Final - Assignment Block 4

Economics of Security (WM0824)
Group 1

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

October 18, 2015

1 Introduction

This paper is about the assignment of block 4 of the course Economics of Security and is a continuation to the papers produced in Block 2 and 3. In the paper of block 2 a general security issue was established using the data-set of the ZeuS and Feodo trackers. Then the metrics which would describe and help evaluate the security issue were analyzed. In the previous paper the variance in security performance in relation to a metric and how different risk strategies can shape this variability has been analyzed. For a short recap of the results of the previous assignments see section 1.1.

This paper aims at understanding the factors influencing this variance, i.e., instead of analyzing what the differences among different actors are, it will be investigated what the underlying reasons behind the existence of these are.

This paper is structured as follows. The general information in the introduction, which also includes a short recap of the previous assignments (see section 1.1) is followed by the methodology of how this assignment will be solved. This also includes a roadmap of how different steps which will be taken (see section 2). Sections 3 to 4 are about answering the questions of the assignment:

1. Select 3 actors (including the problem owner) involved in the security issue and, for each one:
   (a) Identify one concrete countermeasure that they could take to mitigate the security issue.
   (b) Analyze the distribution of costs and benefits among the different actors that the deployment of the countermeasure would entail.
   (c) Analyze whether the actors have an incentive to take the countermeasure.
   (d) 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.
   (a) Identify different factors explaining (causing) the variance in the metric.
   (b) Collect data for one or several of these factors.
   (c) Perform a statistical analysis to explore the impact of these factors on the metric.

Finally, a conclusion is given (see section 5).

1.1 Short Recap of Assignment Block 2 & 3

This assignment builds on the work done in the previous two assignments. In Block 2, we analyzed the data-sets of the ZeuS and Feodo botnet trackers. These trackers attempt to detect and analyze existing *Command & Control centers* (C&C's). From these data-sets, it was chosen to focus on the following security issue: *Law enforcement agencies* *have to fight against ever adapting financial malware and methods of spreading financial malware.* From the perspective of *Law Enforcement*, several metrics were defined that can be used to analyze the security issue. The metrics that can be applied using the data-sets are for example: the increase/decrease of detected C&C's over time and the occurrence of different versions of the C&C's over time.

In block 3, the security issue was expanded on by analyzing all the different actors that influence the security issue. Law Enforcement was chosen as the problem owner and other actors for example governments and security companies were discussed. For all actors, risk strategies were defined which can tackle the issue from the perspective of these actors. For one of the strategies, training employees within a company, a ROSI calculation has been made to determine whether this strategy is efficient for the actor. In this assignment, the defined security issue, the actors and the corresponding risk strategies from the previous blocks will be used.

2 Methodology

To make sure this assignment could be solved properly, a selection of the actors and strategies defined in the previous assignment will be made. For this assignment all questions are answered in the given order and finally, a conclusion is given.

The steps can be summarized as follows:

- Write a short recap of assignment of block 2 & 3;
- Select 3 actors;
- Analyze the strategies per actor;
- Choose one strategy per actor;
- Define a countermeasure for each actor;
- Define actors related to the countermeasure;
- Analyze the distribution of costs and benefits of those different actors;
- Analyze whether the actors have an incentive to take the countermeasure;
- Reflect on the role of externalities;
- Identify an actor whose security performance is visible in the metrics;
- Identify different factors explaining the variance in the metrics;
- Collect data for some factors;
- Perform a statistical analysis to explore the impact of these factors on the metric;
- Write a conclusion.

3 Countermeasure Analysis per Actor

In this section a strategy analysis is given for three actors: law enforcement agencies, governments and security companies. First, for each actor a countermeasure is given and after that, a cost/benefit distribution is given for every actor that is affected by the countermeasure. This distribution is used to determine if the actors have an incentive to contribute to the countermeasure. Finally, the role of externalities around the security issue is described. A total overview of the results can be found in table 4.

3.1 Law Enforcement Agencies

One of the actors that is affected by the security issue is law enforcement agencies. They are also the problem owner of the security issue. Law enforcement agencies can follow multiple strategies to mitigate or solve the security issue, for example: cooperate with other agencies, take down C&Cs, trace criminals, block certain countries or ip-address ranges with high malicious rates and create awareness campaigns.

3.1.1 Countermeasure

A countermeasure for law enforcement agencies can be: take down ZeuS C&Cs. This countermeasure can be deployed actively by law enforcement agencies. This countermeasure directly influences the security metric, i.e. by taking down C&Cs, a decrease in the total number of C&Cs should be seen.

3.1.2 Cost/benefit distribution

There are multiple actors affected with the countermeasure described above, these are: banks, companies, government, security companies and law enforcement agencies. For all of those actors costs and/or benefits are shown in table 1. Companies and banks (actually their customers) benefit from

Table 1: Cost-benefit distribution for taking down ZeuS C&Cs

Actor	**Costs**	**Benefits**
Banks	-	Lower chances of customers becoming a victim
Companies	-	Lower chances of becoming a victim
Government	Budget for law enforcement agencies	Higher national safety Lower crime rates
Security companies	-	Income More knowledge on financial malware
Law enforcement agencies	Working together with security companies	Getting a better reputation Lower crimes rates

this countermeasure by having lower chances of becoming a victim of ZeuS. As can be seen, the costs for this countermeasure lie at the side of the government, since they make a budget for the law enforcement agencies to work on when taking down ZeuS C&Cs. In return of those costs they hopefully will benefit of this countermeasure, by lower crime rates and finally increasing national security. Law enforcement agencies also have costs when they want to cooperate with security companies, they can use the budget they get from the government for this. When taking down more ZeuS C&Cs law enforcement agencies can lower the crime rates and can get a better reputation. Finally, security companies can help law enforcement agencies with taking down ZeuS C&Cs, in return they get paid for it and gain more knowledge on financial malware.

3.1.3 Actor incentive

All actors who do not have costs have an incentive, since they benefit from the countermeasure without losing something. For the law enforcement agencies and government there are besides the benefits, also some costs. The governments allocate a budget for the law enforcement agencies to take down ZeuS C&Cs. On the other hand this may result in a higher national safety and lower crime rates, thus they have an incentive. The budget of the government can by law enforcement agencies be used for working together with security specialist/companies. Next to that, the benefits may be that they get a better reputation and lower crime rates, so, law enforcement agencies also have a incentive.

Concluding, all actors (banks, companies, government, security companies and law enforcement agencies) have an incentive. But, for government and law enforcement agencies the incentives may be lower, since they have costs for this countermeasure.

3.1.4 Externalities

Besides the direct actors there are also some externalities who perceive negative or positive effects of the countermeasure. First, there are attackers/botnet owners who are influenced by and respond to take down of ZeuS C&Cs. If they want to continue their crime, they have to make sure new C&Cs are set up, which results in more work for the law enforcement agencies. So law enforcement agencies actually have to catch those attackers, to make sure they do not perform the crime again. Another externality are hosting providers, they are not directly linked to the countermeasure, but will perceive some positive effects when law enforcement agencies take down ZeuS C&Cs. For example, when multiple C&Cs on their host are taken down quickly, they suffer less reputational losses, because the public has less time to find out the hosting provider might not be secure and productivity loss, because they do not have to investigate the hosts themselves.

3.2 Governments

Another actor that is affected by the security issue is the government. There are different strategies that governments can follow to positively influence the security issue, for example: cooperate with law enforcement agencies and take down C&Cs or trace criminals and create awareness campaigns.

3.2.1 Countermeasure

Awareness campaigns consists of multiple parts, for example: radio commercials, television commercials, posters in cities and a website with information about financial malware. One countermeasure governments can take is informing civilians about financial malware using television commercials.

3.2.2 Cost/benefit distribution

There are three actors affected with this countermeasure, namely: civilians, television channels and government. First governments have to create one or multiple television commercials which bring costs for them, but also may result in less victims of financial malware and a higher national security. Then television channels will broadcast the commercials, which is an income for them. Finally, civilians will see the commercial on their television and are being informed about financial malware and hopefully will be more aware of financial malware. The distribution between those benefits and costs can be found in table 2.

3.2.3 Actor incentive

Civilians and television channels do have incentive for this countermeasure, since they only perceive benefits. The government may have an incentive, but that depends on the level of costs. When other countermeasures, for example posters in cities are cheaper and reach the same amount of people they may consider doing that instead of television commercials.

3.2.4 Externalities

When television commercials are broadcasts, civilians will see it and hopefully do not become the victim of financial malware anymore. When civilians become more aware of financial malware, this also have a positive effect on the companies the civilians work and the banks they are a customer of. Attackers will perceive a negative effect, since they have to find other ways of spreading the financial malware. Security companies may be negatively affected by this countermeasure since less financial malware attacks may happen, which results in less jobs for security companies.

3.3 Security Companies

Security companies can also positively influence the security issue and they also can follow multiple strategies. Examples of those strategies are creating antivirus programs and cooperate with other agencies.

3.3.1 Countermeasure

A countermeasure that security companies can create is: developing and selling antivirus programs. Note that there are also free antivirus programs, but those versions often have less functionality than the versions that have to be paid for.

3.3.2 Cost/benefit distribution

There are three kind of actors that will be affected by the countermeasure. First there are customers who can buy antivirus programs. They can also take the free antivirus program, but it is less secure. Customers include companies, banks, civilians and law enforcement agencies. Another actor that is affected by the countermeasure is the government. They also can buy the antivirus program, which results in a better protection. Besides that, the benefit for them is that there is a higher national security. Finally, the security companies have to create and sell the antivirus programs which also results in some costs. The positive side of selling antivirus programs is that the security companies get income and gather more information about financial malware. In table 3 the cost-benefit distribution for the mentioned countermeasure can be found.

3.3.3 Actor incentive

Customers have the cost of buying an antivirus program, but also the benefit of better protection. The incentive for them depends on how well they want to be protected. Since there are also free antivirus programs, they can decide to take that one. For Governments the above reasoning holds as well.

Table 2: Cost-benefit distribution for television commercials

Actor	**Costs**	**Benefits**
Civilians	-	Being informed about financial malware Lower chances of becoming a victim
Television channels	-	Income
Government	Creating television commercials	Higher national security Less victims of financial malware

Table 3: Cost-benefit distribution for antivirus programs

Actor	**Costs**	**Benefits**
Customers	Purchase antivirus program	Better protection
Government	Purchase antivirus program	Better protection Higher national security
Security companies	Developping antivirus programs Selling antivirus programs	Income More knowledge about financial malware

Next to that, it will result in a higher national security when security companies create and sell better anti-virus programs. So, governments do have an incentive. Security companies have to create and sell the antivirus programs, which brings some costs, but also income when enough programs are sold. When developing the programs, they may gather more information about financial malware. They have to make a consideration in creating and selling antivirus programs or not, the incentive depends on that decision.

3.3.4 Externalities

Criminals may be influenced by the countermeasure, but are not directly an actor linked to the countermeasure. When trojans can be found more easily by antivirus programs, criminals have to develop new trojans, which are harder to detect or decide to stop creating trojans and try a different tactic altogether.

4 Security Performance

In this section a type of actor is identified whose security performance is visible in a chosen metric. After that, different factors explaining (causing) the variance in the metric are described. For some of those factors data is collected to perform a statistical analysis to explore the impact of these factors on the metric.

4.1 Actor and Metric

In the previous assignments, several metrics were discussed related to the ZeuS and Feodo datasets (see also section 1.1). From some of these metrics, it can be observed that they are influenced by the actions of actors. Law enforcement, for example, has effect on the decrease of C&Cs depending on their performance in taking down these servers. Another example is the difference in performance between law enforcement agencies in different countries. Since these performances differ, the actors influence on the metric should also be different, hence it should be measurable.

Since most of these metrics, like the increase/decrease of C&Cs and distribution of C&Cs per country, have a direct correlation with the actions of the law enforcement, the security performance of this actor is chosen to be analyzed.

4.2 Different Factors

4.2.1 Increase

The following factors have a effect on the increase of Command & Control servers.

- Free/lower costs for web hosts
  Criminals need web hosts to place dropzones for their corresponding C&Cs. As the prices for web hosting come down, or web hosting is offered for free, criminals will have a higher incentive to use malware which needs web host-

Table 4: Countermeasure analysis per actor

Actor	**Strategy**	**Affecting actor**	**Incentive**
Law Enforcement Agencies	Take down ZeuS C&Cs	Banks	+
		Companies	+
		Government	+-
		Security Companies	+
		Law Enforcement Agencies	+-
Government	Television commercials	Civilians	+
		Television channels	+
		Government	+-
Security Companies	Developing and Selling Antivirus Programs	Customers Government Security Companies	+- +- +- +- +- +

ing. The ZeuS trojan is an example of this. Thus, as prices for web hosting decrease, there should be an increase in the number of C&Cs.

- Easy access to crimeware kits
  As ZeuS develops, it becomes easier for criminals to install and set up a C&C. The ZeuS trojan comes with an installation guide and thus the technical background of the criminal does not need be very advanced. Criminals will be more inclined to use malware which is easier to deploy. Also, as the installation process becomes easier, the malware will attract a larger audience of criminals.
- More criminals
  As the number of normally distributed criminals increase, there should be an increase in the number of criminals using financial malware. Thus, the number of C&Cs will change.

4.2.2 Decrease

The following factors have a effect on the decrease of Command & Control servers.

- Hosting providers take down C&Cs
  The act of taking down C&Cs directly influences the metric. When a certain C&C is taken down, at least all infected hosts related to that C&C are no longer vulnerable.
- Criminals decided to take down the C&C by themselves
  See above.
- Law enforcement agencies take down C&Cs
  Besides the general consequences of botnet take-down as shown above, the effect of take-down by law enforcement might bring forth some extra characteristics. A take-down operation often looks into behavior or specific elements of a certain botnet type, causing a chain reaction. Therefore, this factor might cause a propagating drop in active C&C's.
- Higher prices for web hosting
  As the prices for web hosting increase, criminals will have more costs for setting up drop-zones. This may affect their incentive to use ZeuS as their desired tool for criminal activities.
- More criminals traced
  When law enforcement agencies are getting better at tracing criminals, the incentive of criminals should drop. The number of C&Cs should decrease as well.

4.3 Data Collection

The above section looked at factors which either increased the C&C count or decreased it. To analyze the impact, two factors have been chosen; one factor which increased the C&C count and one which decreased it: (1) free/lower costs for web hosting and (2) the take-down of C&Cs by law enforcement (possibly in cooperation with other organizations).

These two factors have been chosen so that two types of impact can be statistically analyzed. Firstly, this paper will analyze a factor which possibly increases the security problem. Data for this should be readily available on the Internet since web hosting has become increasingly popular. Secondly reports of C&C take-down operations are available on the internet. By analyzing their dates and the size of the operation, an analysis of the impacts of such operations can be made.

The rule of law indicates how well law enforcement is performing per country. It is based on several factors. One of these factors is 'Order and Security', which includes how effective crime is controlled. Evidently, this is in line with C&C takedown. (analyse: map roli naar dataset en kijk of landen met veel C&Cs lage roli index hebben)map roli naar dataset en kijk of landen met veel C&Cs lage roli index hebben)

4.4 Statistical analysis

This section will initially look at botnet takedowns and view the impact of a takedown on increase of the number of C&Cs per country. This in turn is mapped to the ROLI index. Then the appearance of new free web hosting services is checked against variation in the increase/decrease of C&Cs per country.

Botnet Takedowns In the previous assignment a normalized set of C&C's per country was constructed (Figure 1). If the rule of law in countries with high C&C peaks is low, and vice-versa, then rule of law might be a statistically significant aspect of botnet take-down.

Operation Tovar was a takedown operation conducted in June 2014 with the help of various organizations and governments. This data can be matched with the graph showing the increase/decrease of C&Cs (figure 2). It can be seen that initiative of the law enforcement institutions in the various countries, together with universities, security companies and other organizations had a small impact on the number of detected C&Cs. However, quickly after the takedown operation, the number of detected ZeuS C&Cs increases again. It can thus be said, that the takedown operation maybe certainly impacted the botnet infrastructure, however, this did not impact the overall problem that new C&Cs are being set up with different configurations.

Web hosting prices in different countries A study done by `royal.pingdom.com` shows the difference in prices between hosting in 2008 and hosting in 1998. We can compare these prices again to the prices of today. The study reveals that there is no major change in the prices itself, but only big changes in the volume of data being transferred. For the same price, larger storage spaces and data rates can be acquired.

This however is not relevant to cyber criminals wanting to deploy ZeuS. They have no benefit from having more storage space, since all they need is enough space to store a dropzone file. The introduction of free webhosting might explain an increase in the faster appearing C&Cs.

The number of free webhosting providers has nearly doubled in 2013 compared to the number of providers in 2005

5 Conclusion

This paper looked at different actors influencing the metrics and focused on the countermeasures. It analyzed the different countermeasures per actor, and which actors have the incentives to deploy which countermeasures. Then the cost/benefit distribution of these countermeasures is looked at per actor. The second part of the paper looked at factors influencing the metric and how they impact the metric. The paper analyzed the performance of the law enforcement by looking at Operation Tovar and how it changed over the years. It also looked at how the web hosting prices has changed over the years and how this relates to the metric.

References

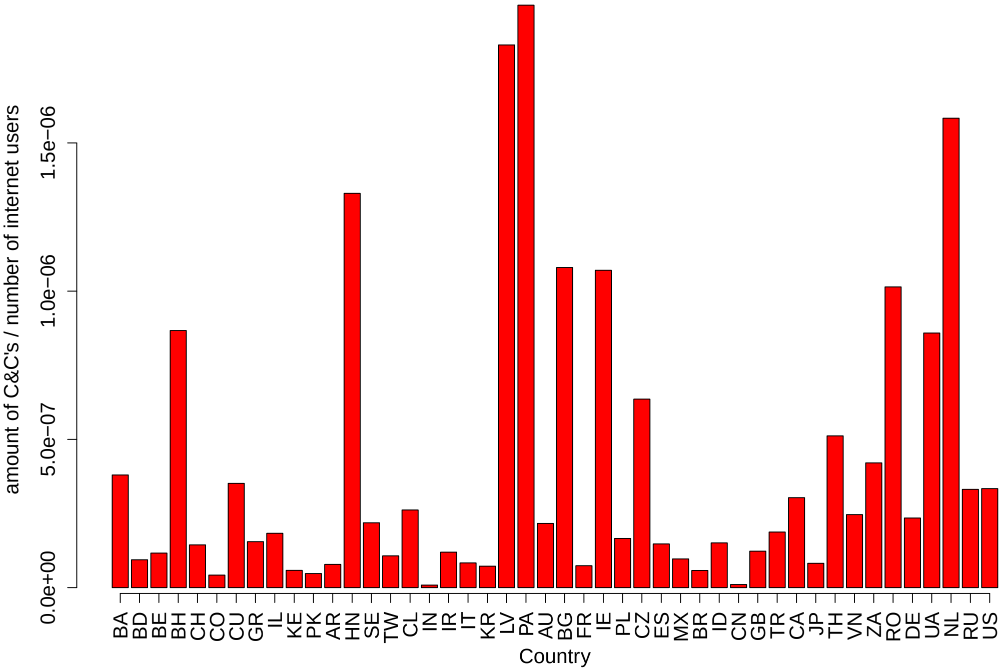

Figure 1: Normalized C&Cs per country

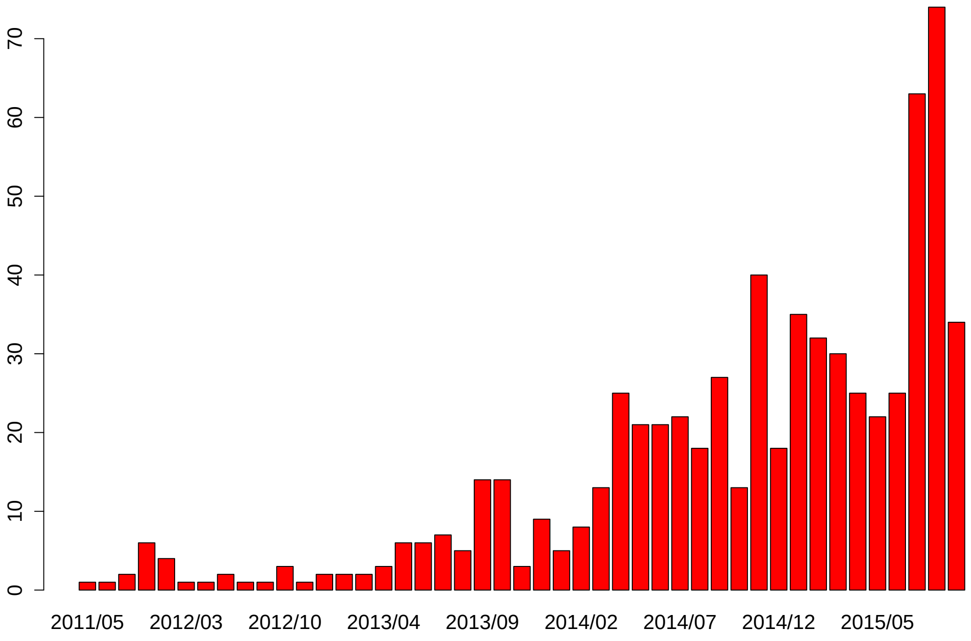

Figure 2: Detected ZeuS C&Cs per month