Assignment 3 - 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

1. Introduction

This assignment stays in line with the previous assignment by using the police task force, the crypto market operator and the software company as actors for this analysis. The security issue that is identified for this assignment is the availability of cybercrime assets in crypto markets. The crypto market operator is the maintainer of the market and as such defends the asset of the crypto market, whereas the police task force is focused on reducing the availability of cybercrime assets by attacking the crypto market. The police task force is modeled as an attacker, therefore this actor has no asset to defend and nothing to lose. The software company has the objectives to protect the assets of the company and to reduce the amount of cyber assets on the crypto market with as much as possible. Figure 1 provides an overview of the actor field.

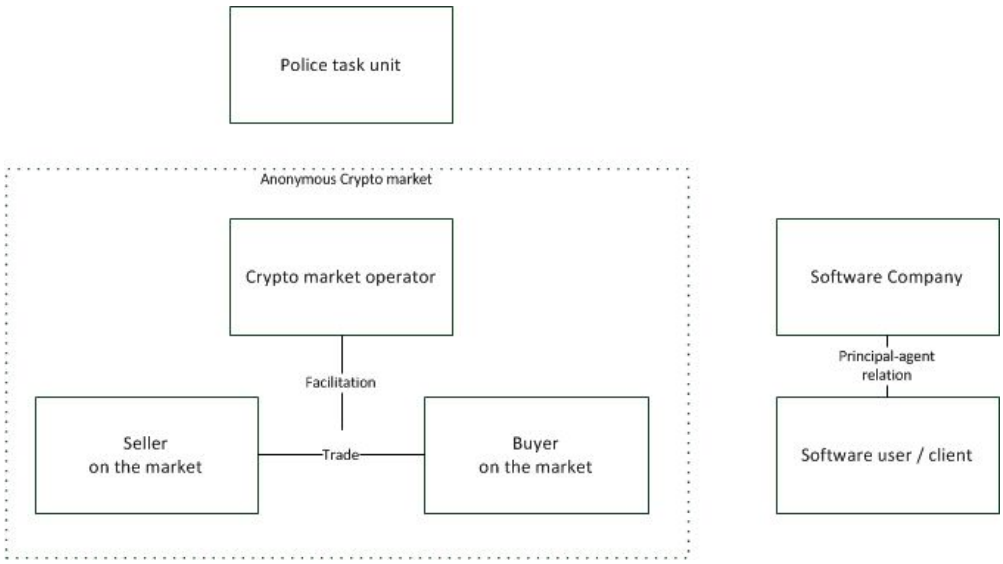

Figure 1: Formal chart actor relations

2. Actor analysis

Select 3 actors (including the problem owner) involved in the security issue (you can draw on the previous assignment)

A) The Software Company

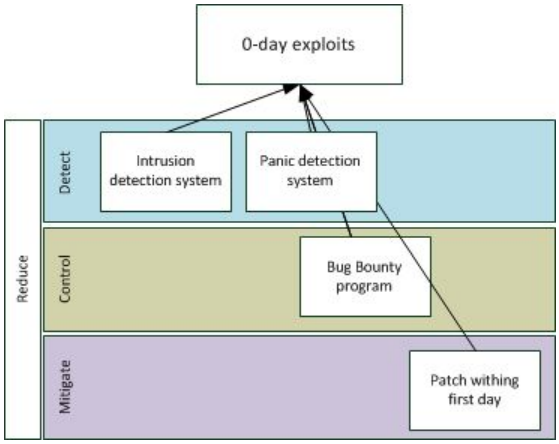

Figure 2: Counter Measurements for the software company.

A1 Identify one concrete countermeasure that they could take to mitigate the security issue.

The countermeasure the software company could take to mitigate the security issue selected for this assignment is the bug bounty program (see figure 2), which was also used for the ROSI calculation in the last assignment. A bug bounty program creates an incentive for researchers which are not affiliated with the software company to disclose the discovered vulnerability to the company, instead of selling it on a black market. Subsequently, the software company pays a fee to the researcher and patches the vulnerability (Krishnamurthy, S., & Tripathi, A. K., 2006). Not having these vulnerabilities available on the market helps to prevent the availability of exploit by reducing the supply.

A2 Analyze the distribution of costs and benefits among the different actors that the deployment of the countermeasure would entail.

A bug bounty program, according to Krishnamurthy *et al.* (2006), rewards freelance bug hunters with a prize for being the first and/or best at offering a solution for a bug they also newly discovered. For the company, the benefits are less development cost because fewer developers at the company have to look for bugs. At the same time, Krishnamurthy *et al.* (2006) states the possible costliness of such a bug bounty program. Overall, the bug bounty seems to be profitable for the software company since it can help find about a quarter of all bugs of an average software company (Finifter, M., Akhawe, D., & Wagner, D., 2013). The other principal benefactor is the researcher who discovers the bugs and is rewarded for that. However, this is not a viable alternative to a salary to many, which may prevent professionalism coming up amongst these freelance bug bounty hunters (Krishnamurthy *et al.* 2006, Finifter, M *et al.*, 2013). Furthermore, this actor is out of the scope of the analysis and thus will not be covered further.

This countermeasure has probably little effect on the police task force, who is focused on disrupting the trade of the market and not on the exploits of the company. The countermeasure may reduce the supply of exploits on the crypto market, but not fundamentally change its working. Therefore, the crypto market operator will not be directly affected by the countermeasure.

A3 Analyze whether the actors have an incentive to take the countermeasure.

The software company has an incentive to implement a countermeasure to reduce the security issue, since insecure software would have a negative impact on the reputation of the software company. An example of this is the usage of flash. Adobe's Flash is considered as insecure, and as a result the number of Flash users is declining[1]. By not undertaking action to reduce security issues, software companies take the risk that their software becomes insecure, which would lead to a lower number of users, and eventually, less revenue. Therefore, the software company has an incentive to undertake action against the existence of darknet markets, since these markets form a threat to the level of security.

Furthermore, the software company has an incentive to use the bug bounty program counter measurement since, considering the work of Finifter, M et al., (2013), the bug bounty program is cost-efficient. In the article, a three year program at both Chrome and Firefox have been analyzed, costing respectively $580,000 and $570,000 and yielding respectively 28% and 24% of the patched vulnerabilities. Therefore, the company has a financial incentive to adopt a bug bounty program.

A4 Briefly reflect on the role of externalities around this security issue.

A bug bounty program has also positive and negative externalities for the software company. A positive externality is that researchers will specifically search for vulnerabilities in the software because they are driven by the financial reward they can earn. As a result, that more vulnerabilities are found than there would be without the bug bounty program. A negative externality on the other hand, is that the software company's own developers can disclose these vulnerabilities via the bounty program in order to earn extra money.

[1]https://www.fastcompany.com/3049920/tech-forecast/the-agonizingly-slow-decline-of-adobe-flash-player

B) Police Task Unit

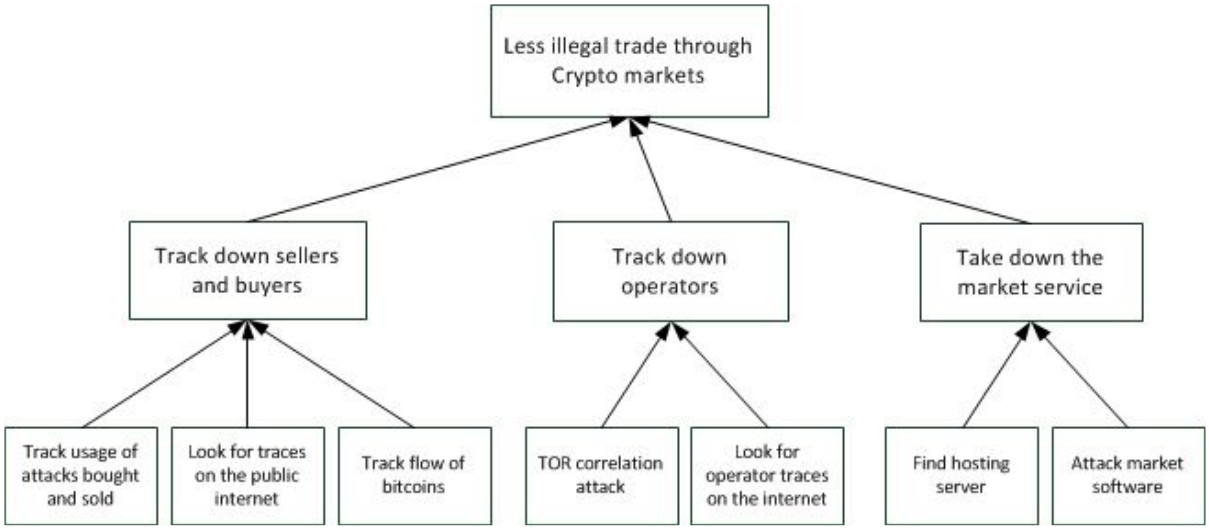

Figure 3 Counter Measurements for the police task unit.

B1 Identify one concrete countermeasure that they could take to mitigate the security issue.

One concrete countermeasure (see figure 3) that the police task force could undertake is to dismantle the crypto market by attacking the market software, as has been done previously during operation Onymous (Reitano, T., Oerting, T., & Hunter, M, n.d.). This dismantling of the market obviously eliminates the availability of cybercrime assets on the attacked market, which increases the difficulty for threat agents to buy vulnerabilities or exploits.

B2 Analyze the distribution of costs and benefits among the different actors that the deployment of the countermeasure would entail.

The police task force will have a budget allocated for these attacks, which has been assigned by a government authority (Stol, Leukfeldt & Klap, 2012). Interestingly, the execution of these attacks and the dismantling of crypto markets has benefits for other actors, most notably the software company and the software user.

B3 A Analyze whether the actors have an incentive to take the countermeasure.

The task of monitoring and attacking crypto markets is assigned to the police task force by the government. The cyberspace is defined as as a public good and dismantling these markets is therefore for the benefit of all people in the country (Stol, Leukfeldt & Klap, 2012). Therefore, there is e.g. no financial incentive for the police task force to do this, it is commanded by the government.

B4 Briefly reflect on the role of externalities around this security issue.

The actions of the police task force can result in both positive and negative externalities. A positive externality of dismantling crypto markets with the goal to reduce the availability of cybercrime assets is that also other products that are offered on these markets are reduced, such as hard drug and credit cards. A negative externality, however, can be that criminals

are forced to find other ways to offer these products for sale, e.g. on other crypto markets or through other means.

C) Crypto Market Operator

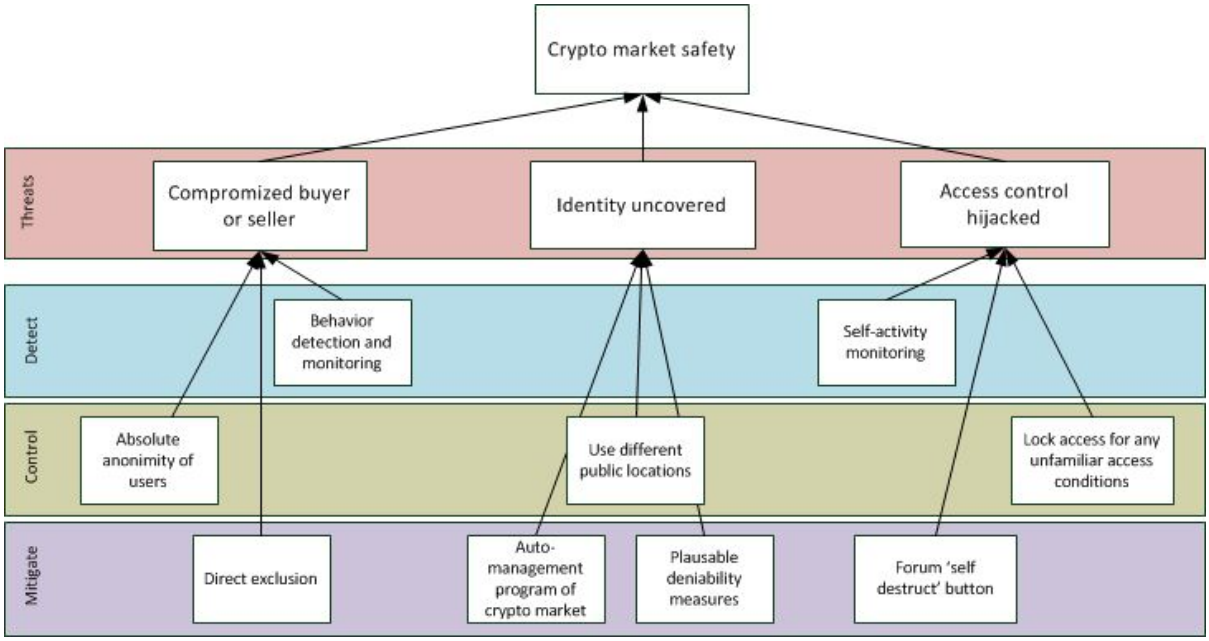

Figure 4 Counter Measurement for the Crypto market operator.

C1 Identify one concrete countermeasure that they could take to mitigate the security issue.

The crypto market operator has a different perspective on the security issue compared to the police task unit and the software company. For the software company and the police task unit, the very existence of the market is a threat to their security performance. Therefore, as described above, these actors use certain counter measurements against the existence of the market to increase their security performance. These counter measurements threaten the security performance (or safety in figure 4) of the crypto market operator. Therefore, the crypto market operator will use certain counter measurements against the counter measurements of the other two actors. One example of a concrete countermeasure that the actor could take is to use different public locations when he accesses his crypto market. Doing this makes it harder to track him down and enables him to operate the crypto market for a longer (possibly for as long as he wants) time. 'Dread Pirate Roberts', the crypto market operator that operated Silk Road also used this method (Donald, Bernice B., and N. Chase Teeples, 2014).

C2 Analyze the distribution of costs and benefits among the different actors that the deployment of the countermeasure would entail.

Taking this countermeasure is beneficial for the crypto market operator, because it becomes harder for the police task unit to catch him. As as result, he has a higher chance of successfully securing his assets, while it becomes more difficult for the police task unit to trace down the crypto market operator, allowing the market operator will be able to continue

the operation of the market. As described in the previous assignment, the continuation of the crypto market indirectly harms software company through the availability of the cybercrime exploits.

C3 Analyze whether the actors have an incentive to take the countermeasure.

The crypto market operator has the incentive of preventing himself from being identified to protect the asset of the crypto market because the crypto markets have a high revenue (Kruithof et al., 2016). Kruithof et al (2016) estimate that crypto market operators made a total monthly revenue of between $12m and $21m. This revenue incentive the crypto market operator to take certain counter measurements to keep this revenue at this level by the continuation of the existence of his platform.

C4 Briefly reflect on the role of externalities around this security issue.

The creation and maintenance of a platform that allows for the trade of dangerous goods creates negative externalities for potential targets of the dangerous goods. More specifically, maintaining the crypto market causes more availability of cybercrime assets and thus negative externalities for the software company and the user of the software. A positive externality is, remarkably enough, that criminal money positively adds to the economy of a country. When crypto markets are up and running, money is generated and the economy is fueled (Kozy, 2012).

2. Security performance

Identify the type of actor whose security performance is visible in the metric(s) you selected (e.g. ISPs, software vendors, countries). Note that this is not necessarily the problem owner, rather is the unit of analysis in your metric.

- *1. Identify different factors explaining (causing) the variance in the metric,*
- *2. Collect data for one or several of these factors,*
- *3. Perform a statistical analysis to explore the impact of these factors on the metric.*

1.

For this assignment, the software company will be the actor that will be analyzed. The metric that will be used is the *number of cybercrime assets* that are available in the darknet market per company. Table 1 provides an overview of the companies that can be found in the dataset, together with their products that are targeted. As can be seen in this table, there are several product categories, which make it difficult to compare them. Therefore, only companies that offer an operating system will be taken into account: Google, Microsoft, Apple and Linux. Figure 5 displays the number of cybercrime assets that are available for these companies.

Company	**Product**
Google	Android
Microsoft	Internet Explorer Windows
Apple	iCloud, Apple-ID
Linux	Linux
WordPress foundation	Wordpress
Mailbird	Mailbird
Adobe	Adobe Flash<= 16

Table 1 - Companies and product in the dataset.

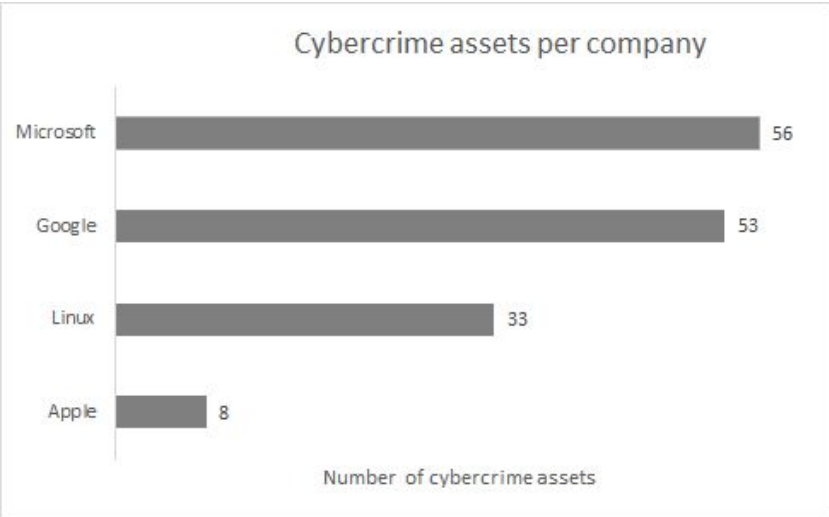

Figure 5 Cybercrime assets per software company.

2 & 3.
In order to compare the security performance of these companies, several factors that can explain this variance are assessed

Market share

Company	**Marketshare[2]**
Google	35%
Microsoft	45%
Apple	18%
Linux	2%

Table 2 - Market Share of OS providers.

Table 2 shows the market share for these four software companies. From this table, the following hypotheses can be formulated. The first hypothesis out of three to be tested is the question of whether a higher market share results in more security incidents. A popular line of thought is that a system with more market share is appealing for attackers because there are more assets at risk (Chen, P. Y., Kataria, G., & Krishnan, R., 2005). The hypothesis are as follows:

H0: Market share has no influence on security performance.
H1: Market share decreases security performance.

The results of this test can be found in Appendix A. The coefficient is 0,774583, indicating that a higher share contributes to more security issues and therefore a worse security performance. The p-value is significant at 0,337363, but because of N = 4, the sample is too low and no conclusions can be drawn from the test.

Open Source
The second hypothesis to be tested is the question whether open source or closed source contributes to more security. One might suggest that closed source contributes to extra security of a system because attackers cannot look for vulnerabilities in the source code of the system. On the other hand, the system's code being open source might also result in developers finding and fixing vulnerability issue's faster which in turn makes the system more secure. (Paulson, J. W., Succi, G., & Eberlein, A., 2004). The hypothesis are as follows:

H0: Open source and closed source do not contribute to the security performance.
H1: Open source contributes to a better security performance than closed source.

Windows and Apple software are closed source whilst Apple and Google (Android) provide open source software. The results of this analysis are displayed in Appendix A. The

[2] http://gs.statcounter.com/#all-os-ww-monthly-201607-201607-bar

coefficient is 11 and the p-value is 0,71339. This means that open source has more vulnerabilities than closed source, but because of N = 4, the sample size is too small and no conclusions can be drawn from the test. It is remarkable that the coefficient of this factor is positive, since it is assumed that popular open source projects are often more secure since more people can peer review code and patch faster since there is no need to contact a software company about a bug (Collins, 2009). However, by looking at the number of cybercrime assets for the open-source OS Linux, which has the highest number of cybercrime assets, this result seems to be legitimate.

Price hypothesis

The Apple computers are almost twice as expensive than their PC and Linux counterparts[3]. The same is true for Android and iOS devices, where the Apple product is more expensive. The question is whether paying more for a system will also result in more security benefits. The basic idea is that if a company's business model is to charge the user for security, the security should be in line with the interest of the user and not the company (Anderson, R., 2001). The hypothesis are as follows:

H0: Expensive and less expensive computers show no difference in software security.
H1: Expensive computers have more secure software than less expensive computers.

The results are as follows: the coefficient is -39,3333, which means that when the product is expensive, the product is more secure. The p-value is significant at 0,112456 but because of N = 4, the sample is too low and no conclusions can be drawn from the test.

3. Reflection

The dataset that is used for this assignment made it very difficult to come up with a metric to compare performances that were within our scope. The problems with the dataset were, amongst others, the large number of duplicates, the limited number observations and the anonymity of all participants in the market, making it hard to say anything meaningful about the sellers and buyers. The best we could do was to assess the exploits available by analyzing the description of the products that were offered and relate them to the company that develops this product.

In order the make comparisons more realistic, we decided to focus on companies that offer operating systems. For our data set, this resulted in four companies, which is a very small number of observations. Therefore, it was not surprising that all of the factors that were used in the hypotheses were found to be not significant. For this reason, it is not possible to determine if there are causal relations between the number of cybercrime assets and the various factors, even though the sources we use indicate that there is a relationship.

---

3 http://gizmodo.com/5033865/study-average-mac-computer-price-more-that-twice-that-of-average-pc

References

Anderson, R. (2001). Why information security is hard-an economic perspective. In Computer security applications conference, 2001. acsac 2001. proceedings 17th annual (pp. 358-365). IEEE.

Chen, P. Y., Kataria, G., & Krishnan, R. (2005). Software Diversity for Information Security. In *WEIS*.

Collings, H (2009) Is Open Source Software More Secure than Proprietary Products? Government technology . Retrieved at 25-10-2016 from http://www.govtech.com/security/Is-Open-Source-Software-More-Secure.html

Donald, Bernice B., and N. Chase Teeples. "Not Your Father's Legal Profession: Technology, Globalization, Diversity, and the Future of Law Practice in the United States." U. Mem. L. Rev. 44 (2013): 645.

Finifter, M., Akhawe, D., & Wagner, D. (2013). An empirical study of vulnerability rewards programs. In Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13) (pp. 273-288).

Kozy, J. (2012) *How the economy works: The necessity of crime*. Available at: http://www.globalresearch.ca/how-the-economy-works-the-necessity-of-crime/32125 (Accessed: 27 October 2016).

Krishnamurthy, S., & Tripathi, A. K. (2006). Bounty programs in free/libre/open source software. BITZER Jurgen, The Economics of Open Source Software Development, Lavoisier, Paris, 165-183.

Kruithof, Kristy, Judith Aldridge, David Décary Hétu, Megan Sim, Elma Dujso and Stijn Hoorens. (2016). Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands. Santa Monica, CA: RAND Corporation. Retrieved at 25-10-2016 from http://www.rand.org/pubs/research_reports/RR1607.html.

Paulson, J. W., Succi, G., & Eberlein, A. (2004). An empirical study of open-source and closed-source software products. IEEE Transactions on Software Engineering, 30(4), 246-256.

Reitano, T., Oerting, T., & Hunter, M. Innovations in International Cooperation to Counter Cybercrime: The Joint Cybercrime Action Taskforce.

Stol, W., Leukfeldt, E. R., & Klap, H. (2012). Cybercrime en politie. Justitiële Verkenningen, 38(1), 25.

Appendix A

	Coefficients	Standard Error	t Stat	P-value	Lower 95%	Upper 95%	Lower 95,0%	Upper 95,0%
Market share	**0,774583**	0,619048	1,251248	**0,337363**	-1,88897	3,438132	-1,88897	3,438132
Open source	**11**	26	0,423077	**0,71339**	-100,869	122,869	-100,869	122,869
Expensive	**-39,3333**	14,43761	-2,72437	**0,112456**	-101,453	22,78667	-101,453	22,78667