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

Due to time other deadlines this week, this draft will only contain main ideas. Please check if we're on the right direction rather than whether the details are correct. We apologize for the inconvenience. Thank you!

Actors involved in the security issue follow different strategies to mitigate its impact. For this assignment:

1. Select 3 actors (including the problem owner) involved in the security issue (you can draw on the previous assignment). For each one:

For this assignment, we stay in line with the previous by using the police task force, the crypto market operator and the software company as our actors. To recap, the security issue is the availability of cybercrime assets. These can easily be obtained through crypto markets in which all participants are anonymous. The crypto market operator is the maintainer of the market and as such defends the asset of the crypto market. The police task force is tasked with reducing the availability of the cybercrime assets by attacking the crypto market. The police task force is modeled as an attacker and as such as no asset to defend and nothing at risk.

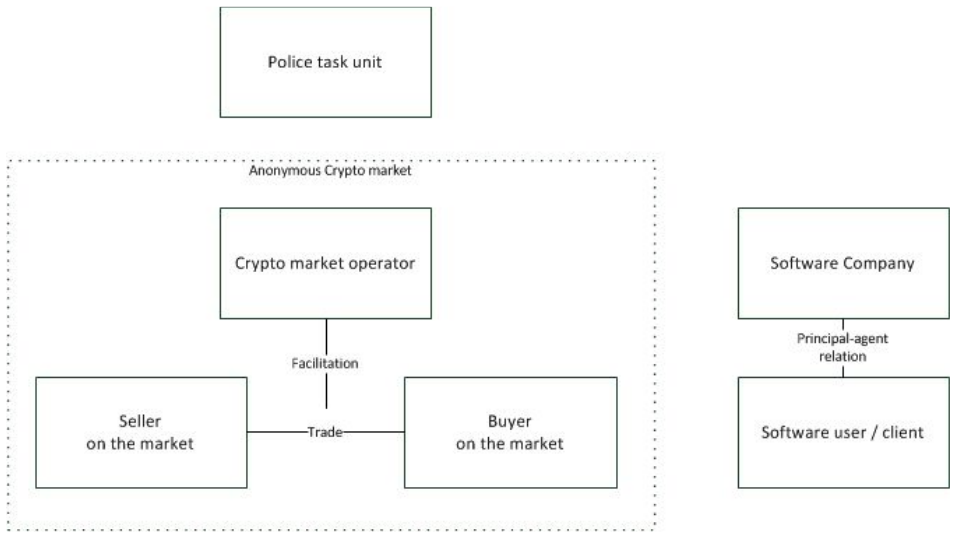
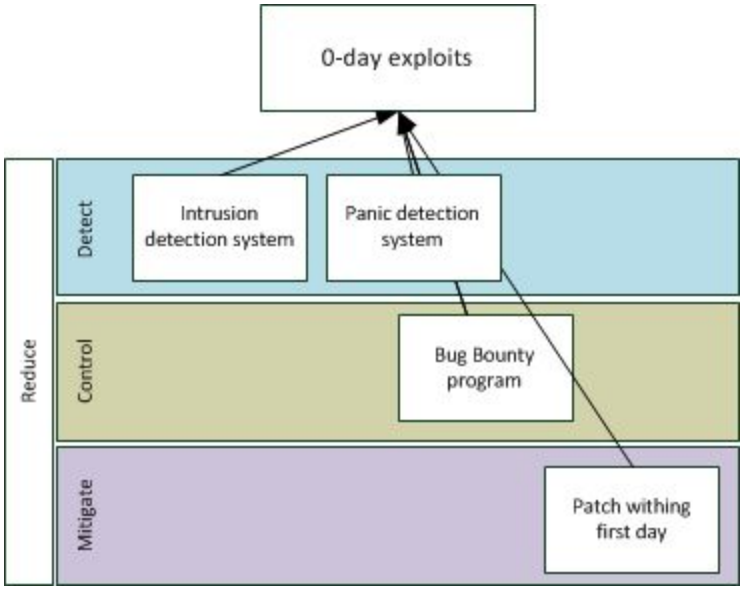


Figure X: Formal chart actor relations

Software company



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

Zero-day exploits per definition are something that cannot be completely prevented (otherwise it shouldn't be called a zero-day exploit). To mitigate the damage being done by zero-day exploits our best option is to try to reduce the amount of zero-day exploits that are used on our system. A concrete countermeasure that could be taken is to organise a bughunter program that allows the online community to search for bugs and zero-day exploits for specific rewards. Every exploit that is being found can be repaired by the company and will prevent potential damage being done in the future.

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

The software company in general holds most assets to be protected the burden of costs will mainly be at the software company. The police task force will generally be concerned with making sure that the law is obeyed and that general order is created. Depending on how critical the software (company) is for governmental operations, the police task force might also choose to invest in the programme to make the software being used by citizens more secure. The crypto market operator will suffer a penalty because every zero-day exploit being found by the bounty hunter program is one potential zero-day exploit less that could be sold on his crypto-market (which would earn him money). The software company however will generally benefit from the program since every exploit being found reduces the likelihood of a zero-day attack.

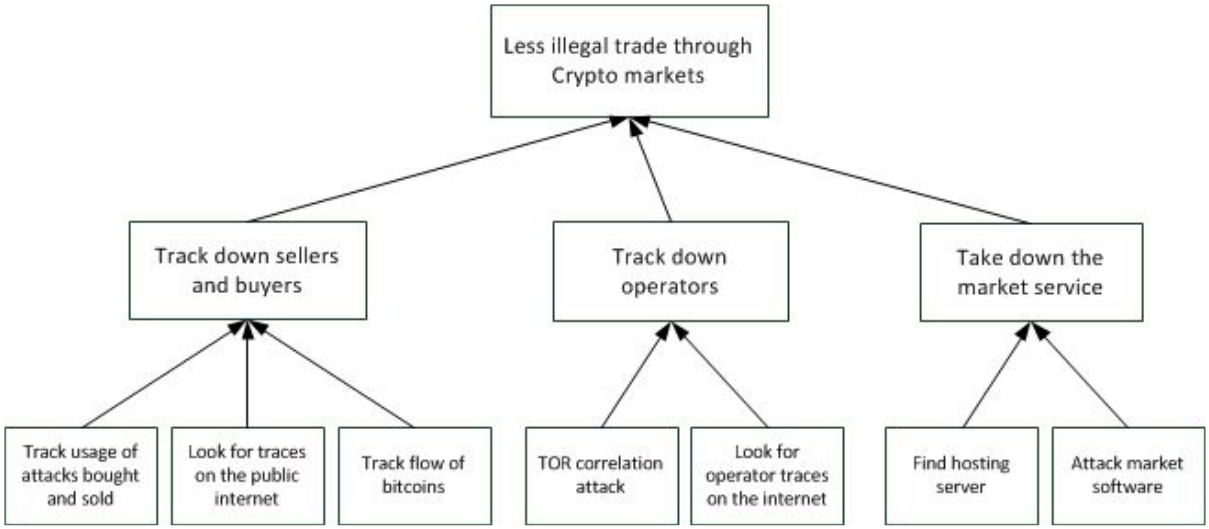
Analyze whether the actors have an incentive to take the countermeasure

The crypto market operator obviously has no reason to take this countermeasure. As has been explained in the previous section, every zero-day exploit being discovered reduces the chance of him earning money of him selling a zero-day exploit on his market. Taking the countermeasure from the software company's perspective will only generally only be

beneficial. For the police task force however, the incentive is much more complicated. Investing money in the security of software will give the software and its users better protection against exploits and security breaches, but investing in a bounty hunter program does not help them catch the people that use the zero-day exploits, which might be something they want to solely focus on.

Briefly reflect on the role of externalities around this security issue
TODO

Police Task Unit



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

One concrete countermeasure that the police task force could take is to take down the market service for as long as possible (potentially forever). This results in the inability of cybercrime assets being sold which in turn will likely reduce the amount of attacks that occur.

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

The police task force will be the party that will generally completely pay for these attacks. Since the police task force is a party that is completely independent (and should be independent so that it cannot be corrupted by influencing parties) it is unlikely that they can receive money from other software companies even though they are likely to also benefit from the attack on the crypto market. The benefit of the police task force is that no illegal trading can occur via the crypto market anymore and that the chance that illegal goods or services cannot be obtained anymore which will possibly reduce the amount of crimes.

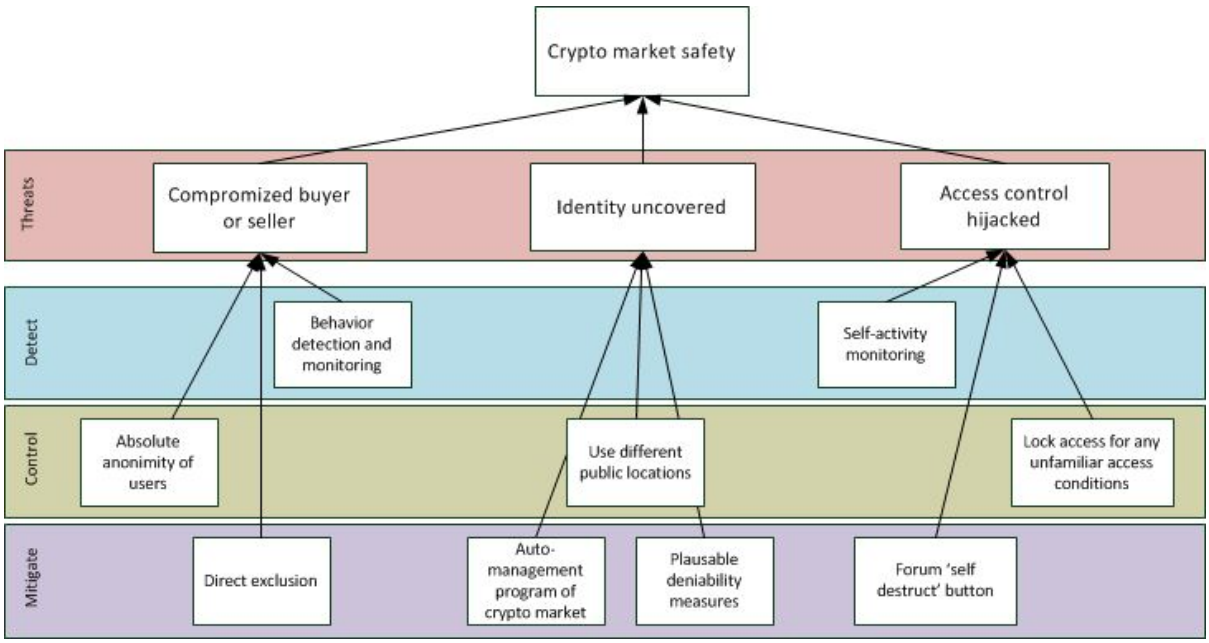
Analyze whether the actors have an incentive to take the countermeasure

Since taking down a market service is an action that is generally only allowed by the police task force unit it is unlikely that software companies will ever result to this type of action. The software companies could maybe make an investment in tools or supplies that the police task force could use, but it might be complicated for the police task force to accept external investments since they need to remain independent of other parties. The crypto market operator has no incentive at all to take the countermeasure since taking down his market will only result in a loss of money for him.

Briefly reflect on the role of externalities around this security issue

TODO

Crypto Market Operator



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

A countermeasure that the crypto market operator 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.

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

Taking this countermeasure is definitely beneficial for the crypto market operator since it will prevent him from being caught by the police task force or by unsatisfied market users. For the police task force it will however make it harder to maintain the law and order because the market operator will be able to continue his illegal activities. The software companies indirectly also suffer from this, because the longer that the market is online, the more cybercrime assets might be sold and traded, likely resulting in a larger amount of attacks towards the software company.

Analyze whether the actors have an incentive to take the countermeasure

The crypto market operator has the obvious incentive of preventing himself from being caught whereas the police force and the software company would rather have this countermeasure not being taken such that the crypto market operator can be caught.

Briefly reflect on the role of externalities around this security issue

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