Final - Assignment Block 3

Economics of Security (WM0824)
Group 1

Anirudh Ekambaranathan (s1366432)
Joris Diesvelt (s1007114)
Sem Spenkelink (s1375490)
Lisa de Wilde (s1091514)

October 11, 2015

1 Introduction

This paper is about the assignment of block 3 of the course Economics of Security and is a continuation to the paper produced in Block 2. The previous paper analyzed the data-set of the ZeuS and Feodo trackers. From this data-set a general security issue was established (see section 1.1). Then the metrics which would describe and help evaluate the security issue were analyzed. These metrics included criteria such as, infected hosts, social engineering and rate of change of C&Cs.

This paper will look into which actors are influencing the security issue, how the issue might be mitigated and the costs related to implementing these mitigations.

This papers is structured as follows. The general information in the introduction, which also includes a slightly changed security issue and perspective (see section 1.1) is followed by the methodology of how this assignment will be solved. This also includes a roadmap of how the steps which will be taken (see section 2). Sections 3 to 8 are about answering the six questions of the assignment:

1. Who is the problem owner of the security issue as measured in your first assignment? (see section 3)
2. What relevant differences in security performance does your metric reveal? (see section 4)
3. What risk strategies can the problem owner follow to reduce the security issue as measured in your first assignment? (see section 5)
4. What other actors can influence the security issue as measured in your first assignment? (see section 6)
5. Identify the risk strategies that the actors can adopt to tackle the problem. (see section 7)
6. Pick one of the risk strategies identified previously and calculate the Return on Security Investment (ROSI) for that particular strategy. (see section 8)

Finally, the conclusion of the assignment is given in section 9.

1.1 Security Issue and Perspective

After receiving feedback on the assignment of block 2, the security issue and perspective have been changed slightly. Initially, the security issue was related to companies defending themselves from financial malware. However, the corresponding metrics which were defined did not match the security issue. Therefore the issue has been slightly altered and the perspective has been changed. This paper now concerns itself with the following security issue:

Law enforcement agencies have to fight against ever adapting financial malware and methods of spreading financial malware.

The issue is now viewed from the perspective of the Law Enforcement and covers tracking C&C's and eventually tracing criminals and protecting civilians and organizations against the ever adapting financial malware and methods of spreading financial malware, which includes creating awareness about the problem. The data-set used is mainly for

tracking C&Cs, so more data is needed to link the C&C to a certain criminal.

The issue thus also covers protecting civilians, and a part of this is raising awareness about malware the threats in the cyber world. The dataset does not directly speak to this, however, this is a vital part of the security issue.

2 Methodology

To make sure this assignment could be solved properly, the security issue and perspective of the issue defined in assignment 2 are extended and changed a bit, so it fits better to the data-set of the Zeus Tracker and Feodo Tracker. Besides that, there are certain terms that need to be understood before the assignment can be solved, for example: 'problem owner', 'actors' and 'risk strategy'. All questions are answered in the given order and finally, a conclusion is given.

The steps can be summarized as follows:

- Clarifying and extending the security issue and perspective;
- Finding information on the terms 'problem owner' and 'actors';
- Identify the problem owner;
- Choose a metric for question 2;
- Choose the differences to investigate;
- Create a graph in R;
- Evaluate the graph;
- Finding information on the term 'risk strategy';
- Identify risk strategies for the problem owner;
- Identify actors that influence the security issue;
- Identify risk strategies that the actors can adopt to tackle the problem;
- Investigate if the strategies have changed significantly over time;
- Choose one strategy for the ROSI calculation;
- Define the risk exposure for the strategy;
- Define the percentage risk mitigated;
- Define the solution costs;
- Calculate ROSI;
- Extend the ROSI calculating with a probabilities;
- Write a conclusion.

3 Problem Owner

There are different perspectives which address the security issue. This research dives into the perspective from law enforcement agencies who fight against the financial Trojans. The law enforcement agencies can trace the criminals, protect civilians and companies and can create awareness about the problem. Besides that law enforcement agencies are the most affected by the security issue and would benefit from a solution or mitigation. Therefore, the problem owner of the security issue are the law enforcement agencies.

4 Differences in Security Performance

As is discussed in the previous assignment, the problem owner can make use of different security measures to improve their risk strategy. It is often useful to analyze how different parties use these metrics and how they perform against each other. These relative performance differences can be used to enhance the problem owners own metrics and thereby his risk strategy.

4.1 Increase of C&Cs

Considering the problem owners are the law enforcement agencies as discussed in section 3, it is useful to know the growth of botnets and the performance of the corresponding tracker. While it is hard to estimate the size of a certain botnet, trackers give accurate data as to how they perform. In the previous assignment, it was concluded that the detection rate of ZeuS and Feodo tracker increases over time. In figure 1 the amount of newly found Zeus C&C's is set out for every month. Every month is compared to the previous month, providing insight about the relative difference in C&C-configures per month. Large positive spikes (followed by an around-zero-pattern) indicates a sudden vast increase of C&C-servers found by our tracker. The data was measured on a daily basis, however that graph showed no visible increases or decreases, making it infeasible for proper analyses.

4.2 C&C's per Country

As a second metric for law enforcement it might be very interested to know the physical location that thrives in malicious activity regarding the financial Trojans. Knowing what countries play a large part in the C&C-infrastructure can contribute to tracing down the servers and possibly the criminals. It might also be a reason to block certain address spaces from which only malicious traffic propagates. Figure 2 shows the number of C&Cs per country, normalized by the number of hosts. Since solely measuring the C&Cs per country does not give a reliable estimate of the danger and distribution of ZeuS C&Cs, the choice had been made to normalize it by the number of internet users. Also, all countries with less than 500.000 internet users have been filtered, because they make the graph less readable and does not add to measuring the metric.

5 Risk Strategies of the Problem Owner

Law enforcement agencies can apply multiple strategies to reduce the security issue. There are four types of strategies: avoidance, limitation, transference and acceptance. Avoiding the risk is the action that makes sure the law enforcement agencies are not at all exposed to the risk. This is the most effective risk strategy when purely looking at reducing the effects of the issue. However, risk avoidance is also the most expensive risk mitigation option. Since solutions are often made based on cost-efficiency a more likely approach is risk limitation. This strategy limits the law enforcement agencies exposure to the security issue. Another strategy law enforcement agencies could use to reduce the security issue is transferring the mitigation process to a third party. Lastly, ever adapting financial malware and methods of spreading financial malware, is a problem of immense size. In some cases it will be impossible to enforce measures without making substantial losses. It might be more feasible to employ risk acceptance. In this section different specific strategies are given for the law enforcement agencies, they suit to one of the categories described above.

5.1 Cooperating with other agencies

Different agencies and organizations will have their own sources and databases with information. Sharing this information and cooperating with other institutions will lead to more efficient and effective problem solving. This is displayed by attempts to take down botnets such as Operation Tovar FireEye [2014] and the attempt to take down the Cutwail botnet in 2010 Symantec [2010] show. To reduce the security issue the Law Enforcement can cooperate with other law enforcement agencies, governments, universities, researchers etcetera all over the world. When cooperating with other parties, the collaboration needs to be evaluated every now and then to make sure it is still effective to cooperate. Major events triggered by cooperation can be evaluated by analyzing the amount of online C&C's propagating from the moment the cooperation event is executed. Besides that, the metric described in section 4.2 can be used to decide with which countries cooperation should be started.

5.2 Taking down C&C-servers

Tracing C&C-servers and taking them down would be a first step towards a safer environment for all kinds of actors. Law enforcement agencies can focus on tracing these servers. The Zeus and Feodo C&C-servers are used to infect people, the address space of these servers can ultimately be traced, as joint efforts have proven (see 5.1). From here it can move into two directions. Firstly, analyzing whether taking down C&C-servers is effective by comparing it to the amount of newly configured C&C's and secondly evaluating if the general flow of C&C-servers has a downward spiral. For Zeus and Feodo this can be realized with provided datasets. By analyzing the amount of C&C's per day, agencies can gather whether there is an increase or decrease of C&C's. If taking down servers generates a decrease of servers, it might very well prove to be an effective strategy.

5.3 Tracing criminals

Taking down a hijacked server removes a slight part of the problem, since new servers can be configured and set-up, this is still a big problem to look into. In the physical atmosphere law enforcement

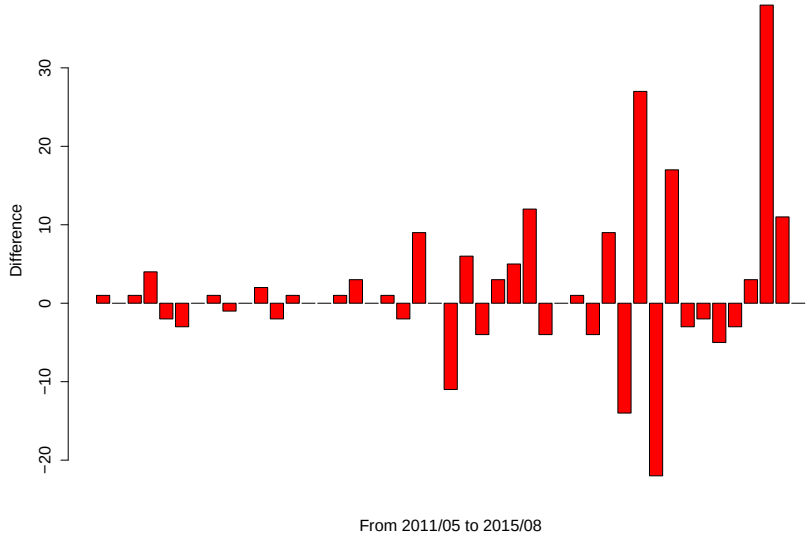

Figure 1: Incremental Rates of Zeus C&C's

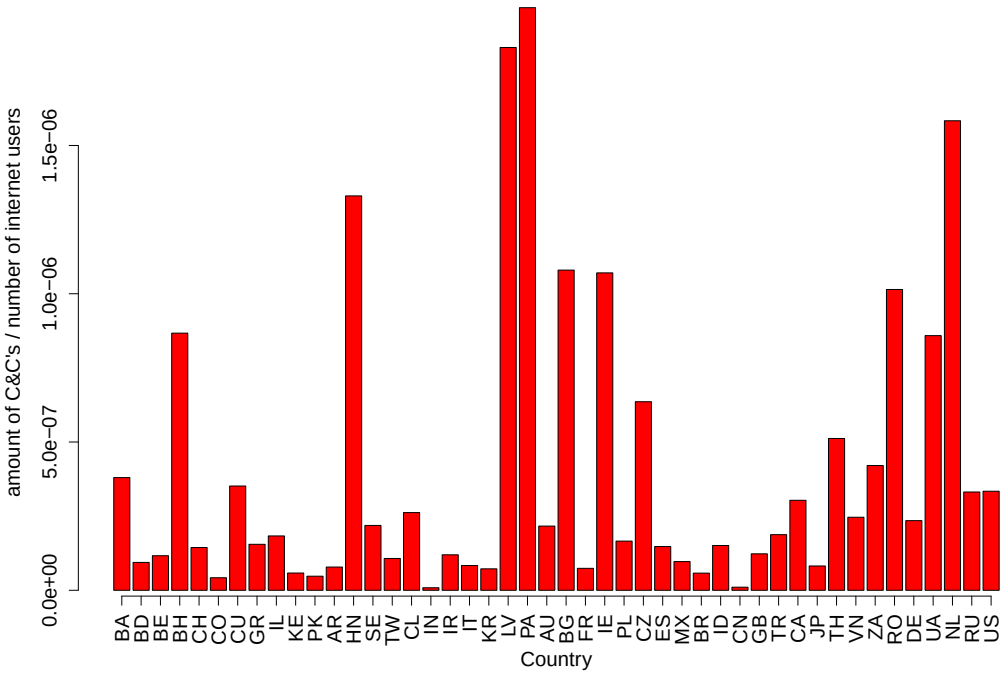

Figure 2: Normalized C&Cs per country

is evidently working on putting criminals behind bars. In cyberspace the purpose is not any different. However, the available resources to find botmasters are scarce, which makes tracing the criminals physically rather hard. On scientific levels there is a lot of work related to botmaster traceback. For example, the watermarking technique of Ramsbrock et al. [2008] tags C&C traffic to, eventually, find botmaster commands. If law enforcement manages to physically arrest a botmaster, it is also possible to evaluate whether this has an effect on the decline of C&C-severs. It also might be a reason for other botmasters to cancel their activities, making this strategy more effective. Finding a botmaster, however, is a tough job and only few successful events have taken place. Physically finding botmasters and putting them behind bars does happen though, often in cooperation with other agencies. The effect of botmaster-takedown can be measured in a similar way to C&C-takedown. The effectiveness of an entire botnet going down due to physical arrests should trigger a very sudden and steep decrease of C&C's of that type.

5.4 Block certain countries or ip-address ranges with high malicious rates

A way for law enforcement agencies to protect against C&C-infections would be to limit the possible access towards these servers. If a certain country shows a lot of malicious activity law enforcement with governance admittance might consider blocking that malicious area entirely. This could be done precisely or with broad measures. Firstly, the blocklists provided by tracker-instances such as the Zeus- or Feodo trackers can be used to specifically block certain C&C's. Secondly, an agency might choose to block an entire network-area that proves to be a hive for malicious activity.

5.5 Awareness campaign

It is not feasible for law enforcement to protect all civilian and/or organizational machines connected to the Internet. That would mean law enforcement would have access to these devices, and apart from the fact that it is not possible to process all these devices, it forms a breach of privacy. Instead law enforcement, in cooperation with other government institutions and banks, can launch awareness campaigns which inform civilians and organizations about the dangers of financial malware. These campaigns will inform civilians and organizations about the dangers of financial malware and decrease the number of infections. This can for example be done by radio and/or television commercials, posters in cities, sending letters to all citizens/organizations, creating a website with information about financial malware and going to schools to teach children about phishing and financial malware. To make sure it is effective, some of the methods should be repeated several times.

6 Actors that Influence the Security Issue

Besides the problem owner, there are multiple other actors who can influence the security issue in a positive and/or negative way. The different actors are described in this section and in section 7 it is described how these actors can influence the security issue.

6.1 Positive Influence

The following actors can positively influence the security issue i.e. they can help the problem owner to fight against ever adapting financial malware and methods of spreading financial malware.

- Companies;
- Universities;
- Researchers;
- Governments;
- Banks;
- Security companies;
- Schools

6.2 Negative Influence

A negative influence on the security issue by an actor occurs when the problem owner will be effected negatively by a action of the actor. In this case there is only one actor with a negative influence:

- Criminals

7 Risk Strategies

In this section a risk strategy to tackle the security issue is given per actor or group of actors.

7.1 Companies

1. *Awareness training.*
   Companies are interested in protecting their employees from cyber security harm. Such harm will influence productivity and may lead to loss. One way is to make employees aware of financial malware and the ways it will be spread. This can be done by an awareness training including measuring the effectiveness of the training. It is intended that all employees follow a training and do not provide their credentials to phishing websites anymore.

   The focus of awareness training has shifted over the past couple of years towards the cyber domain. Threats in the cyber domain have increased, so companies focus on techniques such as phishing, cross site scripting etc.

2. *Awareness campaign.*
   Besides, giving awareness training to the employees, companies can also send e-mails to their employees about financial malware, creating posters about the problem and adding some information about the companies website. This strategy is meant to spread information about financial malware with low costs and low effort. Employees can be surveyed afterwards to gain insight into the effectiveness of the campaign. Awareness campaigns also occur more over the internet, instead through, for example, workshops and lectures.

3. *Up-to-date antivirus programs on every device.*
   Antivirus programs can detect viruses and trojans. When a company makes sure that every device within the company has a antivirus program which is up-to-date, the virus may be found when it exists on a device. The strategy may be to check for antivirus every three days and install antivirus programs on new devices when the are bought. Besides that, every month it must be checked if the used antivirus program is still up to date.

4. *Cooperating with other agencies.*
   Companies may not always be interested in cooperating with other agencies. There may be several reasons for this. They might think that other companies may gain an unfair insight in their security matters or they might lack financial motivation. However, when companies feel that the infections are influencing them or their clients, they might have plenty of reasons to cooperate with other agencies to tackle the security issue. One strategy may be setting up a group of multiple companies who all together fight against financial malware. To do so, a company needs to find other organizations who want to cooperate with them and create a goal for the group. Once the group is complete and working the effectiveness of the cooperation needs to be measured. When the effectiveness is lower than expected new guidelines need to be created.

   Using antivirus, cooperating with other organizations and raising awareness campaigns are techniques which are used by other actors as well.

7.2 Universities

1. *Cooperating with other agencies.*
   There are numerous university research groups dealing with the phenomenon of botnets. They have interest in sharing information data efforts with other organizations to track botnets.

2. *Awareness Campaign.*
   The university may not always be interested in creating awareness campaign for students. However, the infrastructure of Universities can often be complex, and this makes it possible that various student organizations may choose to create awareness campaigns. This begs the question whether this initiative is from the University or only that corresponding that student organization. Furthermore it is possible that the University only deploys an awareness campaign for their administrative employees and not for all their students. Universities can organize such campaigns with other actors such as governments and banks, since they too follow the same strategy.

7.3 Researchers

1. *Performing research.*
   Researchers can do research on financial malware and the spreading of financial malware. The strategy they can have is to create a paper about this topic every two year and read at least every three months a paper about this topic. This is a strategy which is not quickly followed by other actors. Banks and other institutions may have Research and Development centers, however the focus will then not always be on cyber security, but will be related to their services or products.

2. *Sharing knowledge at conferences.*
   Researchers and other experts can go to conferences to share knowledge about financial malware. During this conferences new insights may be found and new cooperations can be set up. This may help improve the security issue. The strategy a researcher on the topic of financial malware can have is to go every year to at least 2 conferences about this topic. This is again a strategy not easily followed by other actors because they may lack the knowledge. Security companies may possibly follow this strategy, however their papers and talks will often be related to their products rather than financial malware and botnets per se.

3. *Cooperating with other agencies.*
   As mentioned by the other actors one strategy may be cooperating with other agencies. Researchers too have interest in sharing information with other organizations to track botnets. Sharing knowledge among parties can often benefit research from both ends.

7.4 Governments

1. *Awareness campaign.*
   It is in the interest of the government to protect their civilians. Therefore awareness campaigns are an important strategy for governments to employ. Since this strategy is described above, this will not be explained further anymore.

2. *Taking down C&C servers.*
   To mitigate the security issue C&C servers needs to taken down. The government will not deploy this strategy alone and this usually happens in cooperation with the national law enforcement. The strategy of the government may be to take a certain number of C&Cs down every month or to make sure less C&Cs are set up every month. This strategy now is more reliant on internet technology, instead of the police physically interacting with the criminals.

3. *Tracing criminals.*
   Again, governments in cooperation with their law enforcement will have an interest in tracing C&Cs and taking them down. But when only taking down the C&Cs the criminals still can set up new C&Cs. Therefore, the C&Cs need to be linked to criminals, so they can be punished and lower the chance that they will continue with spreading financial malware. The government may have a strategy to trace the criminals by finding the profiles of the owners of the C&Cs. Besides that the strategy may ensure that a certain percentage of the found C&Cs are linked to a criminal.

4. *Cooperating with law enforcement agencies.*
   As you can see in the two strategies above, governments need also to cooperate with other agencies. This will not be explained here any further.

7.5 Banks

1. *Cooperating with other banks.*
   Banks have an interest in sharing information regarding security breaches with other banks and organizations in order to improve their security. Furthermore, sharing botnet information will is advantageous to them, since banks are targets of financial malware, such as ZeuS and Feodo; mitigation of botnets will thus prevent financial losses.

2. *Making customers aware of phishing.*
   If the customers of banks fall victim to financial malware it will damage their reputation and may lead to loss of clients. Banks therefore have an interest in protecting their clients from falling victim to financial malware. This strategy is similar to the strategy deployed by

companies to train their employees. Banks will change their strategy over the years and make the awareness courses entirely available over the web, if it is not already the case.

3. *Creating safer tools for customers.*
   For the same reason as that banks want to raise awareness of phishing, banks want to ensure that their clients make use of secure web tools. This may happen in cooperation with security companies. However, as cyber security grows, it is possible that banks have their own security teams producing these tools, and that the cooperation with security companies will decrease.

7.6 Security Companies

1. *Creating antivirus programs.*
   Security companies can contribute to protecting users from malware infections by producing up to date antivirus programs. This may happen in cooperation with researchers and universities, since these actors can provide valuable insight.

2. *Cooperating with other agencies*
   Security companies may enter agreements with other agencies regarding the sale of their antivirus and other security related products. For example, the law enforcement has an interest buying security products and the security companies have an interest in selling them. Therefore the security companies may agree to sell their products at a lower price. Furthermore, it is possible that these security companies exchange information regarding botnets and financial malware with other organizations. A similar strategy is used governments, researchers and universities.

7.7 Schools

1. *Course about Cyber Security.*
   Schools and other educational institutions can protect their students from falling victim to various forms of malware by introducing courses on cyber security. These courses will give students a thorough understanding of security risks, and protects them from phishing attacks and other forms of social engineering. Students can be exmaminated to test the effectiveness of the course. This exact strategy is not taken by other actors, but this is similar to user awareness training and awareness campaigns. This strategy will be implemented more and more in the future, given that cyber security is becoming popular and vital to the cyber domain.

2. *Guest lectures.*
   It may not always be necessary give entire courses on cyber security, sometimes it is enough to ask guest lecturers to inform students on specific threats. Students can afterwards to be tested to see the effectiveness of the lectures by asking security related questions. This strategy is similar to user awareness training employed by companies. Since cyber threats are becoming more frequent, these types of guest lectures may become more popular in the future.

8 Return on Security Investment

In this section the Return of Security Investment for one strategy is calculated. Since companies are an actor that can influence the security issue, one of their strategies has been chosen. The chosen strategy is: training employees to create more security awareness (and more specific phishing attacks). In order to calculate the Return on Security Investment, the assumption is made that a certain Dutch organization has 40 employees which need to be trained. Besides that, it is assumed that the training will take place in the evening and that the employees get paid (loan) for it.

The data used for this calculation is not from the data-set of ZeuS and Feodo tracker, but from external sources. But, it is assumed that there is a link between the number of C&Cs and the number of phishing mails that is being send.

8.1 Risk exposure

According to Kaspersky [2014] the risk exposure of a phishing attack is $35.000 for a small business. This includes the costs of hiring professional services, increased downtime, and lost business oppor-

tunities. Since the example company is located in the Netherlands, the costs need to be converted to euros, which results in a risk exposure of €31.222,- per year. Note that the training includes protection from many different attacks and not only phishing, but that is not taken into account here. Besides that, the found risk exposure has a probability of 100%. Since this is not the case in real life, the ROSI is calculated using different probabilities of occurrence (see section 8.4).

8.2 Percentage risk mitigated

To calculate the percentage of risk mitigated, data is used to see how many people provide information to phishing websites before and after the training. According to Sheng et al. [2010] 47% of the people provide information to phishing websites and after a training this percentage is decreased to 28%. This results in a risk mitigation of 47% - 28% = 19%.

8.3 Solution Costs

One part of the ROSI calculation is the costs for following a strategy, also known as solution costs. The chosen strategy consists of a training on security awareness, for example to make employees aware of phishing e-mails. The solution costs consists of two parts. First the costs for the training and secondly the loan costs

According to SecurityAware [2015] a "complete aware training" costs €24,- per participant and includes an intake, 2 hours classical training, text book, exam and a certification. Since there are 40 participants the costs of following the training are: 40 x €24,- = €960,-.

According, to gemiddeld inkomen.nl [2015], the modal income in the Netherlands was €2.695 per month in 2014. This number is used to calculate the loan that the organization has to pay for the training. When assuming that this is a full time salary, an employee costs on average €15,55 per hour. The number of employees that need to be trained is 40 and the training lasts two hours. This means that the training costs are estimated at 2 x €15,55 x 40 = €1244,-.

Together with the training costs of the vendor, the total training cost are €2204,-.

8.4 ROSI

The Return on Security Investment is calculated using formula 1. Filling in the risk exposure, percentage risk mitigated and solution costs that were found in section 8.1, 8.2 and 8.3 results in a ROSI of 169,16% (see formula 2). But, this calculation assumes that the risk exposure has a probability of 100% which is not realistic. So, a graph is created which takes into account that there is a certain chance that a phishing attack occurs. As the probability of risk exposure changes, the ROSI changes as well.

The graph (see figure 3) shows that the investment is worth its money, when the probability is 74,3% or higher. But note that the used data can differ per organization, this was just an example on how organizations can calculate the return of investment of the training strategy.

9 Conclusion

This paper contains the answers of the questions of the assignment of block 3, which is a continuation to the paper produced in block 2. First the security issue and perspective of the assignment of block 2 has been changed a bit to make it more suitable to the data-set (see section 1.1. The new security issue was formulated as: Law enforcement agencies have to fight against ever adapting financial malware and methods of spreading financial malware.

We then described the problem owner of the security issue (see section 3). In the section containing the answer of the second question, we described the relative difference in detection rate over time (see section 4). Section 5 describe strategies that the problem owner can follow the reduce the security issue. Section 6 defined all actors that can influence the security in a positive or negative way. Luckily, most of the actors should be willing the help the problem owner in mitigating or solving the security issue. In section 7 ways to mitigate or solve the issue are given for all those actors. Finally for one of those strategies, training employees within companies, the return on investment is calculated.

In conclusion, this paper analyzed which actors are influencing the security issue, how the issue might be mitigated and the costs related to implementing these solutions.

$$ROSI = \frac{(\text{Risk Exposure} \times \%\text{Risk Mitigated}) - \text{Solution Costs}}{\text{Solution Costs}} \tag{1}$$

$$ROSI = \frac{(€31.222,- \times 0,19\%) - €2.204,-}{€2.204,-} * 100\% = 169,16\% \tag{2}$$

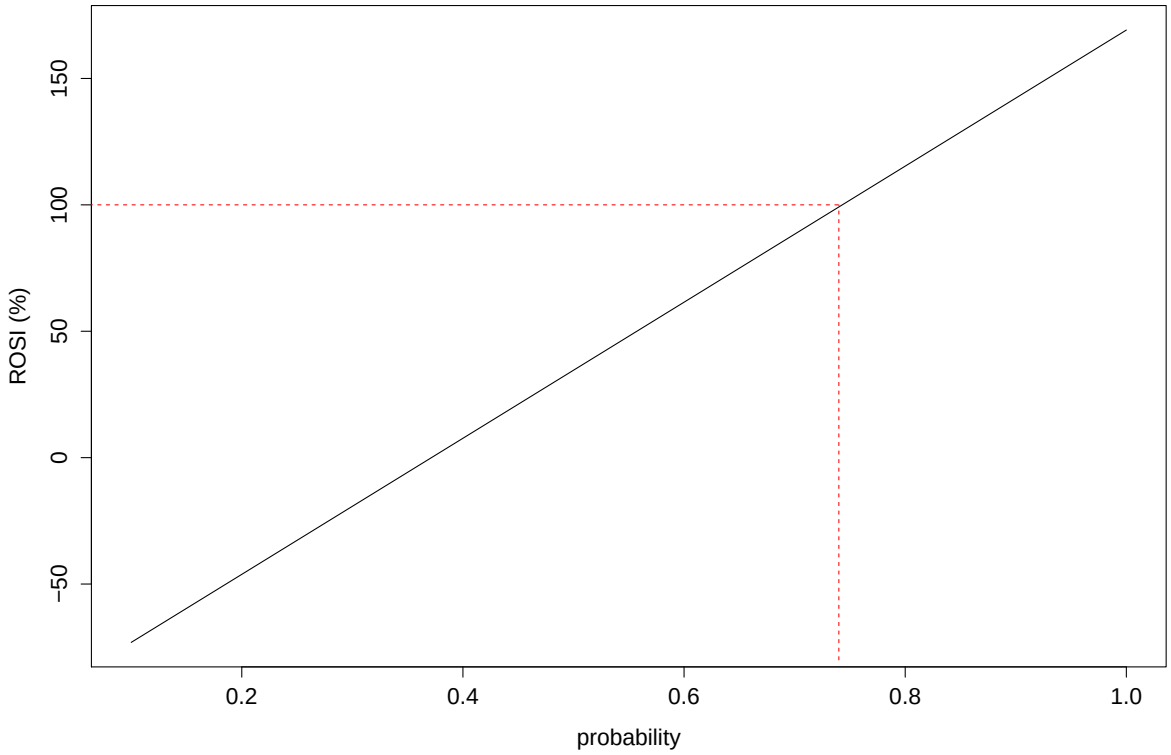

Figure 3: Return of Security Investment

References

FireEye. Operation tovar: The latest attempt to eliminate key botnets, 2014. URL https://www.fireeye.com/blog/threat-research/2014/07/operation-tovar-the-latest-attempt-to-eliminate-key-botnets.html. Accessed: 2015-10-04.

gemiddeld inkomen.nl. Modal income, 2015. URL http://www.gemiddeld-inkomen.nl/modaal-inkomen-2014/. Accessed: 2015-10-03.

Kaspersky. Global it security risks survey of 2014, 2014. URL https://business.kaspersky.com/how-phishing-affects-businesses/3793/. Accessed: 2015-10-03.

Daniel Ramsbrock, Xinyuan Wang, and Xuxian Jiang. A first step towards live botmaster traceback. In *Recent Advances in Intrusion Detection*, volume 5230, pages 59–77. 2008. doi: 10.1007/978-3-540-87403-4_4. URL http://dx.doi.org/10.1007/978-3-540-87403-4_4.

SecurityAware. Security aware complete aware, 2015. URL https://www.security-aware.eu. Accessed: 2015-10-03.

Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 373–382. ACM, 2010.

Symantec. Cutwail takedown cripples bredolab trojan; no effect on spam levels, 2010. URL http://www.symantec.com/connect/blogs/cutwail-takedown-cripples-bredolab-trojan-no-effect-spam-levels. Accessed: 2015-10-04.