Assignment 2 - Economics of cyber security

An analysis of the darknet market The Real Deal

Group 6
Vishan Baldew - 4180992
Martijn Cligge - 4152220
Stephan Kool - 4151895
Christian Veenman - 4495705

DRAFT

1) Who is the problem owner of the security issue as measured in your first assignment?

In the previous assignment, several parties are discussed that are involved with crypto markets that sell cybercrime assets. With the specific focus of cybercrime assets, such as 0-day exploits, source code and accounts, the perspective of the software company whose software is exploited is interesting to take a look at. Figure 1 provides an overview of the objectives of such a company, modeled as an 'objective tree' (De haan et al., 2009).

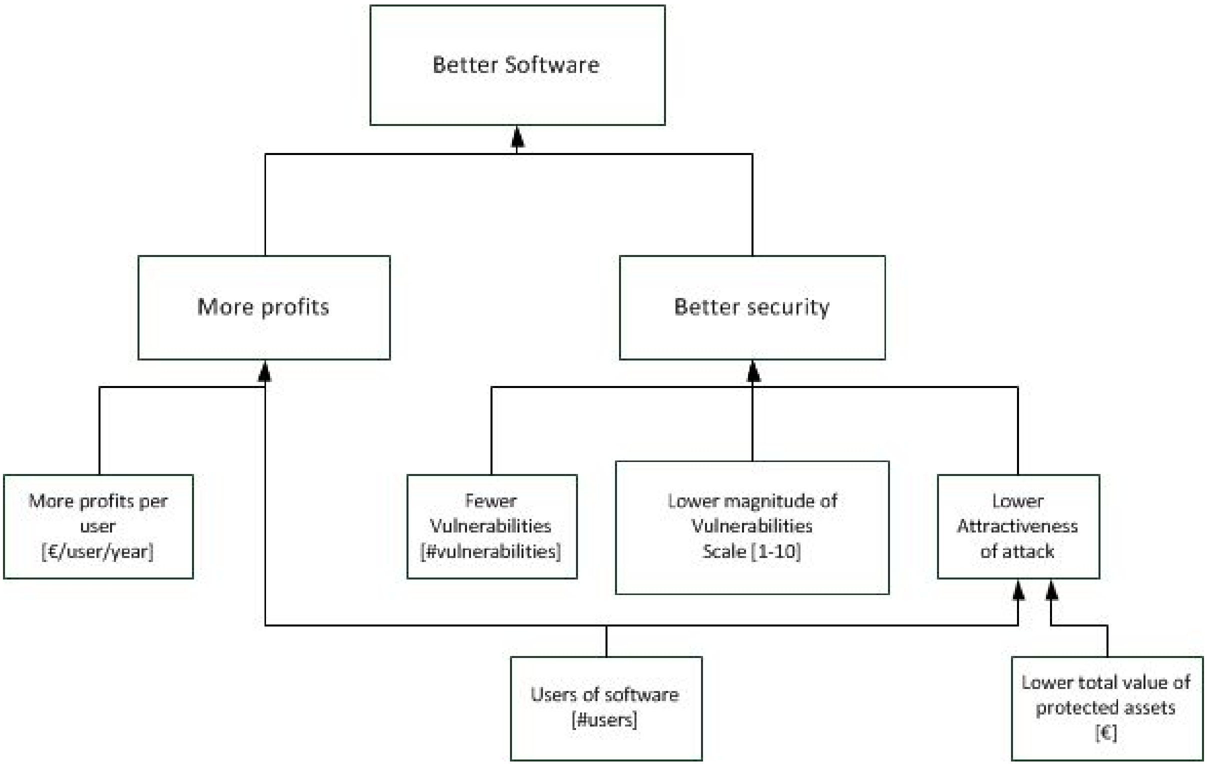
Better Software
More profits
Better security
More profits per user [€/user/year]
Fewer Vulnerabilities [#vulnerabilities]
Lower magnitude of Vulnerabilities Scale [1-10]
Lower Attractiveness of attack
Users of software [#users]
Lower total value of protected assets [€]

Figure 1: Objective tree software company

This refers to the following metrics for a software company: more profits per user, fewer vulnerabilities, lower magnitude of vulnerabilities, lower total value of protected assets and a trade off between both more and fewer users. The more users the company has, the more profits it will make (generally speaking). Yet having a high number of users also increases the attractiveness of an attack, lowering security.

2) What relevant differences in security performance does your metric reveal?

Several metrics are inferred from the dataset that is used for these assignments; a web scrape of products sold on darknet market The Real Deal. One metric is in particular interesting for software companies; the number of cybercrime assets per software company. This can be interesting, because companies can compare themselves with other companies, and a high number of available exploits can mean that there should be invested more in targeting these exploits.

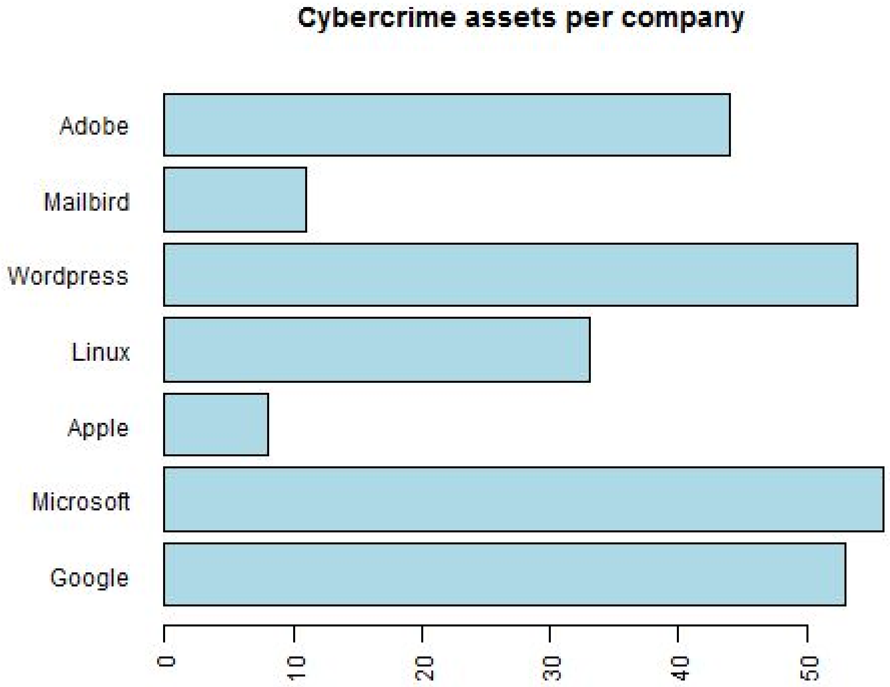

Figure 2: Number of cybercrime assets per software company

From figure 2 can be inferred that Microsoft, Google and Adobe have relatively more exploits for sale than e.g. Apple or (the much smaller) Mailbird, this can be seen as a relevant difference in security performance of the software company.

3) What risk strategies can the problem owner follow to reduce the security issue as measured in your first assignment?

The software company is on a victim of the sold exploits on the crypto web and as such uses generally defensive tactics. It can improve the security of its software continuously or take a more proactive approach and reduce the possible future attacks or even take preventive actions.

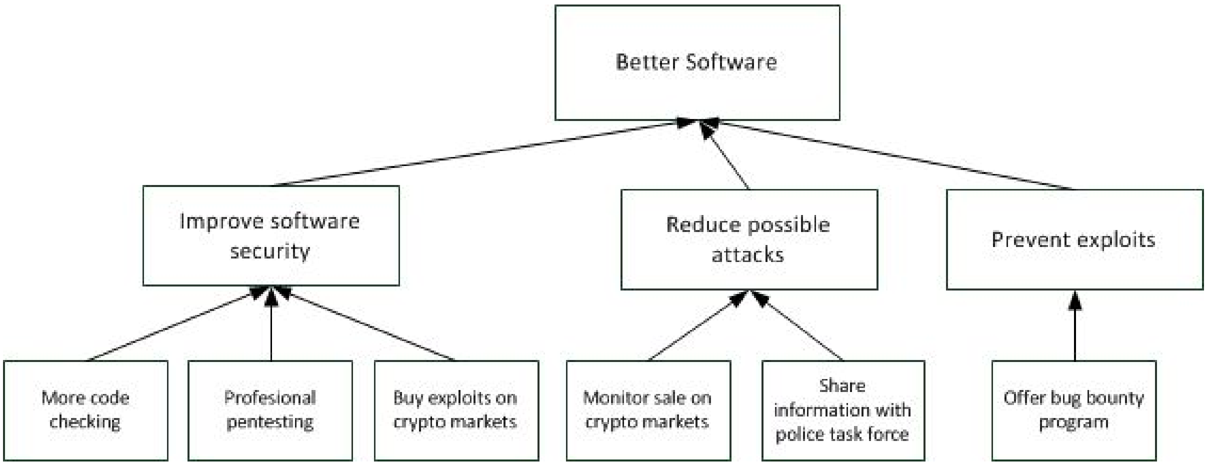
Better Software
Improve software security
Reduce possible attacks
Prevent exploits
More code checking
Profesional pentesting
Buy exploits on crypto markets
Monitor sale on crypto markets
Share information with police task force
Offer bug bounty program

Figure 3: Means-End diagram software company

To improve the security, the company itself can opt to do more code checking in order to find gaps or to hire a professional penetration tester to check on the security of the software. It is evenly possible to buy the exploits available on the crypto market in order to be able to patch the weakness the software uses. The company can also opt to reduce the possible attacks by monitoring the offers of exploits on crypto markets and sharing this information with the police task force, a stakeholder that has the legal power to act against individuals in crypto markets. Finally, the company can circumvent most of the problems of exploits arising by offering a bug bounty program which gives a positive incentive to report weaknesses in software instead of creating an exploit off the weakness.

4) What other actors can influence the security issue as measured in your first assignment?

As discussed in our previous assignment, the policy decision makers are able to affect the security issue. To be specific, apart from the problem owner, both the police task force and the crypto market operator have the ability to influence the very existence of the crypto market.

Crypto market operator

The crypto market operator has four main points of approach to improve the crypto market. He can improve the security of the crypto market customers, improve his own personal security, promote the crypto market and improve the ease of use of the crypto market.

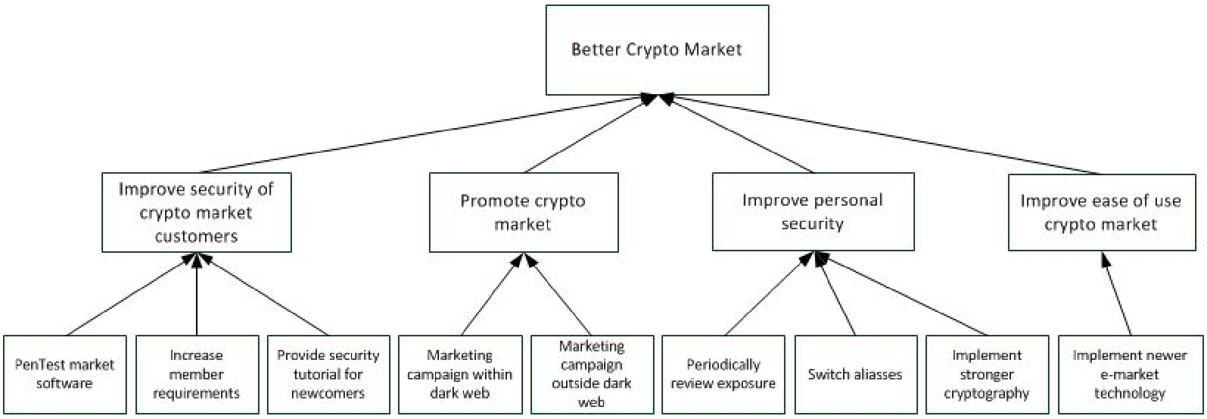
Better Crypto Market
Improve security of crypto market customers
Promote crypto market
Improve personal security
Improve ease of use crypto market
PenTest market software
Increase member requirements
Provide security tutorial for newcomers
Marketing campaign within dark web
Marketing campaign outside dark web
Periodically review exposure
Switch aliasses
Implement stronger cryptography
Implement newer e-market technology

Figure 4: Means-End diagram crypto market operator

The figure 4 above models the means the operator has for each of these main points
The means for the crypto market operator are:

- Pentesting the software that runs the market
- Increase member requirements for members
- Provide a security tutorial for newcomers
- Market the forum within the dark web
- Market the forum outside of the dark web
- Review the personal exposure of the operator in terms of traces on the internet
- Switch aliases to cover more traces
- Implement even stronger cryptography
- Implement newer e-market technology

Police task force

If the crypto market operator is the defender of the crypto market asset, the police task force (PTF) is the attacker. With the objective of reducing the illegal trade that goes through the crypto markets, the police task force has three possible points of attack: the sellers and buyers, the crypto market operators or the crypto market service environment (see figure 5)

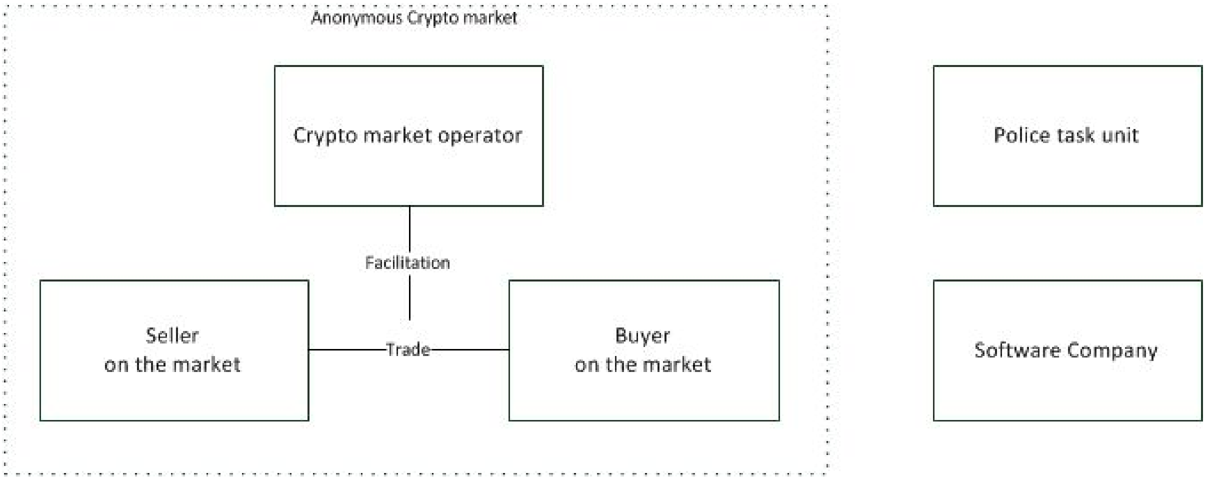

Figure 5: Formal Chart actor environment

As such, the means-end analysis of the police task force is modeled in figure 6:

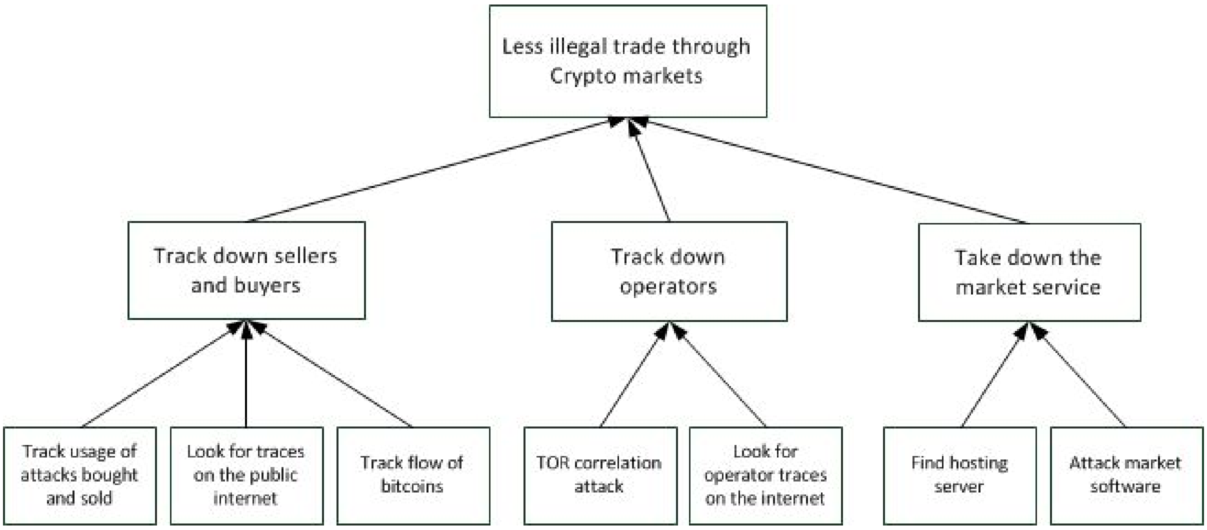
Less illegal trade through Crypto markets
Track down sellers and buyers
Track down operators
Take down the market service
Track usage of attacks bought and sold
Look for traces on the public internet
Track flow of bitcoins
TOR correlation attack
Look for operator traces on the internet
Find hosting server
Attack market software

Figure 6: Means-End diagram Police Task Force

The means of the police task force are as follows:

- Track usage of attacks which are bought and sold on the markets
- Look for any traces on the public internet that match with the traces of the buyers and sellers on the crypto market
- Track the flow of bitcoins
- Perform a TOR correlation attack
- Look for traces of the operator on the public web
- Find the server hosting the service and take it down
- Attack the software on the platform

5) *Identify the risk strategies that the actors can adopt to tackle the problem*
   a) are there actors with different strategies? why?

As explained earlier, we have three actors in our playing field. The metrics provided in the previous assignment can help the actors if and against what threats they need to undertake action. For the first actor, the software company, risk strategies that focus on reducing of the effectiveness of certain cybercrime assets will be important. In general, as explained in the lectures, the software companies do not have security as one of their core competencies since the market conditions rewards first mover with monopoly rents. So therefore it is assumable that they will adopt these risk strategies after they shipped their software: “ship today, fix tomorrow”. These strategies focus mainly on the long term. They need to make their software in such a way that security strategies could be incorporated later. If the software company does not do this, security breaches could lead to indirect costs like reputation loss. The risk strategies could focus on communication of improvements and providing patches (see figure X)..

The risk strategies of the crypto market operator are of course very different for the crypto market operator. This actor wants to facilitate a marketplace where as may cybercrime assets are sold as possible. He therefore needs to adopt risk strategies that can help increase security from his perspective against the police task unit. These strategies focus not on the long term but rather on the short term, since there are different market conditions:

there is not the advantage of the first mover and this actor needs to make his service as secure as possible to prevent it from being shut down. So, he needs to adopt security strategies that focus on the short term. These risk strategies could for example be implementing a newer e-market technology or implementing stronger cryptography (See figure X).

Lastly, the police task unit tries to make the online world a safer place by trying to adopt risk strategies that try to reduce the security level of the crypto market operator. These risk strategies are the core competence of the actor, since this actor could be classified as security provider. These risk strategies could for example be finding hosting servers or attacking market software (see figure X).

b) have the strategies changed significantly over time in a way that reduces or increases risks?

For the software company, the risk strategies of providing patches and communicating them changes of time since these patches become outdated. Old patches will result in an increased risk for the security consumers.

For the police task unit, new risk strategies need to be adopted over time since the opponent of the police task unit, the crypto market operator also changes his risk strategies. If both parties do not change their risk strategies over time, than for both parties this will result in an increased risk (for the police task unit the risk will increase that the means used by the crypto market results in an higher chance that the platform will be online and vice versa).

For the Final Paper: Pick one of the risk strategies identified previously and calculate the Return on Security Investment (ROSI) for that particular strategy. I.e.,

a) Estimate the costs involved in following that strategy

b) Estimate the benefits of following that strategy (assume a particular loss distribution)

References

De Haan, A., W. P. A. C. Willemse, P. de Heer, S. C. Vos, and P. W. G. Bots. "Inleiding technische bestuurskunde." (2009).