Cybercriminal Markets

Economics of Cyber Security Assignment Block 2

Erin Bartholomew, Marrit Hoppenreijs, Christian van Bruggen, Sarah Vetter

Delft University of Technology

Abstract. Cybercriminal activities are often transitioned via underground forums. deliver valuable data**.** By developing incident-focused metrics, law enforcement can learn more about trends in cybercrime activity both in the physical and digital world.

Keywords: cybercriminal markets, underground forums, security metrics

1 Introduction

The Internet has been one of the fastest-growing areas of infrastructure in history. Today, information and communication technologies are essential for our everyday lives. The trend towards digitalization and internet comes not only with advantages but with risks and challenges [1]. While technology increasingly became more advanced over the years, its misuse, especially in form of cybercrime, has progressed at pace [2]. Underground forums are a manifestation of the risks that come with the growth of the Internet.

1.1 Background of Underground Forums

Cybercriminals frequently use underground forums to purchase and sell goods in support of their criminal activities [3]. Due to the wide array of questionable and illegal activities, underground forums deliver valuable information to understand cybercrime and estimate its scale [4]. Because of the amount of illegal activity and the wealth of information these forums maintain, access is tightly controlled. Accounts are often only provided to those who have proved themselves or have a relationship with another person who is already a member of the forum, which is also known as vouching [5]. Furthermore, account ownership itself is anonymous, and forum access is almost always encrypted, making it impossible to track visitors to the sites. Because of this, sales are also conducted anonymously and generally with encrypted payment methods, such as Bitcoin. The anonymity of underground forums is one factor that has led to their growing popularity, making studying these forums essential to monitoring and preventing cybercriminal activities. However, this anonymity makes it difficult to monitor activities, handle fraud, or track users efficiently and effectively.

Further complicating any monitoring efforts is the often-transient existence of many underground forums. Forums are regularly taken down by police efforts or by site administrators, themselves, both due to discovered security leaks and scams perpetrated by administrators [6]. Because of these characteristics, cybercriminal markets represent a significant challenge for any security organization. They have limited resources (manpower and budgetary) and work on complex investigations with technical challenges of following cybercriminal activity through the internet.

The need to address those challenges is expressed in a recently published Regulation of the European Parliament and of the Council [7], focusing on its Cybersecurity Strategy. An evaluation by the European Commission, regarding its ENISA strategy, showed that a majority (88 percent) of the respondents consider mechanisms and instruments available at EU level as insufficient or only partly sufficient to address current cybersecurity challenges [8]. However, there is little research to develop comprehensive security metrics of underground forums and cybercriminal activity therein.

1.2 Method

The aim of this project is to look at the data from the perspective of a national government-based security organization. In most government-based organizations, resources to start an investigation are scarce. Thus, it is important to develop proven metrics that effectively and efficiently reveal patterns and key information about cybercriminal activity on these forums.
To address this need, this paper will analyze the existing security metrics in practice, define ideal metrics, and evaluates a dataset of underground forums. In chapter 2 of this paper, the security issues of cybercriminal markets and the perspective of a national government-based security organization are defined. A set of ideal metrics based on a world of perfect data and understanding is defined in chapter 3, followed by an exploration of the metrics used in practice in chapter 4. Chapter 5 defines metrics based on a provided set of data, which are evaluated in chapter 6. The paper closes by describing limitations of developing metrics for data from underground forums and will discuss any conclusions that can be made.

2 Security Issue of Cybercriminal Markets

The growth of cybercriminal markets is often reasoned by its ease of availability and use, low cost of tools and services are contributing to the growth of these markets. From the perspective of a national government-based security organization there is a keen interest to keep illegal goods from entering the country. They actively monitor criminal activities on the underground markets to combat cybercrime and ensure national security.

National security can be an ambiguous concept if used without specifications and therefore the security conceptualization of Baldwin [9] will be used to determine the specific security issue of the cybercriminal undergrounds. Baldwin characterized security as “a low probability of damage to acquire values” and, its most general sense, in terms of two specifications: security for whom? and security for which values?

2.1 Security for whom?

The question of “security for whom” refers to the stakeholders who are involved in the cybercriminal markets. Benenson, [10] defines in his paper three groups who are acting in cyberspace. First, he defines cyberspace as the landscape of cybercrime; cybercriminal underground markets. The actors are categorized as follows: attackers, users and investigators and will be explained in context of the cybercriminal underground markets.

- The *attackers* are human that act in an offensive manner. In the case of the cybercriminal undergrounds, the attackers are the cybercriminals, since they commit a crime by purchasing and illegal products in the cybercriminal markets (cyberspace).
- The *users* are the people who are acted upon and suffer from the actions of the first group. There are also called the victims. In terms of the cybercriminal market, the type of users could be defined in two types: the internet user or the Dutch citizens. Both of them are indirectly suffering from the cybercriminal markets and depending on the product type that will be explained in section 2.2.
- The *investigator* is a human who is trying to understand and investigate the activities of the attackers and users. This could be security researchers form academia or law enforcement agencies. In this we will be focusing on the law enforcement agency, namely the National High Tech Crime Unit (NHTCU) of the Dutch National Police.

2.2 Security for which values?

This paper focus on the values of the users. As mentioned in section 2.1, there are two types of users (internet user and Dutch Citizens) depending on the product. The products and services which are bought and sold on these underground markets can be categorized into information and resources. Information can be stolen credit cards, ID scans, email accounts with stolen credentials. Resources are exploit kits, drugs and weapons, among other illegal products. [11].

The 'information' products affect the *internet users*. A cybercriminal will steel information from an internet user in order to sell it on the underground market. The cybercriminal market is therefore causing an indirect effect on the internet users. The value of the internet user are their financial resources, privacy and identity that might be stolen by a cybercriminal.

The 'resource' products, such as drugs and weapons, can result in damaging or harming a citizen physically. Drugs increase crime and thereby harm to the Dutch citizens physically. The value of the Dutch citizens is their physical well-being.

Concluding, the values of the users are their financial resources, privacy, identity and physical well-being depending on the type of product.

3 Ideal metrics

Based on the previous chapters it is given that security has a value. Depending on the relevant decision maker, the value varies and is highly relevant to be measured. According to the European Network and Information Security agency the security and reliability of internet and electronic communications are a central part of the economy and society, because incidents are able to largely impact them [12]. As described in 2.1 there are different kinds of stakeholders of its security. This paper focuses on the perspective of both physical and digital users, affected by security issues of underground forums. To measure the security ideal metrics are necessary. In order to justify security investments via a cost-benefit analysis Rainer Böhme [13] proposes a model to measure security investments against security metrics. The framework consists of two steps: the cost of security is scaled by security level and afterwards scaled to its benefits. The model is used to determine which metrics are ideal for investigating in commerce-related underground threats. This framework describes four types of metrics that act as latent construct for the level of security in an organization. These four types are: controls, vulnerabilities, incidents and (prevented) losses. The different types of metrics will be explained and thereafter will be explained which of the metrics fit the cybercriminal market project.

Ideal metrics include tracking of specific accounts and overall activity over the period of collection, with comparison of normalized and unnormalized activity over time periods that overlap between forum collections.

- Controls: These are the measure that are put in place to mitigate risk. It looks at whether is it in place and meet the specifications. There are different types of controls, such as physical (door locks), organizational (incident response team), procedural (credentials policy) and technical (data encryption, firewalls).
- Vulnerabilities: Vulnerabilities are metrics that evaluate how these controls perform considering a certain threat scenario. It focuses on hypothetical attacks.
- Incidents: Events where security is compromised in some form. The controls meet actual attacks instead of potential attacks.
- (Prevented) Losses: The data focused on commerce-related threads (or the buying of selling of goods or services). It includes data about product type, price etc...

Every transaction (selling and buying) in the underground market is an actual attack and includes the threat environment. Therefore, the transaction could be defined as an incident and the amount of transaction gives the incident rate. By tracking the incident rate over time, we could determine if a certain policy has an effect on reducing the underground transactions.

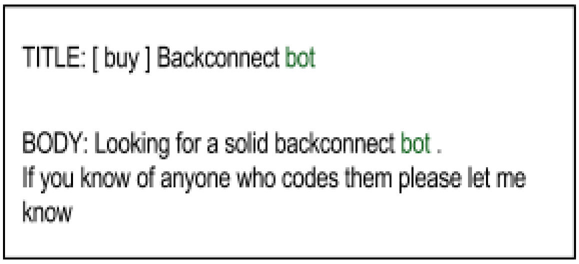
For this reason, the ideal framework would be the incident matrix. Incidents provide important feedback regarding where to allocate your resources. However, with an incident matrix it is difficult to predict and forecast which transactions will come. Therefore, we need metrics that not only focus on incidents, but (to a lesser extent) also on controls and vulnerabilities. These metrics are called the hygiene metrics and are strong predictors of actual infection rate.

To trace and measure the scale of incidents of sales, transactions made via underground forums need to be monitored. To do so, certain metrics need to be available, accessible via an up-to-date database. Most of the metrics are deducted from the Cyber Security Incident Report Form [14] as well as the ENISA Technical Guideline on Security Measures [12]. Those metrics are:

- Incident details: Those metrics help to determine the incident and its scope. For example, date, time, location of affected site, what/where/when it happened, description of the incident, incident category, classification level of the security issue, whether foreign countries are involved, estimated injury level, affected organizations, incident status, report of incident to authorities.
- Mitigation actions: the status of mitigation actions help to determine which actions need to be taken once the incident is reported.
- Assets in scope: The determination of the assets in scope support assessing all secondary assets involved in enabling the incident, e.g. base stations, routers, registers, critical assets, key personnel, third parties and outsourcing.

4 Metrics in practice

In practice, developing security metrics that analyze activity on underground forums can be challenging. Data regarding cybercrime is fragmented, often due to an inability to collect complete data or a debate about how to define which posts should be considered criminal acts [15]. Furthermore, this data is often collected as plain text forum entries that have a format similar to what is shown in Figure 1, below. This data must be parsed for key features, such as the username, date, product, price, type of post (for example purchasing or sales). Only after the data is processed is it available for analysis.



TITLE: [buy] Backconnect bot

BODY: Looking for a solid backconnect bot .
If you know of anyone who codes them please let me know

Figure 1: Example of a post scraped from one underground forum

Both security organizations and academic groups have developed metrics to track incidents of sales that represent a threat to security. One such study is described in the Tools for Automated Analysis of Cybercriminal Markets Report by Portnoff et. al. [2]. This study focused on developing tools to parse raw forum data, but also demonstrated the effectiveness of using their parsed data to monitor incidents using metrics. Using a different set of data that covered 4 underground forums throughout several years, this report developed the following categories of posts:

- Post Type. Determines the nature of the post, specifically, whether it is an offer to buy, offer to sell, offer to exchange currency, or a post not related to trade.
- Product. Determines the product being offered or requested (buy/sell posts) or the currencies being exchanged (currency exchange posts).
- Price. Extracts the price offered in commerce (buy/sell) posts or the exchange rate (currency exchange posts).

These categories and corresponding analysis tracks activity on each forum over the period in which data was collected. These categories were used to develop incident metrics that led to the following conclusions:

- Using the post type and product categorization and rule analysis to determine which sales posts indicate sales of bulk and often hacked accounts.
- Using the post type, product, and price categories together, metrics were developed to track patterns in currency exchange requests, for example bitcoin for PayPal or bitcoin for bitcoin, or PayPal/bitcoin to credit card exchanges.

Another study used information from underground forums to monitor prices of sales of fraudulent social media accounts, including Twitter, Facebook, Google, and Yahoo [16]. This report analyzed data over 10 months, to develop incident-based metrics which revealed the sale of fraudulent Twitter accounts over that period. This included the following:

- Calculating merchant sales over the entire period, to determine the large players in the sale of fraudulent Twitter accounts.
- Track price trends and time between offer and sale of fraudulent Twitter accounts

The authors of this study partnered with Twitter to further track the fraudulent accounts, developing metrics that analyzed the IP address of activation, track patterns in fraudulent registrations, and more. In addition, and in cooperation with Twitter, authors used the information on fraudulent account sales to shut down the discovered accounts. The data gathered can also be used to determine the efficacy of barriers a social network company like Twitter put in place to reduce the number of fraudulent accounts being created.

Data from underground forums that is relatively recent can also be used to track potential losses, based on patterns in communication between forum members, as was demonstrated in a study "Exploring Threats and Vulnerabilities in Hacker Web" [17]. This study examined contents from underground forums to develop metrics that track posts that mention several subjects, including sales of stolen credit card data, posts referring to specific financial institutions, and requests for hacking services. These metrics were used to identify recent, current, and near-future threats to information. Apart from describing analysis completed on data from underground forums, this study also focused on the challenges involved in collecting data from such sources in the first place.

Finally, a study completed at the University of San Diego, examined data from six underground forums [16]. Instead of metrics that analyze trends over time, this study focused on analysis of relationships between buyers and sellers. This enabled the authors to gain a better understanding of the forces shaping cybercrime on underground forums, including how price, trust, and customer service influence relationships and therefore the nature of exchanges on. These conclusions can be leveraged by law enforcement to identify key users on a forum and to develop methods to interrupt trust relationships and reduce the amount of cybercriminal activity on a forum.

This is not a comprehensive review of all analysis that has been completed with data from underground forums. However, several points of commonality can be discovered. First, that data from forums requires extensive natural language processing to format the data in a form ready for analysis. The second is that most analysis, at least that is not confidentially held, focuses on tracking incidents and trends that happened in the past, frequently involving forums that are no longer active. The nature of data collection from these forums means that analysis is only possible using old postings. Furthermore, the nature of official government-sponsored investigations into these forums means the analysis involved in security efforts is kept confidential and not made available for wider study.

5 Applied metrics

The dataset used for this report is a confidentially sourced database that has already undergone extensive natural language processing, with data on user history, product, shipping to and from location, price, feedback from sales, and other information delineated in an SQL database. The focus of this section will then be on defining and analyzing metrics that can be applied using this specific dataset. Due to confidentiality reasons, we cannot provide access raw data, but only the results of our analysis.

5.1 The dataset

In order to elaborate metrics of measurement of cybercriminal markets and to address the security issue, a large-scale dataset is used in this research. The data used for this analysis was taken from seven marketplaces over a 4-year period, stored initially as a relational database [6]. Details of the seven marketplaces are as follows:

- Silk Road 1.0, an underground marketplace started that was active from 2011 to 2013, when the Federal Bureau of Investigations shut it down. Data for this marketplace was collected from June 2011 to October 2013.
- Silk Road 2.0, online immediately following the takedown of Silk Road 1.0 in 2013 and online until its own shutdown in 2014. The Silk Road 2.0 dataset was collected from November 2013 until October 2014.
- Agora, an underground marketplace founded in 2013 and taken down by its own administrators in 2015. Data from Agora was collected from December 2013 to February 2015.
- Black Market Reloaded, a marketplace active at the same time as Silk Road 1.0, which took on much of the traffic from Silk Road 1.0 after its closure. Black Market Reloaded was closed by its administrators in early 2014 as it could not handle this sudden influx in traffic. Data was collected from this site from February 2013 to December 2013.
- Pandora, one of the largest underground forums in 2014 that experienced multiple scams and phishing attacks. Data was collected from this forum from June 2013 to October 2014
- Hydra, an underground forum that traded primarily in drugs and narcotics and was shuttered in the same effort that shut down Silk Road 2.0. Hydra data is from April 2014 to October 2014.
- Evolution, opened in 2014 and grew steadily in the wake of the closure of several underground forums in 2014. The site was closed by its administrators in what is known as an exit scam, where administrators shutter the site and steal millions in bitcoins it was holding in escrow. Data was collected from Evolution from April 2014 to October 2014.

Figure 2 shows the overlap of data collection periods from each of the seven marketplaces captured. It demonstrates the limited and sometimes nonexistent overlap periods between the analyzed datasets.

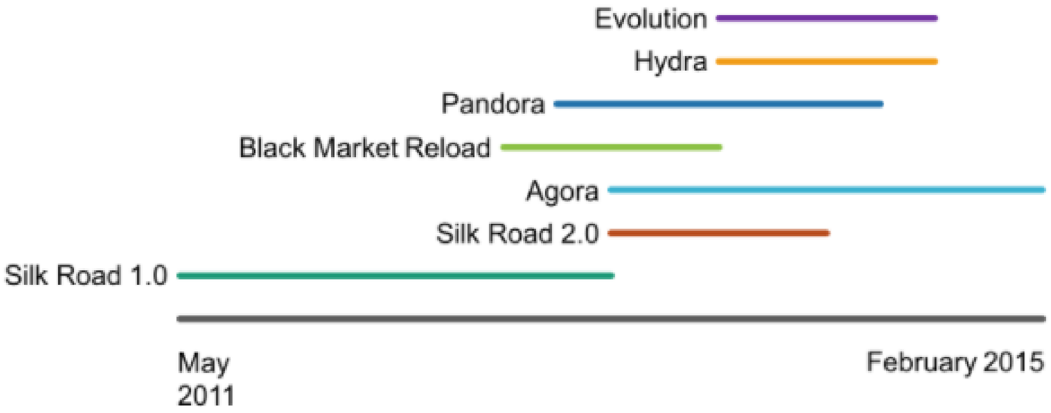


Figure 2: Timeline of forum data collection

The data collected was parsed and formatted into the following four tables, which can be used for further analysis:

- Items: containing information regarding the sold items, such as the marketplace, description, product category, and total sales.
- Feedback: containing data provided via feedbacks on purchases, such as the feedback text itself, the order amount, and date of feedback
- Marketplace: contains information about the marketplace platform, including name and total sales over the time period of data collection
- Users: details about individual user accounts, including purchase and sales histories

5.2 Metric Definition and Evaluation

Using the discussed ideal metrics, as well as those that have been shown to be used in practice and in other research, and keeping in mind the dataset used in this report, we have developed the following metrics. There was some additional processing when grouping several country names such as ‘The Netherlands’ and ‘NL’.

Metric 1: Sales by volume of product
First, to determine what type of sold products to focus investigations on, examine what accounts have generated the most revenue. This metric examines relative percentages of generated revenue for certain product categories exported from a country. By using percentages, this metric is not dependent on the total number of transactions, but on normalized totals. A limitation of this metric is that only total generated revenue is known. As different products can be sold at different prices, it is possible for sales from one product category to be significantly higher than others due to the higher price. The total number of goods sold in this case would in reality be much lower.

Below is a representative evaluation of the metric that examines percentage of generated revenue exported from Netherlands for a product category over five years of forum data. This metric can be applied to any country's data to generate information about the source of various potentially illegal goods around the world.

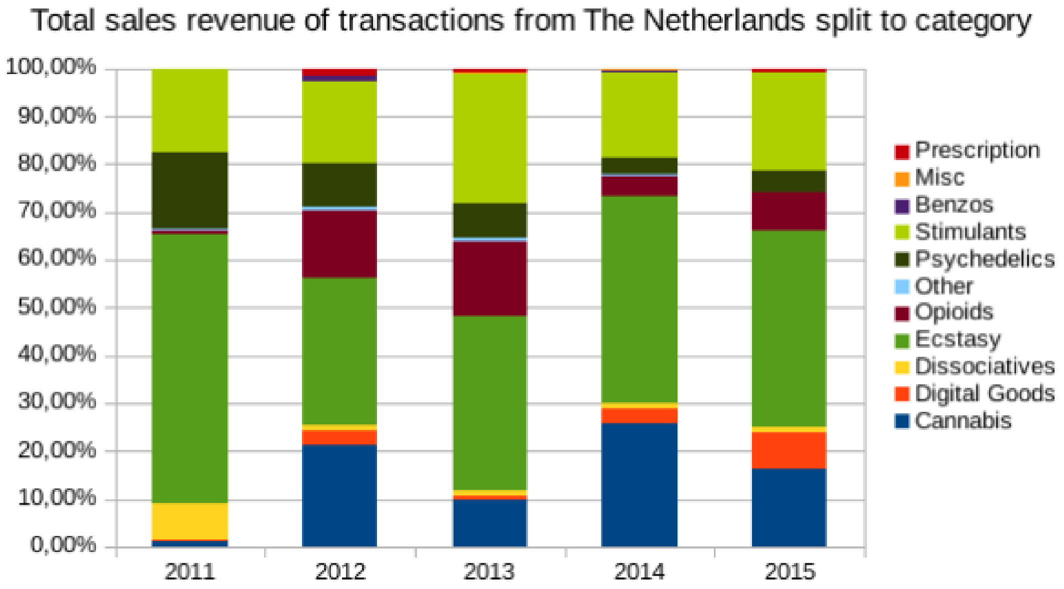


Figure 3

Metric 2: Sales revenue over time

This metric allows a law enforcement agency to examine trends in total sales revenue volume for their country, and may reveal the scope of and rate of growth of cybercriminal activity on underground forums in their country.

Figure 4, below, shows the trend of total sales revenue from transactions originating in the Netherlands over the 4-year period from 2011 to 2014. 2015 data has not been included here because there is only 2 months included in the dataset. This metric indicates a rapidly growing number of incidents of sales on underground forums in the Netherlands.

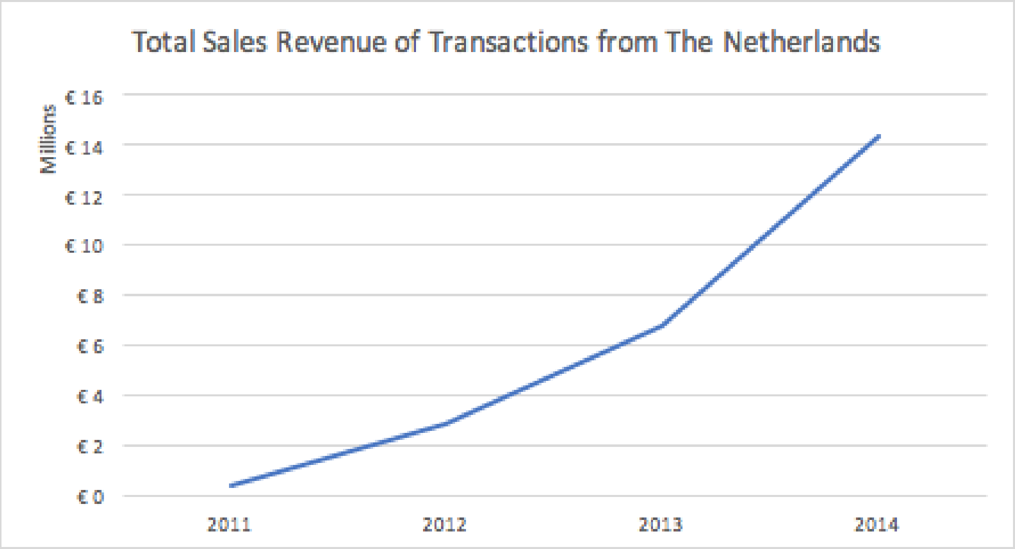


Figure 4

Metric 3: Product sales trends

This metric involves tracking sales of specific product categories over time. Based on the data provided, we can divide sales of products in several ways, including the forum the sale was conducted and the origin or destination of any goods sold. This metric will allow law enforcement to detect trends in incidents of sales of goods, which may indicate both digital and physical security vulnerabilities, depending on the type of product sold.

Below is a listing of product categories whose sales are tracked in this database:

- Benzos
- Cannabis
- Digital Goods
- Dissociatives
- Ecstasy
- Misc
- Opioids
- Other
- Prescription
- Psychedelics
- Stimulants

Note that according to this database, all digital goods are tracked in one category, despite tehre being a wide variety of digital goods sold on these forums, including bulk social network accounts, stolen credit card information, hacking tools, and more.

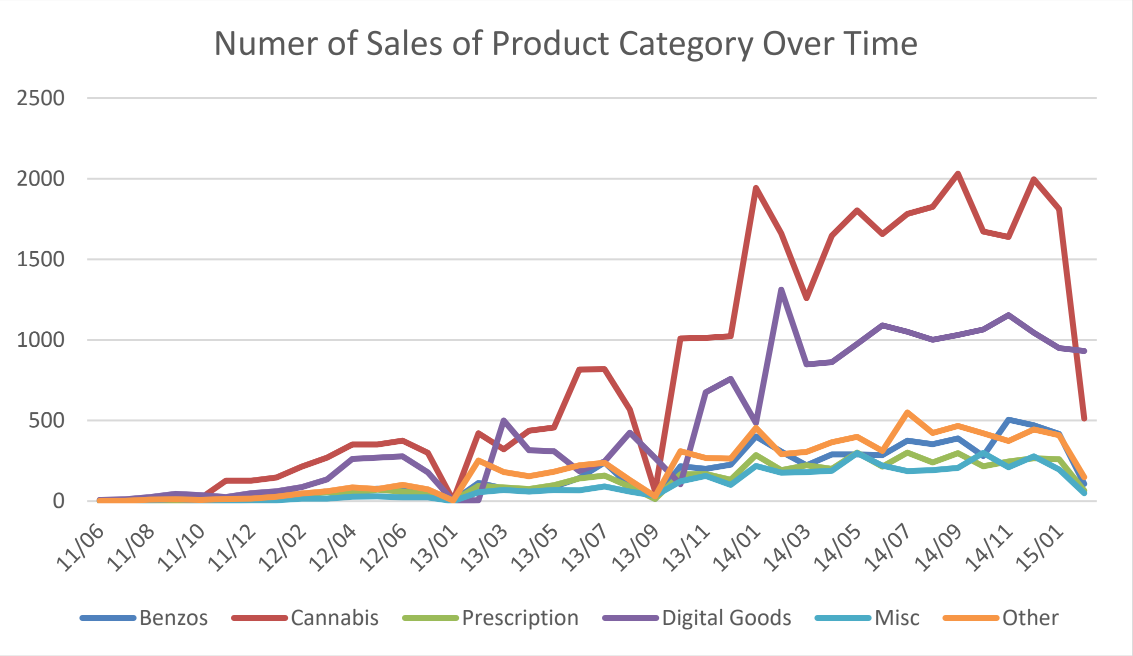


Figure 5

Figure 5, above, indicates the sales trends for six product categories from the period of June 2011 to January 2015. Data is not normalized, so it is clear that most sales are in cannabis and digital goods. For further analysis, data can be broken down into sales per forum, which can provide law enforcement with information about types of goods sold on the different underground forums in addition to trend data.

These three metrics are a small number of what can be developed using the confidential dataset provided to us. For example, the trust relationships between sellers and purchasers can be analyzed using information found in the Feedbacks database. This will enable law enforcement to determine key sellers in a forum, as well as purchase patterns by specific users.

6 Limitations

Using data from underground forums to develop security-based metrics of cybercriminal activity has several limitations. First, as discussed earlier in this report, information is often retrieved in plain text form and must be processed before it is available for further analysis. This processing is impossible to do manually, so natural language processing algorithms must be developed that, when applied, can lead to errors in recognition of important information in a post. Spelling errors, variable placement of information, and other factors can make these algorithms difficult to develop, as well.

What's more, much of the data available for study is only retrieved from forums that are no longer active, meaning data retrieved refers to incidents that have occurred, sometimes months or years, in the past. This, along with the fast pace that cybercrime often moves at, makes it likely that any trends or information gathered is no longer relevant to the current environment.
The final major limitation to be discussed in this report is based on the research completed by Noroozian et. Al [18] regarding the problems of analysis using noisy and heterogeneous datasets. Data from underground forums matches the type of data described as problematic for use in analysis in this paper. Data from underground forums is often incomplete, includes a large amount of extra information is not applicable for analysis, and is extremely heterogeneous. Each of these issues must be addressed when developing metrics and interpreting analysis for such a dataset.

These limitations demonstrate that analysis done using data from underground forums must be undertaken carefully to ensure that results are an accurate representation of the real environment.

7 Conclusion

To sum up, underground forums provide rich datasets to track and measure cybercriminal activities. However, the datasets available require a large amount of preprocessing before they can be evaluated and information to understand the scale of the security issue can be retrieve. Furthermore, the collection of data from underground forums is limited, due to the noisy and heterogenous datasets. The dataset can be used to analyze previous trends in cybercriminal markets, to be able to gather an understanding of the key interests of cybercriminals and threats to the users. Nevertheless, the data available comes from forums no longer active, which makes it hard for national security organizations to capture current trends to keep up with current security issues.

Based on the dataset given and analyzed in this paper, three metrics measuring cybersecurity issues were defined. First, the sales by volume of product, to determine the focus of investigations on those with the most revenue. Secondly, the sales revenue over time, allowing law enforcement agencies to examine trends in total sales revenue volume for their country. And thirdly, sales trends can be gathered by product categories; enabling law enforcement agencies to detect trends in incidents of sales of products, indicating vulnerabilities, both digital and physical, depending on their type.

Overall, cybercrime in underground forums is an emerging challenge, continuing to grow alongside technological developments. Therefore, it is necessary to set law enforcements and tracking capabilities as the key focus of national organizations regarding cybercrime. Keeping in mind, that it is nearly impossible to eliminate cybercrime completely. As long as there is a demand for cybercriminal activities, cybercriminals will continue to find ways to distribute their services.

References

[1] M. Gercke, “Understanding cybercrime: Phenomena, challenges and legal response,” 2012.

[2] R. S. Portnoff *et al.*, “Tools for Automated Analysis of Cybercriminal Markets,” *Proc. 26th Int. Conf. World Wide Web - WWW ’17*, pp. 657–666, 2017.

[3] R. Downs and V. Ray, “Exploring the Cybercrime Underground: Part 1 – An Introduction,” Palo Alot, 2016.

[4] G. Durrett *et al.*, “Identifying Products in Online Cybercrime Marketplaces: A Dataset for Fine-grained Domain Adaptation,” *Proc. 2017 Conf. Empir. Methods Nat. Lang. Process.*, pp. 2588–2597, 2017.

[5] M. Motoyama, D. McCoy, K. Levchenko, S. Savage, and G. M. Voelker, “An Analysis Of Underground Forums,” *Proc. 2011 ACM SIGCOMM Conf. Internet Meas. Conf. - IMC ’11*, p. 71, 2011.

[6] A. Gopalakrishnan, “Traversing Underground Economy For Hacker-Goods,” Amsterdam, 2017.

[7] European Commission, “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the ‘EU Cybersecurity Agency’, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (’’Cybersecurity Act’’),” Brussels, 2017.

[8] ENISA, “ENISA Strategy,” 2016.

[9] D. A. Baldwin, “The concept of security,” *Rev. Int. Stud.*, vol. 23, pp. 5–26, 1997.

[10] Z. Benenson *et al.*, “Exploring the Landscape of Cybercrime,” in *2011 First SysSec Workshop*, 2011, pp. 71–74.

[11] S. Khandelwal, “AlphaBay Shut Down After Police Raid; Alleged Founder Commits Suicide in Jail,” 2017. [Online]. Available: http://thehackernews.com/2017/07/alphabay-darkweb-alexandre-cazes.html. [Accessed: 25-Sep-2017].

[12] ENISA, “Technical Guideline on Security Measures,” 2014.

[13] R. Böhme, “Security metrics and security investment models,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6434 LNCS, pp. 10–24, 2010.

[14] “MULTINATIONAL INDUSTRIAL SECURITY WORKING GROUP,” 2013.

[15] C. Hargreaves and D. Prince, “Understanding cyber criminals and measuring their future activity: Developing cybercrime research,” *Secur. Lancaster Secur. Featur.*, pp. 1–38, 2013.

[16] T. J. Holt, “Examining the Forces Shaping Cybercrime Markets Online,” *Soc. Sci. Comput. Rev.*, vol. 31, no. 2, pp. 165–177, 2013.

[17] V. Benjamin, W. Li, T. Holt, and H. Chen, “Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops,” *2015 IEEE Int. Conf. Intell. Secur. Informatics Secur. World through an Alignment Technol. Intell. Humans Organ. ISI 2015*, pp. 85–90, 2015.

[18] A. Noroozian, M. Ciere, M. Korczyski, S. Tajalizadehkhoob, and M. Van Eeten, “Inferring the Security Performance of Providers from Noisy and Heterogenous Abuse Datasets,” 2017.