Underground markets: Security Metrics

Course: WM0824 Economics of Cybersecurity
Date: 15-09-2019

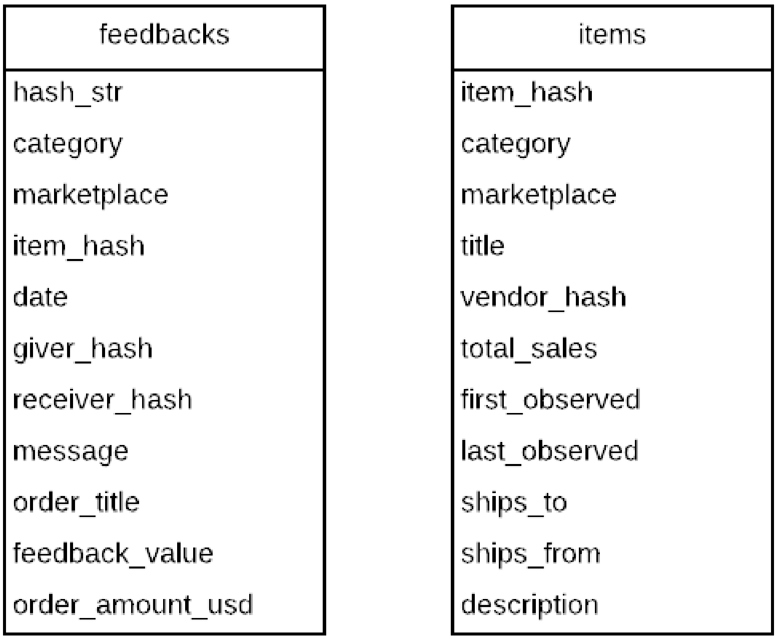
Veroniek Binkhorst - 4276620
Rowdy Chotkan - 4570243
Björn Ho - 4320867
Swaathi Vetrivel - 4900863

- NOTE: We decided to make two "*What security issue does the data speak to"* sections and shall remove one in discussion with you. We could not come to a conclusion as what road to take.

Table of Contents

Introduction

During the lectures we have learned the importance of measuring cyber security and the difficulties to determine the right metric. These metrics are used to prove how security activities affects security goals and help us make the right security decisions. In this report we put this idea into practice and we look into the data of underground markets by examining the data for the project *16_underground_markets*. The project consists of a dataset of given information regarding underground markets. The dataset 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

These columns encapsulate data on sales with item titles and prices, however no specific information on sellers or buyers, apart from hashes. All these transactions have taken place on specific underground markets and contain mostly illegal items such as drugs or stolen credentials. Two security issues the data speaks to will be discussed in the next sections.

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

What security issue does the data speak to (I)?

The database contains information regarding the usage of underground markets.
The main security issue identified from the perspective of the users of the platform regarding the hashes used: the hashes are not unique. This entails easily tracking cash flows between vendors and items. Transaction information can be linked to specific persons, and once the persons are identified and located, severe consequences might follow.

Whose security?

The users that are using the black markets and the owner(s) of the platforms. Once a database gets leaked, the people involved in illegal activities might get prosecuted. Users' personal information might also end up in the hands of malicious persons like criminals.

Security of which values?

The main values in risk are privacy and personal safety. In case of a privacy breach the information the users could be linked to personal information (e.g. names and email) as was the case in the article by Leswing (2017). As a consequence of privacy, personal safety gets put in jeopardy when personal information gets leaked. As was the case as reported by Joseph (2017).

Security from what?

The main threat here are law enforcement agencies and other users on the platforms. These black markets gain attention from law enforcement agencies because of the illegal activities. Other users is also a threat because sellers might scam buyers by not delivering the promised products or services and they might try to retaliate. And once the identities are known from the sellers, they might get doxed by other users, as reported by Joseph (2017).

Incentives

Due to the information asymmetry between the buyers and sellers in underground markets, there exists a two-tier underground economy, one tier that has an incentive to scam buyers and the other that is more organized to avoid being duped (Herley and Florêncio, 2010). The tier with incentive to cheat would tend to be comprised of new buyers with little or no familiarity with the system. Since the deals on the underground markets are by definition illegal, there is no reprimand possible for sellers that scam and their profit margins on these transactions would be high. This, in turn, also provides a higher incentive for them to cheat. The other tier organizes on repeated interactions thereby building a network of trust to safeguard against scammers.

Ideal metrics

The first metric is related to investments in security. This metric is quantified as privacy protection per dollar spent.

Privacy protection / $

Based on this metric, platform owners can draw conclusions on the quantity of investments required in cyber security in order to satisfy their security needs and protect their platform.

The second metric is that of economical impact.

Economical impact in case of data breach

This metric relates to the amount of money lost for the platform owners in case of a data breach. By having this metric, platform owners can determine the best amount of money spent on security to minimize losses.

What security issue does the data speak to (II)?

The existence of underground markets poses an implicit risk to society. The data indicates that there are 44578 unique items being traded by 5585 vendors across eight marketplaces worldwide. The items can be grouped into 17 unique categories of items ranging from pirated software to malware to botnets. These transactions go under the radar and result in negative externalities, the costs of which are borne by the society. For instance, the sale of malware brings with the cost to educate society on the best possible ways to defend against it. Hence, it would be in the interests of the public to mitigate these transactions and curb the shadow economy.

Whose security?

As said the costs of the externalities are borne by society. Since shipping takes place worldwide and is not concentrated on certain areas in the world, the society consists of the whole world's population.

Security of which values?

The values at risk are safety, <>. Safety is in jeopardy because of the selling of for example illegal drugs, fireworks or guns.

Security from what?

All sellers of illegal product on black markets.

Incentives

There are inherent incentives to trading in the underground market for both buyers and sellers. While the primary incentive would be that underground markets are not regulated or monitored which allows for trading of substances that would be considered illegal by the law. Moreover, the sellers can get a higher price for their product in such a market economy that is more free and not restricted by laws and taxes. The buyers in turn also benefit by being able to purchase items that are not available on genuine markets.

Metrics in practice

Metric	**Unit**	**Description**	**Gives insight in**
Price range / item category	[€/item]	Indicates the price range for the different categories of products	The price of products

		sold	
Prevalence of categories	[%]	Indicates the size of the categories of products sold	What is sold
Average turnover / marketplace	[€/month/marketplace]	Indicates the size of the different marketplaces	What the most used platforms are
Period/item	[week]	Indicates how long an item is for sale on average	
Period/buyer	[week]	Indicates how long a buyer is active on a platform on average	
Period/seller	[week]	Indicates how long a seller is active on a platform on average	
Amount of sales per week	[number of sales/week]	Indicates how many sales on average take place per week	The increase or decrease of the amount of sales over a longer period of time
Amount of buyers per week	[number of buyers/week]	Indicates how many buyers were active on average per week	The increase or decrease of the amount of buyers active over a longer period of time
Amount of sellers per week	[number of sellers/week]	Indicates how many sellers were active on average per week	The increase or decrease of the amount of sellers active over a longer period of time

What would be the ideal metrics for security decision makers?

What are the metrics that exist in practice?

A definition of the metrics you can design from the dataset

An evaluation of the metrics you have defined. This should include graphical representations of the metrics (e.g., histograms, scatter plots, time series, bar charts).

Conclusion

References

Cox, Joseph. “The Dark Web’s Most Notorious Thief, Phishkingz, Gets Doxxed.” *The Daily Beast*, 18 Oct. 2017. *www.thedailybeast.com*, https://www.thedailybeast.com/the-dark-webs-most-notorious-thief-phishkingz-gets-doxxed

Leswing, Kif. “The FBI just took down AlphaBay, an online black market for drugs that was 10 times bigger than Silk Road.” *Business Insider Nederland*, 20 July 2017, http://www.businessinsider.com/alphabay-online-black-market-taken-down-silk-road-2017-7

Herley C., Florêncio D. (2010) Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy. In: Moore T., Pym D., Ioannidis C. (eds) Economics of Information Security and Privacy. Springer, Boston, MA