Economics - Security Metrics

Michiel Doesburg
TU Delft
m.s.doesburg@student.tudelft.nl

Cas Buijs
TU Delft
s.j.m.buijs@student.tudelft.nl

Aleksandra Taneva
TU Delft
a.p.taneva@student.tudelft.nl

Elena Tsvetkova
TU Delft
e.o.tsvetkova@student.tudelft.nl

September 2018

Abstract

For the course Economics of Cybersecurity of the Master program Computer Science at Delft University of Technology, we analyse a certain dataset, name and define the security metrics corresponding to the given dataset. Further, a discussion arises considering the connection between security measures and security metrics. By defining the metrics, as the assignment demands, we investigate and determine the impact and threat of the given data extract. Supposedly, the metrics will give the opportunity to quantify and structure a certain characteristics of the data presented and estimate the value of the components. For the purpose of investigating and reviewing of the metrics, a graphical illustration is presented.

1 Introduction

The concept of exchanging goods and services exists for a long time and with the rise of the Internet the offerings have also moved to online platforms, like 'Marktplaats.nl' or 'Ebay.com'. Those platforms are regulated and abide to the laws of the countries they make trade available in but not every platform does that. Platforms which allow the exchange of prohibited goods and services currently exist in various countries, where such offerings are deemed illegal. Online platforms, or also called online marketplaces, that ignore the law are called "illegal 'underground' marketplaces" as they try to hide themselves in the World Wide Web. The widespread use of the Internet in all areas of life has also lead to the proliferation of such marketplaces, such as: ‘Silk Road 3‘, ‘Dream Market‘ and ‘Berlusconi Market‘. The goods and services offered on these markets range from ordinary products like books and apparel, to illicit substances such as drugs and prescription medicines, to harmful digital goods. The retail and distribution of malicious and hamrful software which could disrupt the normal functioning of such systems is a problem in itself, but the bigger issue would be why such an opportunity is presented to cyber criminals in the first place.

This document is structured as follows: Section 2 outlines the issue in the context of the main stakeholders concerned; Section 3 discusses the security issue; Section 4 provides the ideal security metrics; Section 5 gives an overview of metrics used in practice; Section 6 discusses metrics that can be designed from the data; Section 7 provides an evaluation of the metrics from the data and the report is concluded in section 8.

2 Context

There are various stakeholders which are involved or affected by the existence of underground marketplaces. On the one side are the people enabling the illegal trade and facilitating the distribution of harmful software by running these marketplaces, as well as those developing and offering malicious software, like viruses and malware. These activities threaten the welfare of society and the safety of its citizens in a number of ways: they pose a direct threat by endangering the normal functioning of organizations and businesses, thus inflicting serious financial and possibly emotional damages. In addition, the indirect consequences, such as loss of privacy, trust and the feeling of safety could have lasting negative effects. Therefore, another actor would be the government, having the responsibility to enforce the law and protect the rights of its citizens. Taking into account the effects of network externalities, involvement of the government seems as a suitable course of action, due to their ability to stimulate joint activities between multiple parties [2]. Speaking in terms of risk management terminology, the welfare of society and its safety could be viewed as the assets, which the government would have to defend from the activities of cybercriminals, who could be considered the attackers of these assets. Consequently, the existence of underground marketplaces can be seen as a major security issue for governments, as they are the main actor which could make decisions in order to limit their functioning, through their various agencies.

3 What security issue does the data speak to?

The data pertains to 8 underground market places, collected during a period of 6 years (2011-2017). The data consists of 2 tables which encompass the transaction data of these 8 underground markets:

1. Transaction data between users which includes the category of the item

which was sold, the seller, buyer, marketplace on which the item was sold, date of transaction, order amount, and price paid, as well as the feedback by the buyer.

2. Data on the items being sold, which includes the type of item including a feedback from the buyer, the marketplace it was sold on, the total amount sold of each item, from when to where it has been shipped, and when the item was first and last observed.

The security issue is as follows: underground markets facilitate the anonymous flow of goods without governmental oversight, thereby avoiding regulation and evading taxes. These goods also include items which are illegal to trade like malware and stolen goods. The internet facilitates the illegal trade as it provides easy access to potential customers, who remain anonymous through use of bitcoin for payments. The high level of untraceability of the users of these underground markets makes it difficult for law-enforcement and international agencies to track and prevent the illegal exchange of goods. From the perspective of regulatory, governmental and law-enforcement agencies we want to define metrics to help them understand the scope of this security issue. The main actors in this report are the law-enforcement agencies.

4 What would be the ideal metrics for security decision makers?

Security decision makers have to decide how much effort and financial resources has to be spend on certain issues. For this the ideal metrics for them should be answering questions like: "What is the scope of the problem?" and "How much money does this problem cost us?". From the perspective of a law-enforcement agency, it is valuable to know the number of unique users per market to get insight into the scope of the problem. Another example would be the total amount of goods sold. The ideal metrics we came up with, that answer the aforementioned questions are:

- Total amount of goods illegally sold through underground markets per category
- Total number of active sellers
- The growth rates of the illegal underground market places as per total amount of buyers/sellers and total revenue.

The anonymous and secretive nature of underground markets makes it hard to have a complete overview of the goods, flowing through these markets. Even a simple question metric like the total amount of goods sold in a given year on a specific market is non-trivial to figure out. But this kind of information is crucial for security decision makers to know how to appropriately respond to the security issue.

5 What are the metrics that exist in practice?

A paper analyzed the sales on the underground market 'Silk Road' between 2011 and 2012. They discuss several metrics, some of which are considered relevant to the regulatory and law-enforcement agencies. Relevant metrics they used included [4]:

- The distribution of items per category - a breakdown of number sold goods per category clearly reflects the demand of this goods at this particular market. This breakdown of the sold goods is useful for law-enforcement agencies as it clarifies what is mainly sold on the market places.

- The probability of an item being available on the site as a function of days, where they found that a majority of items where available for less than three weeks. This indicates a reasonably high throughput of items.

- The growth of the amount of sellers.

- The probability of a seller remaining on the site as a function of days. About half of the sellers leave within a 100 days of first appearance.

- Proportion of items in the marketplace as a function of the number of sellers. They observed fairly high diversity, with each seller selling at most 1.5% of the total number of items in Silk Road.

Similar metrics can be found in another paper, presenting a long-term analysis spreading over 16 marketplaces during a period of two years (2013-2015). By using data analysis and publicly available resources, the document undoubtedly shows in detail different aspects of the entire ecosystem of the included marketplaces. A few metrics in addition to be mentioned are[5]:

- The seller volume. It is interesting to know for law-enforcement agencies what the distribution of the revenue is over all the sellers. It gives insight in whether a small group makes most of the profit or that it is more equally distributed.

- Seller survivability analysis shows the probability of a seller being active after a certain amount of time regarding the use of the different alias. The short time of existence of a seller creates difficulties for the law-enforcement facilities to build a case.

Further, an economic analysis of the online markets reveals the amount of drugs being exchanged at these marketplaces. The reported data focuses on the effect of ratings and reputation of the buyers, as well as the turnover that these platforms generate. The ratings provide a certain level of security for the buyer, which explains the rapid growth in popularity of these channels. The paper further evaluates the side effects of a platform being seized by law-enforcement and the secondary reaction that this brings [3].

6 A definition of the metrics you can design from the dataset

This section discusses several metrics that we defined from the dataset at hand. First there is a particular definition of metric that we use: "A metric is a system of related measures enabling quantification of some characteristic. A measure is a dimension compared against a standard."[1]. After analyzing the dataset with this definition in mind, the following metrics were designed:

- Total order value, per year. Besides knowing what the total amount of goods are it is also a useful metric to know the value (in USD) of all the orders on those market places. This can be used as an indiciation of the problem becoming bigger or smaller.
- Number of transactions per year. By knowing the number of transactions that take place in those markets every year helps by gaining insight in the scope of the security issue. This through an understanding of the amount of trade that goes through those markets.
- Number of active buyers, per marketplace, per year. While a focus on the goods and transactions is good, the people actively enabling those markets should not be left out. Depending on the time a good insight can be gained in how actively markets are being used, to prioritise further actions to be taken.
- Number of active sellers, per marketplace, per year. Just as with the number of active buyers, the active sellers also enable trade on those markets. Gaining insight in the number of them around helps to prioritise as a law-enforcement agency what to deal with first.

7 Evaluation of metrics

We use data analysis with the help of the Python programming language to create plots in order to evaluate the metrics. It is of essential importance to evaluate the metrics to gain a better understanding of their usability for the law-enforcement agencies in deadline with the security issue outlined in this report.

Total order value, per year

The total order value can be used as metric by the law-enforcement agencies to assess the scope of the security issue. The bigger this number becomes, the more trade occurs on the marketplaces and thus the security issue is becoming a bigger problem. Figure 1 shows the metric as created using the provided datasets. From this it seems the total order value is declining, which could mean the security issue is decreasing, or that traffic has moved to other markets.

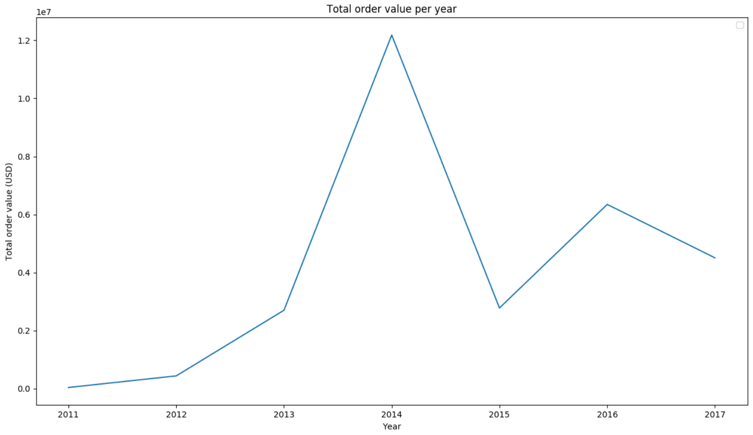

Figure 1: Total order value, per year

Number of active buyers, per marketplace, per year

The number of active buyers participating in those markets can be used, in combination with the number of active sellers, to get a clear picture of the activity of those markets. As can be seen in figure 2 the number of active buyers is not that large and even decreasing. This metric can be used by itself but also in combination with others to define a new activity metric.

Number of active sellers, per marketplace, per year

As aforementioned, in combination with the metric for active buyers it could be combined in a metric regarding the activity on the markets. Figure 3 gives insight in how actively goods are sold in terms of the number of sellers. It seems that the number of sellers either decreases or remains stable. There is a limitation of this metric, which used the $giver_hash$ in the $feedbacks$ table to calculate the number of active sellers. Some markets use a single hash to define the giver, which means that there is no data of them in the figure.

Number of Transactions per year

Looking at "Number of Transactions per year" 4, we compare the given markets on absolute values of the transactions during a period of several years. This quantity metrics of the total sold items are important indicator as it concerns the size and importance of the markets amongst users midst the period. The more transactions and financial exchanges there are, the more substantial are the markets. Formally, this demonstrates the statistical accuracy that supports the prediction of the influence of the markets and would be a starting point for a

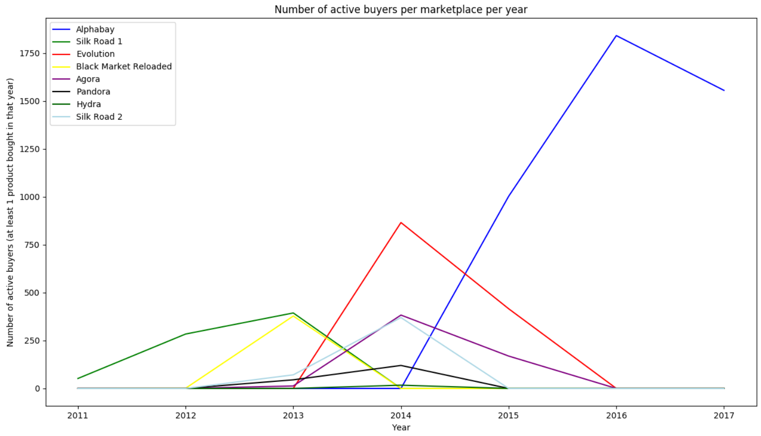

Figure 2: Number of active buyers, per marketplace, per year

security officer or law-enforcement advisor to take into account the significance of a certain market and initiate actions against it. From our given datasets the biggest markets are considered: Silk Road 1, Silk Road 2, Evolution and Agora, as well as Alphabay, so we can conclude that the biggest threat to the security would come from the biggest and most popular platforms. A possible explanation between the drop of transactions closing of some of the markets,

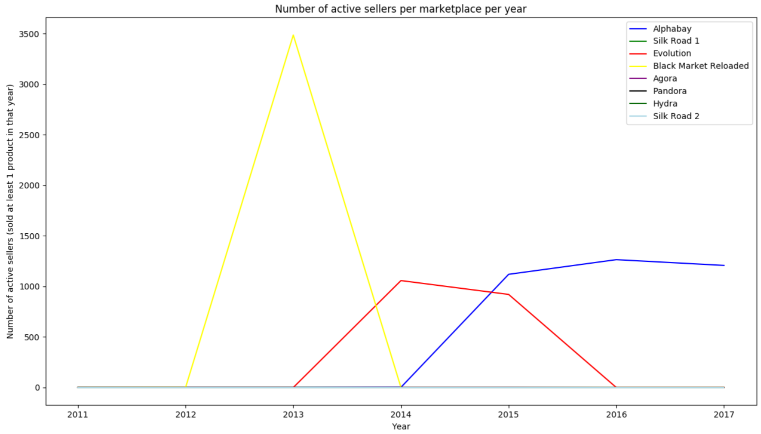

Figure 3: Number of active sellers, per marketplace, per year

but is an indication to the security officers that some markets transformed or moved to another place.

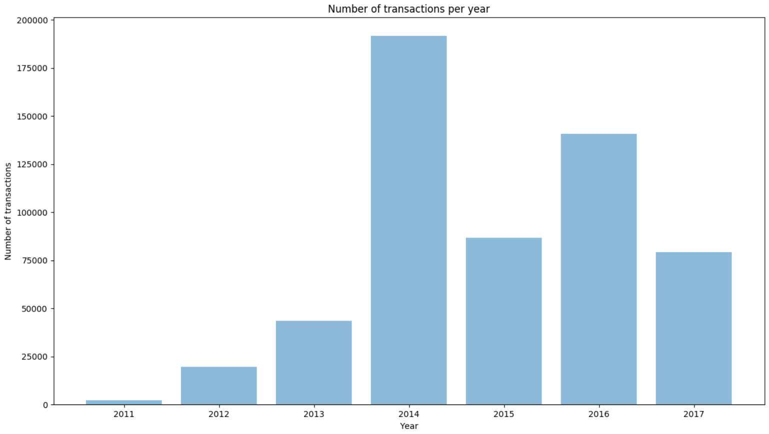

Figure 4: Number of Transactions per year

8 Conclusion

Different metrics can be derived from the dataset provided, with some overlapping the ideal metrics that were defined earlier in this paper. It is important for law-enforcement agencies to understand the scope of their security issue and to have multiple metrics they can use to quantify certain characteristics of the issue at hand. The metrics designed and evaluated in this paper allow the quantification for those agencies of characteristics that those markets have. It helps to understand the activity of markets but also to understand the amount of trade that is occurs by looking at the number of transactions, the value of all orders and the total amount of goods that is being traded. Our metrics will aid law-enforcement agencies to answer the questions they have to make the right security decision in this matter.

References

[1] Z. Abbadi. Security metrics.

[2] H. Asghari, M. Van Eeten, and M. Bauer, J. *Economics of Cybersecurity*. Edward Elgar Publishing, 2016.

[3] V. Bhaskar, R. Linacre, and S. Machin. The economic functioning of online drugs markets. *Journal of Economic Behavior & Organization*, 2017.

[4] N. Christin. Traveling the silk road: A measurement analysis of a large anonymous online marketplace. In *Proceedings of the 22nd international conference on World Wide Web*, pages 213–224. ACM, 2013.

[5] K. Soska and N. Christin. Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 33–48, Washington, D.C., 2015. USENIX Association.