Feedback on block 2 (Metrics)

Feedback on: Group 3 - Cybercriminal Markets
Provided by: Group 1 - Vulnerabilities

Summary of the paper

Cybercriminal markets are underground forums where users can purchase and sell goods illegally. They are regularly taken down by security organizations due to discovered security leaks and scams. The paper looks at this issue from the perspective of a government based security organization which works towards national security and looks to keep illegal goods from entering the country. The attackers, users and investigators are identified as the three main actors involved in these underground markets, and the assets are financial resources, privacy and identity. Incident rate over time (incident is an underground transaction) has been identified as an ideal metric, and the rest of the ideal metrics are classified into incident details, mitigation details and assets in scope.

Existing incident metrics were developed out of the type of posts, products and their price. Another study made use of IP addresses and track patterns of registrations. A study from USD also focussed on the relationship between buyers and sellers and this analysis helped them develop methods to interrupt trust relationships and reduce cybercriminal activity. The common factors in these studies are the need for natural language processing, a strong focus on the past (especially because most markets are closed down), and the nature of government-sponsored research projects leads to classified results.

The dataset is divided into items, feedback, marketplace and users, and metrics defined for this dataset are:

- Sales by volume, split to product categories, measured for each year;
- Total sales revenue over time;
- Number of sales over time, split to product categories.

The requirement of error-free language processing algorithms, especially when the analysis is based on noisy and heterogeneous data is a major limitation here. Also, the retrieved data that is available for study is not active, meaning it is of the past and the information need not be relevant to the current scenario. Cybercrime in underground forums is in ever-increasing demand and national organizations should continue to keep this as a key focus.

Strengths

- The paper is very well structured and easy to read. The language used is excellent.
- The paper contains an in-depth and detailed explanation of the problem statement and security issue.
- The literature is very well used, and there are a lot of references.
- Proper use of actors (i.e. attackers, users, investigator).
- Suitable use of the TU Delft framework for security metrics (i.e. controls, vulnerabilities, incidents, and (prevented) losses).
- Proper normalization of metrics.
- Good explanation of the use of metrics.

Major issues

- No major issues as defined in the assessment instructions. Well done!

Minor issues

- The abstract could contain more information on the conclusions of your paper.
- In Section 2.2, the statement *"The cybercriminal market is therefore causing an indirect effect on the internet users"* seems contradictory to the listed user assets (their financial resources, privacy and identity). The compromise of these assets could have a very direct impact on the internet users.
- In contrast, also in Section 2.2, the impact of 'resource' products, like drugs and weapons, on Dutch citizens, is all directly -- it could be argued that the effects on citizens in general are mostly indirect, like nuisance or tax rate.
- Section 3 concentrates more on frameworks than about the specific metrics than help estimate security issues.
- In Section 3, a description of the incident matrix framework is missing.
- The relationship between defined metrics and the security level could be made explicit. For example: for the metrics *sales by volume of product* the question could be answered what a result on this scale would mean for the chosen perspective of the national legislator. The paper could be further improved by relating the extensive introduction and basis in theory to the developed metrics.
- In 5.2, the monetary measurement is not explained for the first metric. Although this is a normalized metric, still the measured unit is interesting: is it measured in euros, dollars, or bitcoins? And as the bitcoin exchange rates (used to) change rapidly: it this considered or even compensated for?