help the LEA map and prioritize allocation of their resources to defend against those categories that have a higher potential of causing damage. Consequently, it would help the LEA use their limited resources more efficiently and help them justify their security investments. Moreover, these metrics would be useful to determine the payoffs involved in various possible acts and measures against different categories of cybercrime. These metrics can also be used by the other actors discussed in section 3.1 to better focus and target their defence activities.

5. What are the metrics that exist in practice?

One of the common metrics used to measure the systemic costs and impact of cybercrime is the "*economic loss or cost per citizen per year"* due to the direct, indirect and defence costs associated with cybercrime (Anderson et al., 2012). This metric gives a direct hint at the costs borne by society for various cybercrime activities and helps with the allocation of resources in order to target those activities that cause the most impact.

Other metrics in practice are used to categorize the offerings on the underground markets and thereby better understand and catalogue cybercrime activities. These include "*total revenue per category per month* and "*percentage of total revenue per category per marketplace"*, among others (Van Wegberg et al., 2018). The total revenue per category per month gives an indication on which categories contribute most to the growth of sales and revenue in the underground markets. Similarly, the percentage of total revenue per category per marketplace helps to evaluate market specializations,m among the different marketplaces of the underground market. A related metric is "*the proportion of the items in the marketplace as a function of the number of sellers"* (Christin, 2012). This can help to identify the volume of inventories held by individual sellers and isolates the contribution of each seller to the total number of items in the marketplace.

Another set of metrics used in practice tracks the damages caused by cybercrime activities and develops strategies to deal with them. Brenner (2004) analyses the characteristics of cybercrime in comparison with real world crime and suggests possible crime metrics that can be extrapolated to cybercrime. In addition, she also investigates the differences unique to cybercrime and suggests possibilities to develop targeted cybercrime metrics. These cybercrime metrics are divided into three categories based on the harm they inflict - individual harm cybercrime, systemic harm cybercrime and inchoate harm cybercrime. These metrics consider both the harm inflicted by the crime and the culpability of the offender in assessing the harm associated with a specific cybercrime. While these metrics might not help in foreseeing or preventing cybercrime, they serve as a useful framework to analyse their social impact and consequences.

Table 1: metrics in practice

Metric	**Unit**	**Description**
Losses/person/year	€	Provides information on the total economic loss to society due to an activity.
Total revenue per category per month	$/month	Provides information on the total yield of the categories.
% of total revenue per category / marketplace	%	Provides information on the relative yield of the categories.

Proportion of items in the marketplace as a function of the number of sellers	% of all items sold / seller	Provides information regarding the diversity of sellers on the marketplaces.

6. Metrics designed from the data set

Out of the four identified metrics used in practice, three can be applied to the data set. Even though losses/person/year is a valuable metric for the security issue, no data is available regarding the total impact of the transactions in the data set.

In section 4, we have identified ideal metrics to estimate the impact caused by underground markets that facilitate cybercrime and it can be broken down into three costs, namely the defence costs, the indirect losses and the direct losses which also includes the criminal revenue. With this data set it is possible to get insight into only the criminal revenue, but not on the defence costs, the indirect losses and the remaining direct losses.

To get insight into the criminal turnover, we use three of the four metrics identified in theory. However, we do not know whether transaction costs or other costs are subtracted from the order amount, thus we cannot say for certain that we have data regarding the profit. We do have data about the turnover. Therefore, we use turnover in these metrics.
Next to the three metrics from theory, an additional metric has been identified, namely the total turnover per marketplace per month. An overview of these metrics can be found in table 2.

Table 2: Metrics designed from the dataset

Metric	Unit	Description
Total turnover per marketplace per month	$/month	Provides information regarding the turnover for each marketplace per month.
Total turnover per category per month	$/month	Provides information on the total yield of the categories.
Percentage of total turnover per category per marketplace	%	Provides information on the relative yield of the categories of products sold.
Proportion of items in the marketplace as a function of the number of sellers	% of all items sold / seller	Provides information regarding the diversity of sellers on the marketplaces.

First we look at the turnover per marketplace per month. This turnover per marketplace per month will give LEA direct insight into the criminal turnover. To give LEA more insight into which products are responsible for the turnover, we look at the total turnover per category per month. Next, we look at the percentage of total turnover per category per marketplace, to get an insight into the relative yield of the categories of products sold. Finally, we look at proportion of items in the marketplace as a function of the number of sellers, to give LEA insight into the diversity of sellers on the marketplaces. For the first three metrics the table “feedbacks” is used from the dataset, for the last metric the table ‘items’ is used.

With these metrics LEA can estimate the criminal revenue on these marketplaces and see which categories of products are most sold, what they all yield and whether they are sold by many sellers or just a few.

7. Evaluation of the designed metrics

This section contains an evaluation of the metrics introduced in section 6. In the graphs sometimes some lines are interrupted, this is because of empty values within the data set.

7.1 Total turnover per marketplace per month

The graph below describes the total turnover per marketplace per month for the marketplaces found in the data set. From the graph it can be concluded the market Alphabay has increasing turnover per month. This information is useful for the LEA to determine which marketplace should be given the highest priority. They can focus on the marketplace with the highest turnover for defensive resource allocation to minimize the cost to society and maximize the impact of the defensive measures.
Alphabay is the only marketplace of which data has been recorded post 2015. To get the full picture for LEA, it is recommended to gather data from multiple marketplaces.

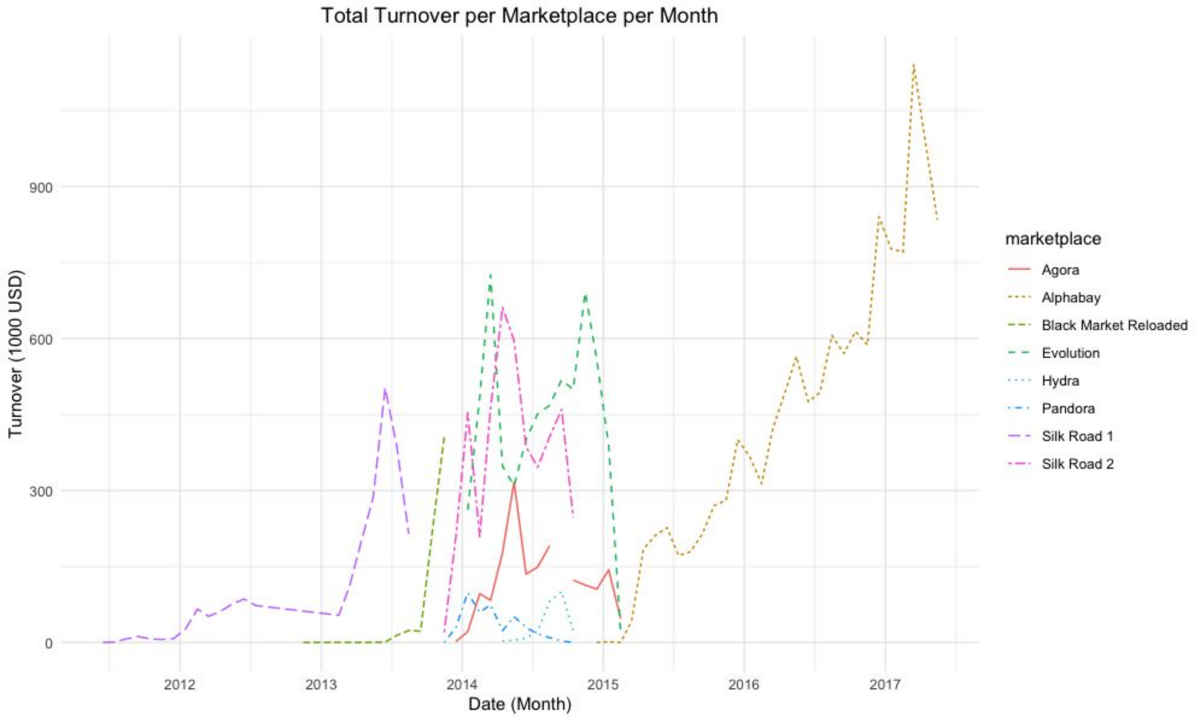


Figure 3: total turnover per marketplace per month

The surface beneath the lines in the graph equals the total turnover per marketplace, which can be seen in table 3. Regarding the total turnover over the whole period data has been collected Alphabay has the highest turnover.

Table 3: Total turnover per marketplace

Marketplace	Total turnover ($)
Alphabay	13.036.489,96
Silk Road 1	2.239.430,04
Evolution	6.125.115,43
Black Market Reloaded	685.107,93
Agora	1.818.989,71
Pandora	394.306,39
Hydra	242.230,61
Silk Road 2	4.455.336,20
Total	28.997.006,27

7.2 Total turnover per category per month

The total turnover per category per month for our data set has been captured in the graphs below. The first graph captures the turnover per month for the Business to Business (B2B) categories excluding the Business to Consumer (B2C) categories that have been grouped with the keyword 'other-' the data set.

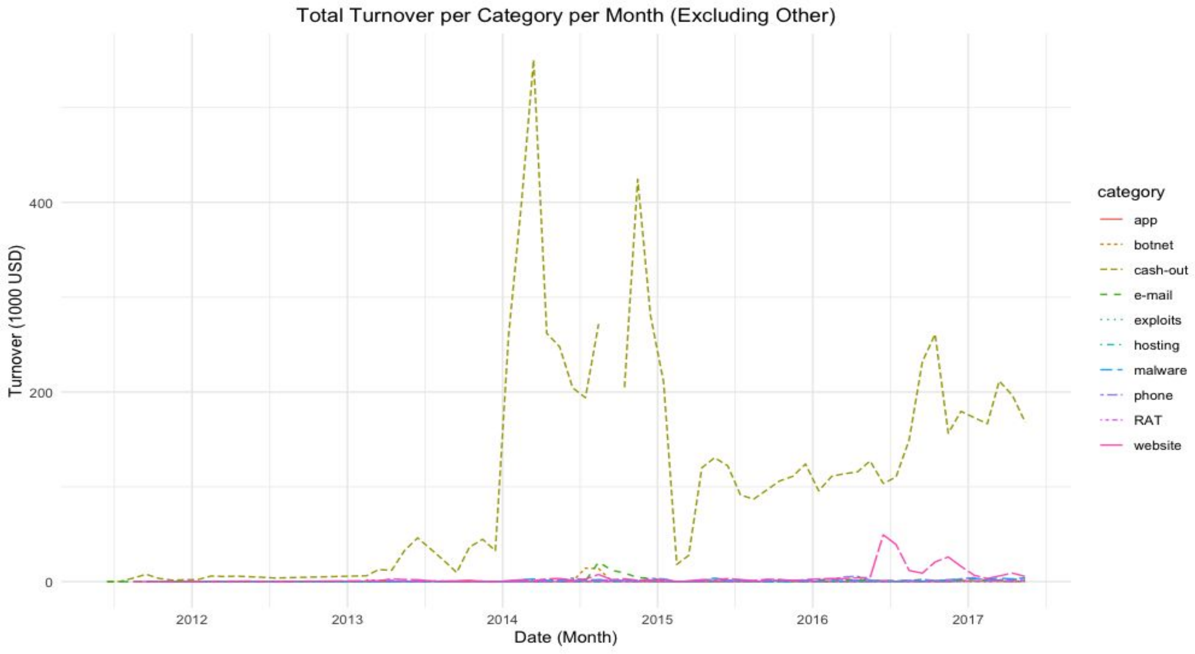


Figure 4: total turnover per category per month (excluding other)

From this graph, it is evident that the category ‘cash-out’ receives the largest turnover by a high margin. The margin of difference between cash-out and the other categories skews the graph causing the values of the other categories to be scaled down to the low hundreds. To overcome this, the second graph plots the values of turnover of all the B2B categories excluding cash-out.

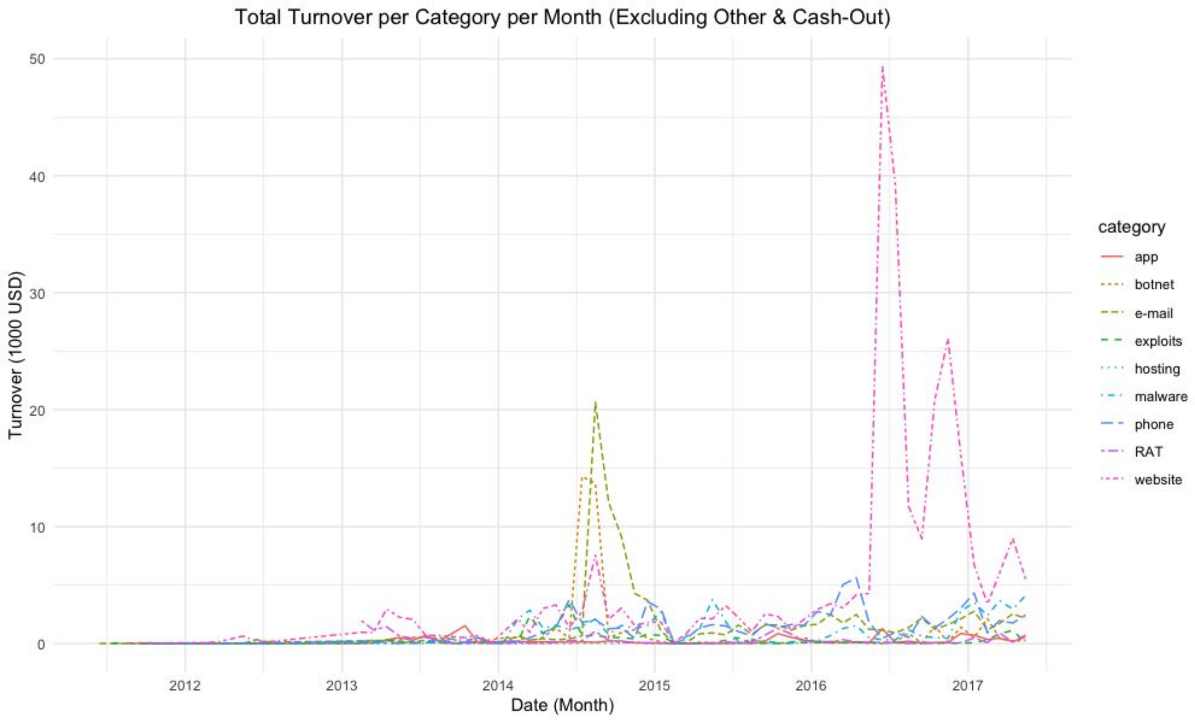


Figure 5: total turnover per category per month (excluding other and cash out)

This distribution has a toned down scale which helps identify the other high turnover yielding categories to be website, email and botnet. Figure 6 contains the turnover of the B2C categories.

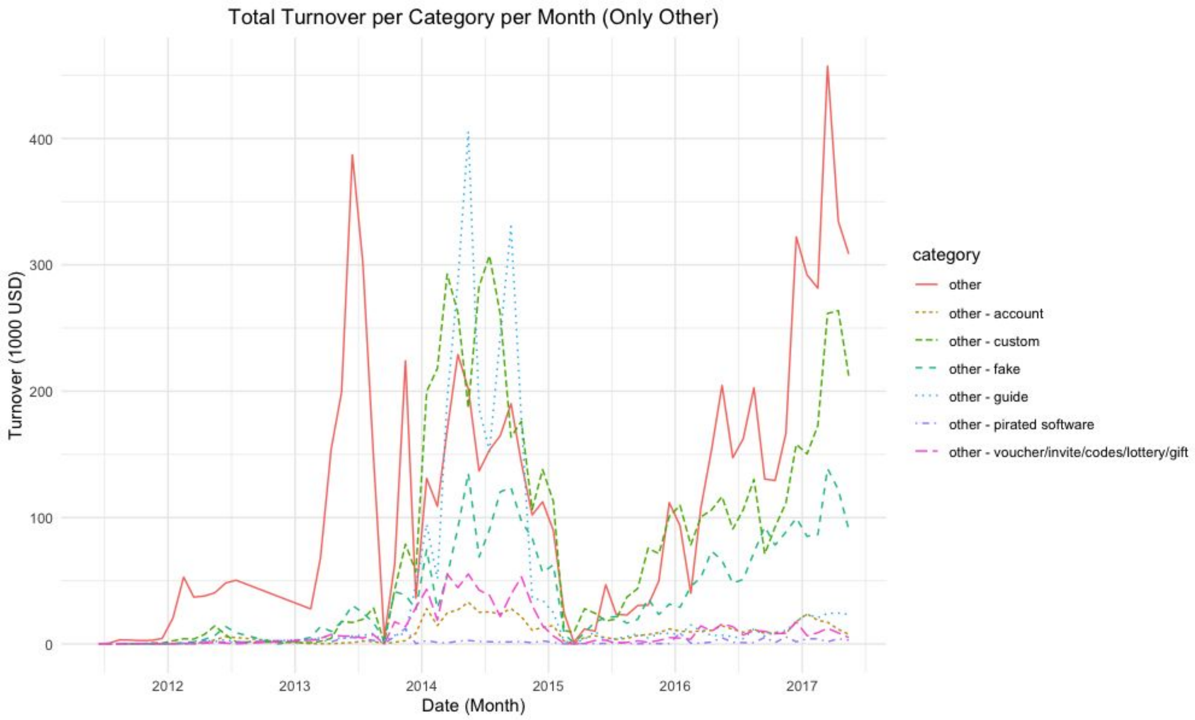


Figure 6: Total turnover per category per month (only other)

Among the turnover of the B2C categories captured in the third graph, the category ‘other’ which contains all the miscellaneous transactions shows the highest turnover. More interestingly however, guides and custom transactions within the B2C generate high turnovers. Knowledge of the categories that have high turnovers can help focus the LEA’s efforts into developing strategies to specifically target these crimes. Reduction of cybercrime activities associated with these categories would decrease the turnover of the underground markets and thereby decrease the funds available circulation within these markets.

Table 4 contains for each category summed for all markets the total number of sales, the mean order amount, the median order amount, the minimum and maximum order amount and the standard deviation.

Table 4: Descriptive statistics for each category

Category	Total number of sales	Mean ($)	Median	Minimum	Maximum	Std. deviation
App	1.152	10,99	4,92	0,00	264,00	22,36
Botnet	954	46,00	3,06	0,00	2475,85	257,83
Cash-out	232.659	32,88	10,00	0,00	9756,16	150,74
E-mail	4.631	18,88	5,90	0,00	1605,78	80,55
Exploits	1.316	13,27	7,90	0,00	500,00	41,66

Hosting	119	9,89	5,44	3,00	99,41	14,31
Malware	2.404	23,28	5,00	0,00	1984,90	68,20
Other	81.883	91,44	19,74	0,00	9941,12	365,33
Other - account	74.621	7,93	5,00	0,00	1.523,19	20,72
Other - Custom	18.259	310,71	59,58	0,00	9.950,00	803,10
Other - Fake	33.559	82,78	35,00	0,00	4.224,92	168,53
Other - Guide	56.303	45,92	3,25	0,00	8.558,88	163,93
Other - Pirated software	11.075	11,53	2,97	0,00	4.000,00	97,30
Other - v/i/c/l/g	22.205	33,09	24,99	0,00	2.725,82	57,16
Phone	2.689	27,40	9,99	0,00	3200,00	92,43
RAT	756	21,21	4,99	0,00	919,20	62,91
Website	8.460	33,59	5,37	0,00	1695,00	122,56

In the table it can be seen that the category ‘cash-out’ has by far the largest amount sales, explaining the large amount of turnover in figure 4. Another thing that stands out in the table is the difference in maximum order amount per category, ranging from $99,41 for hosting to $9756,16 for cash-out.

7.3 Percentage of total turnover per category per marketplace

With the information from the total turnover per month per marketplace to indicate which marketplace has the highest turnover and the information from the total turnover per category per month to indicate which category of product has the highest turnover, it is interesting to know which categories are dominantly sold on the different marketplaces. In figure 7 this information can be found.
This information can be used by LEA for multiple purposes. First of all this information can be used to see what marketplace to target if LEA wishes to target one or more specific categories. Second, it can be used to develop a strategy on how to target a marketplace if a decision has already been made on what marketplace to target.

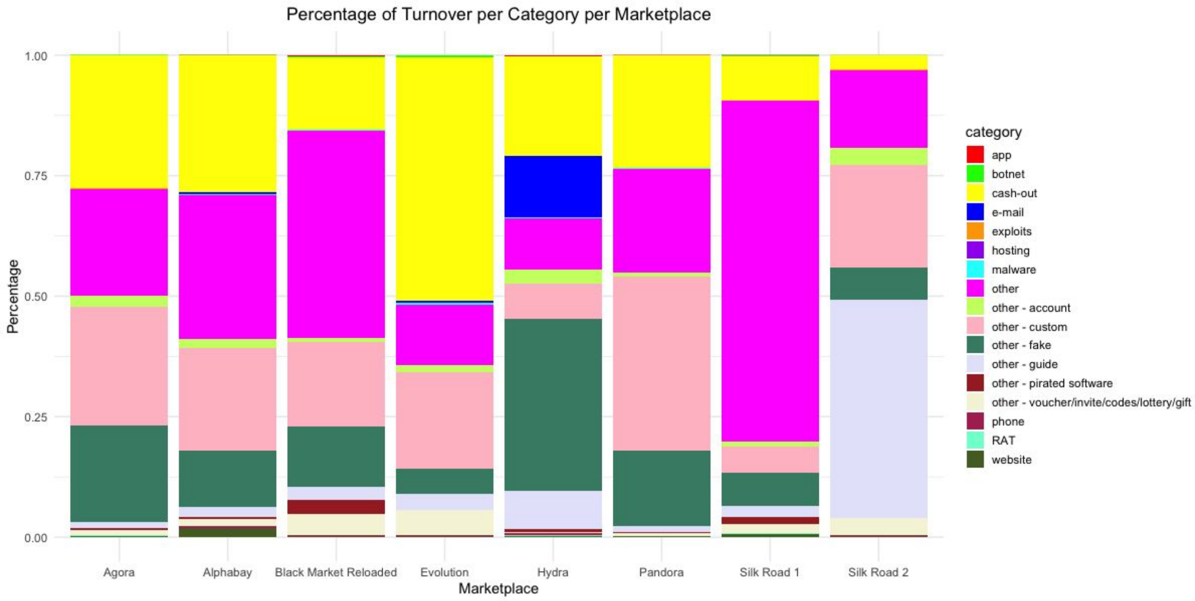


Figure 7: percentage of total turnover per category per marketplace

As can be seen, there is a difference between marketplaces regarding the dominance of the categories sold, measured in percentage of the total turnover. What is interesting to notice is that five categories are a large part of the percentage of the total turnover across all marketplaces, these are the categories ‘cash-out’, ‘other’, ‘other - custom’, ‘other - fake’, and ‘other - guide’. Especially in the marketplace Silk Road 1 the category ‘other’ represents a very large amount of the percentage of the total turnover and ‘other - guide’ is extremely popular on Silk Road 2.

7.4 Proportion of items in the marketplace as a function of the number of sellers

The proportion of items set against the number of vendors in a marketplace gives an overview of how many sellers are responsible for the amount of listings available. Using this information, LEAs can determine the largest vendors of the platforms, the so-called “big fish”. Thus, they can more easily set priorities where to allocate their resources. A takedown of a large vendor will result in a decrease in the amount of listings and make items unavailable. As a result, the threat of the security issue decreases.

The aforementioned metric has been calculated on three different aspects of the dataset. In figure 8, the function has been calculated across all marketplaces. This figure makes it quite hard to draw conclusions on all marketplaces. However, in the curve of “Alphabay” it already becomes apparent that approximately a sixth of its total amount of sellers (~500) is responsible for approximately 70% of its listings. In perspective of the LAEs: this confirms the existence of “big fish” on which the priority should be on a higher level than the smaller vendors.

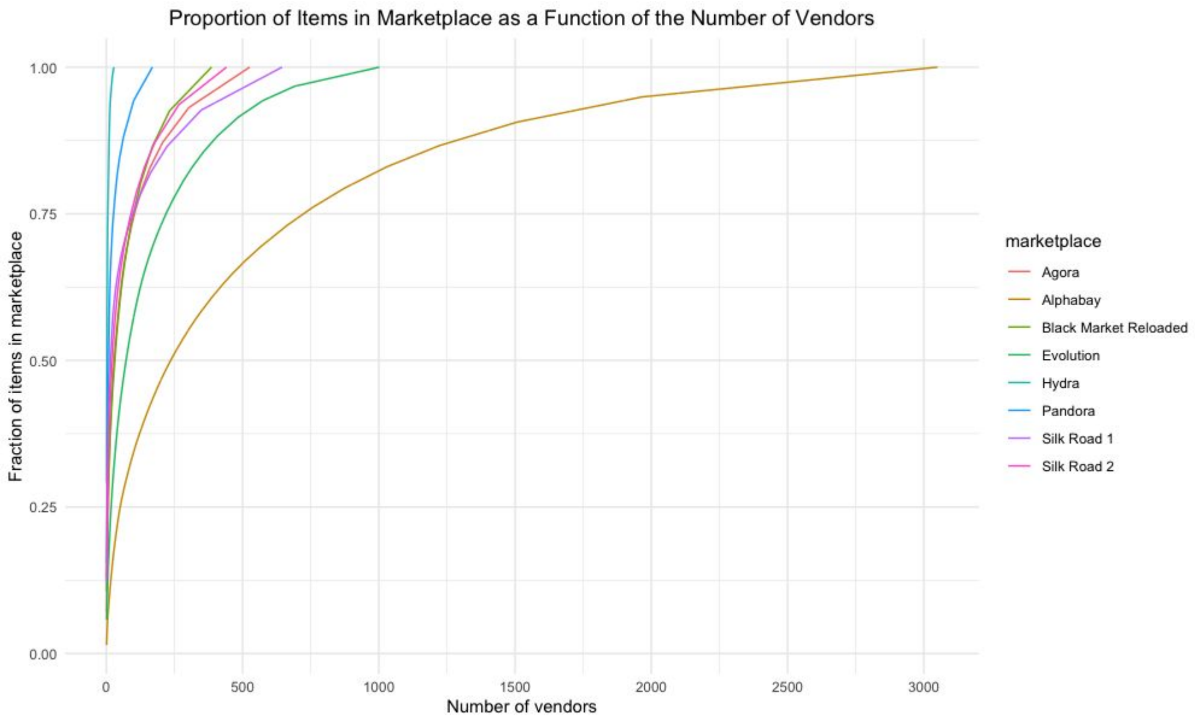


Figure 8: Proportion of items in the marketplaces as a function of the number of sellers

In figure 9 the same function has been calculated. Note that the results of “Alphabay” and “Evolution” have been omitted for readability purposes. The same conclusions can be drawn here, e.g., “Silk Road 1”: approximately a sixth (~100) of its vendors provide over 75% of the listings on the platform.

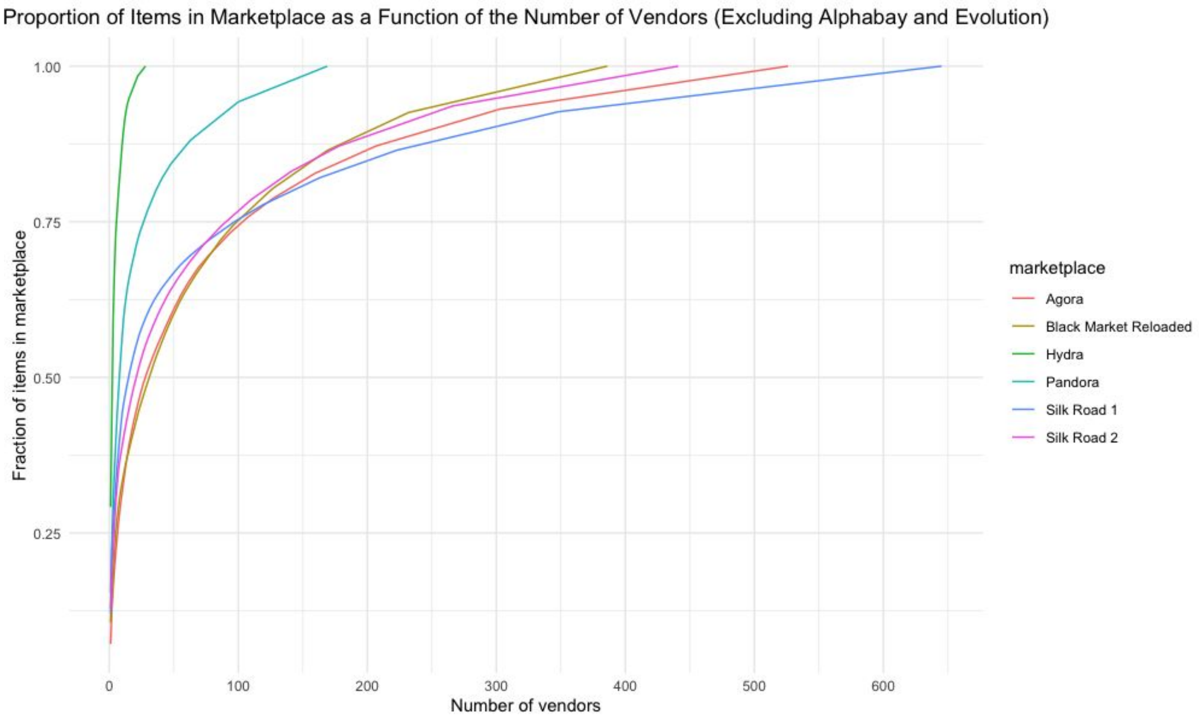


Figure 9: Proportion of items in the marketplaces as a function of the number of sellers (Excluding Alphabay & Evolution)

Finally, in figure 10 the function has been applied to the entire dataset, resulting in a function on the total amount of listings set against the total number of vendors. Here we can see that approximately 5% (~250) of the vendors supply the platforms with almost 50% of their listings. Note here that the dataset tracks vendors across marketplaces. However, there still exists a probability that the same vendor is using multiple accounts, hence resulting in multiple hashes. This means that even less vendors could be responsible for these listings. Using this metric, the LAEs can have a big impact on the marketplaces' listings by focussing on the largest vendors, which is indicated to be only a small amount of the total amount of vendors.

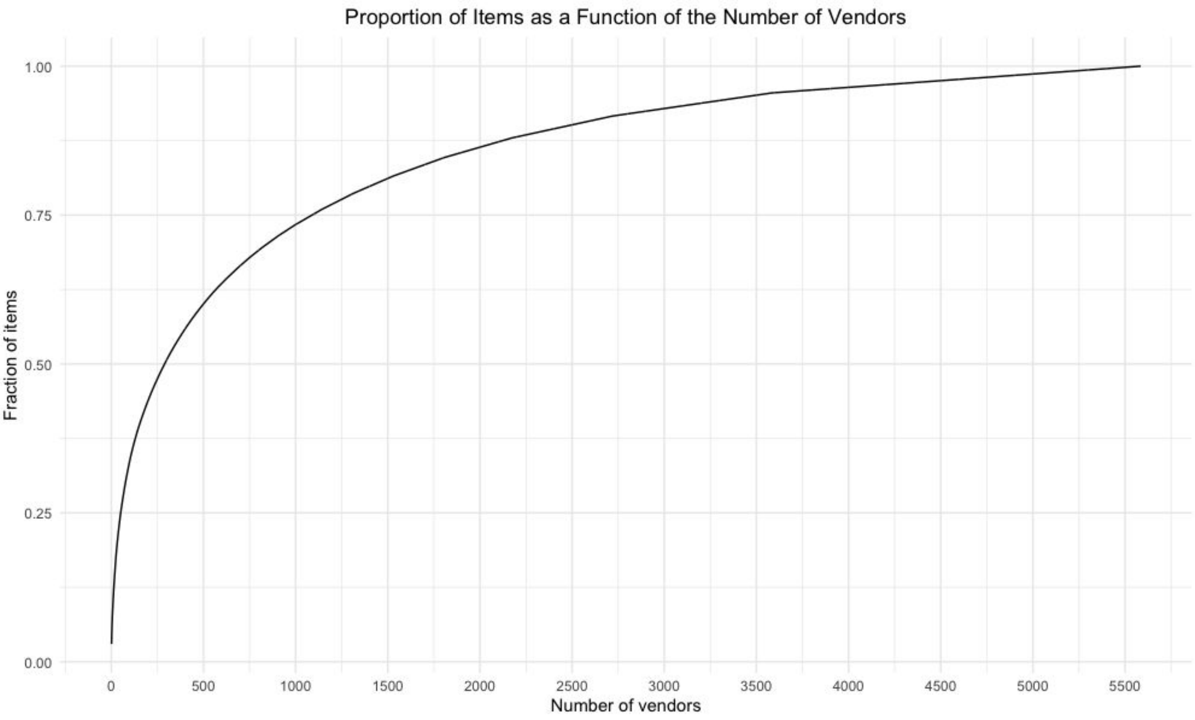


Figure 10: Proportion of items in all marketplace as a function of the number of sellers

8. Conclusion

To conclude, understanding the socio-economic impact on society caused by underground markets that facilitate cybercrime is crucial in developing strategies to deal with the threats they pose. Through the metrics discussed, we quantify the costs associated with various activities in the underground markets. The metrics discussed are the total turnover per marketplace per month, total turnover per category per month, the percentage of total turnover per category per marketplace, and the proportion of items in the marketplace as a function of the number of sellers. With these metrics we arrive at an understanding of key activities that have the highest socio-economic impact on society caused by underground markets that facilitate cybercrime and are able to accurately measure the criminal revenue. Allocation of resources to these key targets would allow for a judicious distribution of scarce security resources to obtain maximal security benefit.

References

Anderson, R.J., Barton, C., Böhme, R., Clayton, R., Eeten, M.V., Levi, M., Moore, T., and Savage, S. (2012). *Measuring the Cost of Cybercrime*. WEIS.

Asghari, H., Van Eeten, M., & Bauer, J.M. (2016). *Economics of Cybersecurity.*

Brenner, S. (2004). Cybercrime Metrics: Old Wine, New Bottles?

Christin, N. (2012). *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace*. Proceedings of the 22nd International Conference on World Wide Web.

Franklin, J., Perrig, A., Paxson, V., and Savage, S. (2007). *An inquiry into the nature and causes of the wealth of internet miscreants*. Alexandria: VA, pp. 375–88.

Soska, K. & Christin, N. (2015) Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. *24th USENIX Security Symposium*, 33–48.

Van Eeten, M & Bauer, J.M. (2009). Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications. *Journal of Contingencies and Crisis Management* 17 (4), pp. 221-232.

Van Voorst, S. (2017) WannaCry-ransomware in 150 landen. Retrieved on 22 September 2019 from https://tweakers.net/reviews/5419/wat-maakt-wannacry-anders-dan-andere-ransomware.html

Van Wegberg, R., Tajalizadehkhoob, S., Klievink, B., Soska, K., Akyazi, U., Gañán, C., Christin, N. & Van Eeten, M. (2018). *Plug and Prey? Measuring the Commoditization of Cybercrime via Online Anonymous Markets*.