Individual Assignment

Economics of Security (WM0824)

Joris Diesvelt (s1007114)
Member of Group 1

November 10, 2015

Abstract

This research concerns the effectiveness of botnet take-downs in terms of the attacker response, where an attacker response is defined as a factor of the response delay, the botnet growth after a take-down and the time to reach its original size. A literature study concluded that there has been criticism on botnet take-downs by the security industry and that there are many factors involved when measuring the effectiveness of such actions. A statistical analysis is formulated to estimate the average attacker response after a ZeuS botnet take-down. This analysis is evaluated using the ZeuS Tracker dataset and information about the B71, B54 and Tovar operations. It was hypothesized that attackers respond to these countermeasures within a week, however, the results show that this is more likely to be two weeks. Furthermore, the average botnet growth was expected to be defined as a linear function, which the results confirmed. The estimation that botnets would reach its original size in less than 6 months after a take-down could unfortunately not be confirmed with the given dataset. Finally this report discusses the limitations of the tools and methods that were used.

1 Introduction

In the Economics of Security course, we had a look at the economic aspect of cyber security related subjects. For the course project, we were given a dataset and several assignments, which required analysis of this dataset and doing research in different areas surrounding the security issue that this dataset speaks to. We will first summarize all our findings from the previous assignments before we introduce the individual and also the last assignment.

Starting the project, we were given two datasets: ZeuS Tracker [2] and Feodo Tracker [1]. The intention behind both trackers is detecting Command and Control (C&C) servers for the ZeuS and Feodo botnets. Researchers can make use of these dataset to perform analysis and companies can use it to strengthen their defence against botnet infections. The purpose of botnets, C&C's, the trackers, ZeuS and Feodo will be explained for in section 3.

Following the intention of the trackers, we defined a possible securiy issue as: *Law enforcement agencies have to fight against ever adapting financial malware and methods of spreading financial malware.* For this issue, we defined several actors that influence it in some way with countermeasures. One major actor is the law enforcement agencies which attempt to take down botnets, track criminals who operate these botnets and protect civilians and other computer users against infections by them. For these countermeasures, we analysed the cost and benefits and following, we determined the incentives for these countermeasures per actor based on this cost/benefit analysis.

As one can expect, the actor incentive is higher when the benefits outweigh the costs for a certain countermeasure. As we figured out during the course however, both the benefits and costs are not always easy to determine and sometimes countermeasures can have a more negative impact on the actor as previously thought.

In this assignment, we dive deeper into the aforementioned countermeasure of taking down botnets. To make a decent cost/benefit analysis for a take-down, an actor needs to make a reliable estimate of the benefits for this take-down. In section 3, we will investigate why this is an issue for organisation and what has gone wrong with these estimates in the past. Using this research we will create a new formal way of estimating the effectiveness of previous botnet take-downs based on the attackers response (see section 4). This goal and our hypothesis is further explained in section 2. Finally, after we have defined our results in section 5 we will discuss the limitations found doing this research and possible improvements for further studies (see section 6).

Note that in this study, we do not restrict ourselves to just the law enforcement agencies as actor, but also include companies and other institutes that have an interest in taking down these botnets. This is because these actors often work together on this countermeasure, for example the combined effort to take down the SIMDA botnet in April this year [8], which was an collaboration between Trend Micro, INTERPOL, Microsoft, Kaspersky Lab and the Cyber Defense Institute.

2 Research Question, Objective and Hypothesis

As introduced in the previous section. The goal of this research is to find the effectiveness of botnet take-downs in a new way. Namely on the basis of attackers response. This brings us to the first research question.

1. **What is the effectiveness of botnet take-downs in terms of attacker response**

To answer this question, we will do a literature study (see section 3) and find out what the effectiveness of several botnet take-downs in the past were and how the adversaries responded to these take-downs. To do this, the attacker response is defined as a combination of three variables.

- **Response delay**
  The time delay between the take-down of Command and Control server and the first action taken by the attackers.
- **Botnet growth after delay**
  The growth of for example the number of C&C's after the attackers first responded to the take-down. More specifically, the botnet growth can be defined as a function of total number of C&C's in time.
- **Time to reach original size**
  The period in which the botnet reaches the same size it had before the take-down. In case the botnet never reaches its original size, this variable can become infinite.

Using these definitions we want to give a meaningful measurement for the attackers response in this research by evaluating these parameters with knowledge from past take-downs. Doing so, we attempt to answer the second research question.

2. **What is the average attacker response to a botnet take-down**

Combining the results from section 5 and possible further research (build upon the limitations and improvements given), this study can be used for law enforcement agencies, security companies and institutes to gain more insight in the effectiveness of botnet take-downs.

2.1 Hypotheses

As we attempt to answer the second research question with relevant data and metrics, a hypothesis can be created to express our expectancy of the results. As the second question concerns the average attacker response, we define the hypothesis in terms of the three variables we defined earlier.

- **Average response delay**
  We expect attackers to react quickly to take-downs, or more specifically, in less than a week.
- **Average botnet growth**
  As discussed previously, botnet growth can be realized as a function of total C&C's against time. We expect this function to be at least linear. Or in other words, after the response delay and the first new C&C's are set up, the number of newly created C&C's in time will not slow down before the botnet has its original size.
- **Average time to reach original size**
  We expect that due to the attacker effort, the average time before the botnet reaches its original size, is less than six months.

Since the given dataset concerns the ZeuS botnet, we will limit the study to attempted take-downs on this botnet. After we have concluded our findings, it can be shown that our hypothesis was right or that our estimates are off. In both cases, the results can be compared to the literature study and it can be concluded whether this method gives a meaningful insight to the security issue.

3 Literature Study

Before we can summarize the existing research on the security issue, we need to establish basic concepts that will be used. A "bot" for example is a piece of malware that is used by an attacker to gain access to an infected machine. This infection usually happens via an exploit or by triggering the user to execute the malware. A network of these infected machines controlled by a single attackers is referred to as a "botnet" [4]. Botnet owners can use the network to let each infected machine do certain tasks, which the attacker would not have the capacity to do without the network. This is the basic setup for, for example, DDoS attacks and bulk spam. Another type of usage is financial fraud. In this way, the malware spies on the users activity on the web and tries to steal financial data, such as the users credentials. To receive instruction or send the intercepted data, bots communicate with a central server, commonly named a Command and Control server [4].

In case of traditional botnets it was difficult for an attacker to set up such a network, because developing the bot and setting up the C&C's was a daunting task. Nowadays, many open source "construction kits" exist which makes it trivial for an adversary to create a new botnet [3]. This is one of the reasons why botnets have been growing rapidly the past years [7]. ZeuS is an example of such an open source botnet and its size is roughly estimated as 3 600 000 bots in all networks [6].

As a botnet requires C&C's to fully operate, removing these servers sound like a viable method of bringing down the network. There are two main countermeasures to achieve this, C&C server takedowns and DNS-based blocking [3]. The former method requires removing the server in its entirety. To achieve this, many cooperation's are needed between Internet Service Providers and Law Enforcement, because legal issues often hinder access to servers. Attackers make use of the law in different countries to effectively protect their servers, which is why these C&C's are often referred to as "Bulletproof Hosting". The second method does not require physical access to the actual servers but blocks routing towards them by removing the domain names from registrars. This circumvents certain legal issues, however, it only works on botnets depending on DNS mechanisms [3].

3.1 Effectiveness of Botnet Takedowns and Criticism

Some research has been conducted to investigate the effectiveness of take-down actions. One example is the elaborate study by Georgia Tech, College of Computing [9]. The researchers acknowledged the difficulties of the proper way to take down botnets and formed a new method of determining their effectiveness. A post-mortem analysis was performed to show the potency of their method.

The previously cited research was done in cooperation with Damballa[1], a spin-off from Georgia Tech. They cited three main reasons why botnet take-downs are ineffective. For one, the organizations that perform the take-downs often do not remove the threat completely. While a portion of the botnet can be taken down, the remaining network can still be strong enough for the attacker. Furthermore, if the critical infrastructure of the botnet is not completely removed, the adversary can repair the damage more quickly. In doing so, organizations also may destroy possible leads that other organizations use, such as sinkholes. Sinkholes are in essence C&C's that are taken over by a party other than the attacker. Since the functionality of the C&C is not changed, bots communicate normally to the sinkhole. Researchers can then use data from the sinkhole to analyse the botnet.

Another reason for ineffectiveness is the inability of organizations to take secondary communications into account. Some botnets have backup communication systems to cope with the loss of parts of the network infrastructure. Removing the primary source of communication proves to be ineffective with such botnet types and may irreversibly dam-

[1] Damballa: `https://www.damballa.com/`

age the potential to destroy the botnet in its entirety.

Finally, Damballa states that take-downs are ineffective when the botnet owner is not arrested. As the perpetrator is not caught, nothing stops him from creating a new botnet, essentially nullifying their actions.

In March 2012, Microsoft executed operation B71, one of the biggest operations against the ZeuS botnet. Several C&C's were taken down and hundreds of domains were secured. One could reason that this was a big blow to the affected botnets and that the operation was a success. Dutch security company Fox-IT had a different opinion though [5]. They stated that Microsoft published false and misleading information, that they invaded privacy and overall took irresponsible actions. Fox-IT argues that the operation possibly did more damage to the security industry than it tried to repair. Their criticism resembles the points stated by Damballa. Only a portion of the network was taken down, no communication with other parties might have lead to other research being destroyed and the attackers were not caught.

To summarize, many factors determine the effectiveness of botnet take-downs. Research has been done to show how these actions can be ineffective and can also do more damage than intended if the acting organizations are not careful. We can therefore state that determining the effectiveness of a possible botnet take-down is needed and to do this, we can use our experience with criticised actions from the past.

4 Research Design

Our objective for this study is to find a way to express the effectiveness of botnet take-downs in terms of attackers response. With the research questions, three variables were defined that can quantify this response. We can now attempt to use data from datasets and data from previous take-down operations to create a quantitative analysis.

4.1 Quantification Method

The first variable is the average attackers response delay. This can easily be calculated by summing up all the delays after each operations and dividing them by the total number of operations. If we have a sufficiently large dataset, these values could also be used to make a delay distribution. By calculating the mean value and the standard deviation, this distribution can be used to estimate the probability of a certain delay. As our number of samples (e.g. number of take-down operations) is not large enough, this is not possible.

The second variable is the botnet growth. We can measure this by finding all newly set up C&C's after the take-down operation, and finding a trend line through this growth. Using regression analysis, we can check how this trend line compares to the actual data samples. As our hypothesis states that we expect at least linear growth in newly found C&C's, a linear trend will be calculated and its corresponding r^2 value.

The time to reach its original size can be calculated by finding the difference in time between the amount of C&C's before the take-down operation, and the earliest occurrence where the botnet has achieved this same size again. As with the response delay, it is possible to generate a frequency distribution when enough data samples are available.

4.2 Take-down Operations

As this research is restricted to only the ZeuS botnet, only take-down actions on the ZeuS botnets are taken into account. In the past five years, there have been three major operations, which are carried out by multiple cooperating organizations. Microsoft is one of the active members behind these take-downs and has published information about these actions. The operations are, in order of executed, operation B71 (March 2012), operation B54 (June 2013) and operation Tovar (June 2014).

4.3 Dataset

The dataset being used is extracted from the ZeuS Tracker [2]. Unfortunately, there are several problems with the available data. Aside from being incomplete and possibly inaccurate, the necessary data needed for this study is not available.

Ideally, we would like a dataset containing the amount of online C&C's for each day. The ZeuS Tracker is able to show this data, but only for a 60 day period ending on the current date and there is

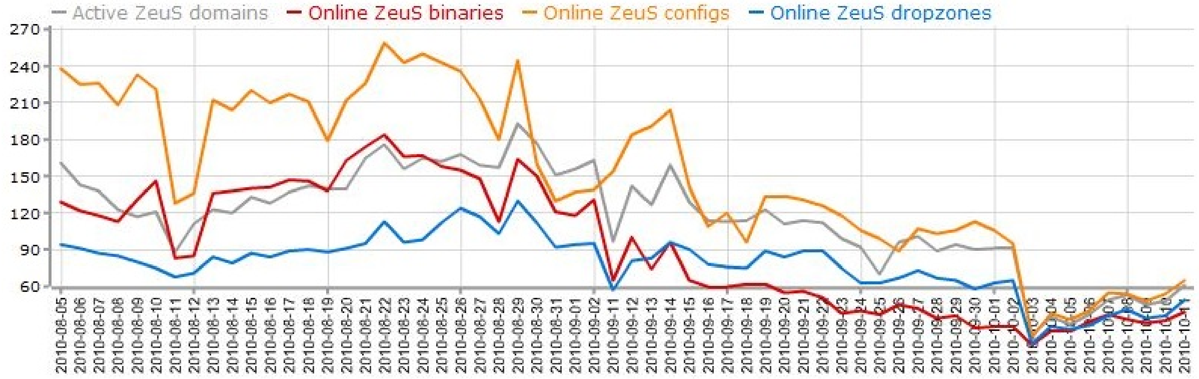

Figure 1: Snapshot of the ZeuS Tracker on 12/10/2010

no option to retrieve data from the past. Figure 1 shows a snapshot of this chart, found by chance on an archiving website. As can be seen, from this chart it is immediately visible when an action has taken place, as there is a sudden drop in active C&C's.

The data that is available, are all servers that are active on the current day. This data includes the day that the servers has been added to the database and thus can be used for our research. Unfortunately, this data is not very accurate, considering many of the servers that have been found on a certain day have since been removed (either because they have been cleaned, or permanently suspended). The ZeuS Tracker does keep track of all these removals, although only the last 300 removals can be requested.

In short, we can only use the data from ZeuS Tracker containing the servers that are still active today and we use the date that these have been added in our results. The implications of the unavailability of data will be explained more in the results and limitations sections.

5 Results

From the dataset, we can gather the number of days before the first new set up C&C's appears after the operation has taken place. For the operations B71, B54 and Tovar, these values are 31, 5 and 3 days respectively. This gives an average of 13 days of response delay. These results can also be seen in table 1.

Our hypothesis stated that we suspected an average response delay lower than 7 days. According to these results, the average delay is actually twice as long. However, during this analysis, a major problem with our data becomes visible. As out dataset contains only servers that are still active today, one can imagine that servers that have been set up recently have had less time to be investigated by defenders. In other words, servers that are older have a higher chance of already been removed. Therefore, directly after operation B71 has taken place, many new C&C's could have been set up, but have been blocked/removed since. The results are therefore not very reliable to be accurate.

Table 1: Attackers response delay

Operation	**First new C&C set up**
B71	31 days
B54	5 days
Tovar	3 days
Average	**13 days**

Following up, we measured botnet growth by plotting the newly found C&C's directly after each operation against the day that they have been found. This results in figures 2, 3 and 4 for the operations B71, B54 and Tovar respectively. These figures also contain the cumulative graph, to show the size of the botnet after each time-frame.

To show the growth of the botnets after a takedown, we calculated the estimated linear trend, which are shown in figures 5, 6 and 7. Each graph

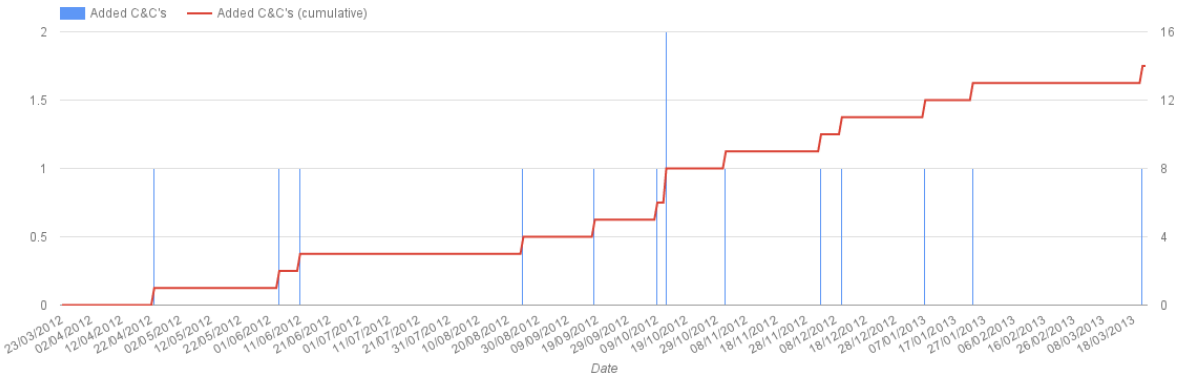

Figure 2: ZeuS C&C's added by ZeuS Tracker after operation B71 vs Date

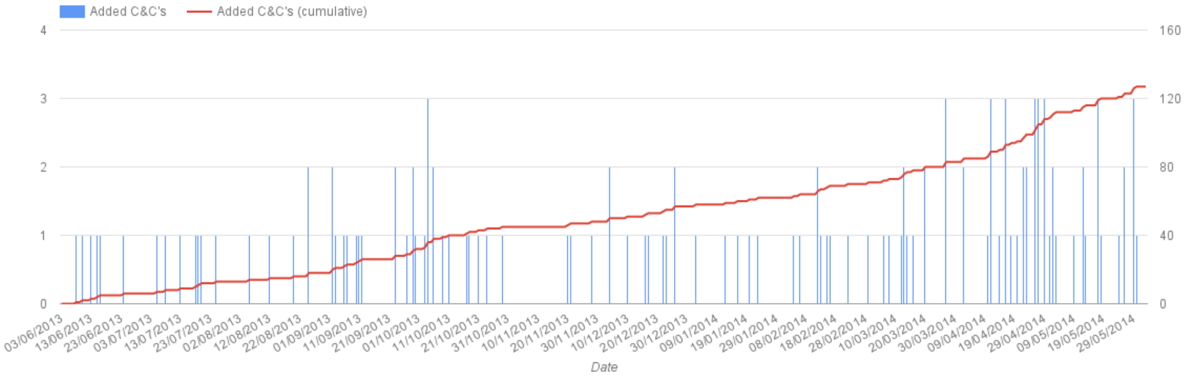

Figure 3: ZeuS C&C's added by ZeuS Tracker after operation B54 vs Date

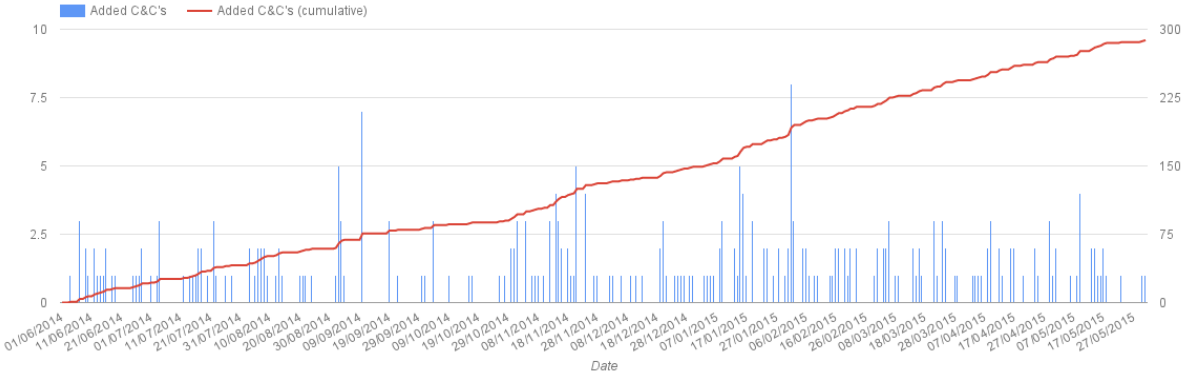

Figure 4: ZeuS C&C's added by ZeuS Tracker after operation Tovar vs Date

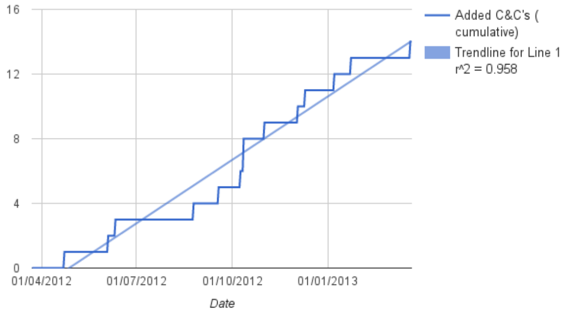

Figure 5: Fitted linear trend for the cumulative additions after operation B71

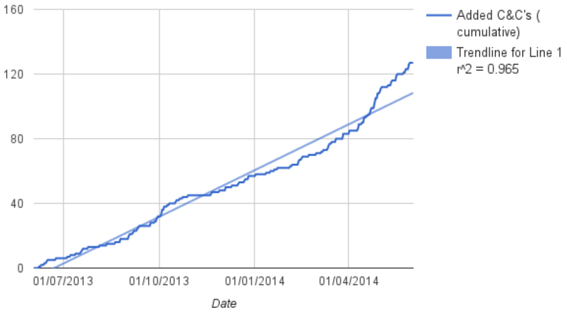

Figure 6: Fitted linear trend for the cumulative additions after operation B54

also shows the corresponding r^2 value, to show the correlation between the data and the linear function.

From these graphs, we can interpret that the results closely resembles our hypothesis. Each function seems to have a close correlation to the dataset and thus the botnets indeed grow linear after a takedown. As can be seen in figure 6, the botnet grows even more than linear 10 months after the take-down.

However, just as we discussed before, we do not have any information on the removals of servers in these periods. Therefore, the results do not have to be accurate. We can also observe the same phenomenon that happened when measuring the attackers response delay. Namely that the more recently occurred actions have more data points, which can suggest one of two things. Either the botnet has been growing more rapidly after more recent take-downs, or there are more data points because newer C&C's have had less time to be cleaned, as said before. Both cases are viable options and without the necessary data, we cannot conclude whichever is true.

Finally, we wanted to calculated the period in which the botnet attained its original size after the take-down countermeasures. Unfortunately, as said before, data is not available in terms of botnet size on certain days in the past. As we cannot measure the botnets size on specific days, we can neither measure their difference in time. The third part of our hypothesis, the average time for the botnet to reach its original size, is therefore inconclusive.

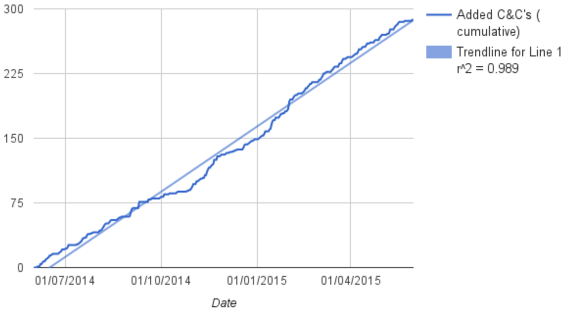

Figure 7: Fitted linear trend for the cumulative additions after operation Tovar

6 Limitations

During this study, many limitations have been found that have influenced the methodology and the results. In this section, we discuss these limitations and suggest possible improvements for further research.

6.1 Limitation of Botnet Trackers

The first limitation to this security issue is the availability of botnet trackers. In the beginning of the Economics of Security course, we were given two trackers, ZeuS Tracker and Feodo Tracker. Aside from the limitations of ZeuS Tracker as discussed below, there is the problem that not much other trackers are available. The Feodo Tracker has much less functionality than the ZeuS Tracker and aside from those two, no other alternatives could be found. This is also an issue for studies like these in general. As there are no effective trackers available, no data can be gathered. It would thus be beneficial for the security industry as a whole to develop more and better botnet trackers.

Even though the two aforementioned trackers attempt to perform as well as they can, there is also the issue that attackers do not take kindly of these trackers as they might cause a problem for them in the future. Therefore these attackers try to obstruct the trackers by frequently attacking them with DDoS attacks, as organizations have observed [10].

6.2 Limitation of Available Data

As is mentioned in the Research Design and Results sections, the available data from the ZeuS Tracker was not sufficient for this research, which let to inconclusive results. The tracker was not defined for this specific purpose and thus lacks the necessary functionality to support this study.

Aside from the problems with the trackers already mentioned, these botnet trackers in general have others issues. For one, it cannot be guaranteed that the tracker captures all Command and Control servers of a certain botnet that exist. Also, the servers that are captured do not always have to be infected. False positives can sometimes be generated which results in inaccuracies in the dataset. Finally, for this specific research, a tracker is required that captures newly found C&C's within a day of being online. The ZeuS Tracker however, has already advanced as much the last years that it can detect new C&C's in mere minutes [11].

6.3 Time constraints

A final limitation for this study is the time constraint. As this is not a full research but a part of a project, limited time is given to complete the assignment. When more time is available, a more thorough study can be conducted. One improvement for further research could be to establish contact with *abuse.ch*, the people behind the ZeuS and Feodo Trackers, and create a better dataset with a joint effort.

7 Conclusions

During the Economics of Security course, we developed the security issue of Law Enforcement Agencies that have to fight against adapting malware. We established the actors, possible countermeasures, their costs/benefits and their incentives concerning this issue. With this research, we attempted to get more insight into the effectiveness of botnet take-downs, by looking at the attackers response.

Two research questions were created, the first being: "What is the effectiveness of botnet take-downs in terms of attacker response". To answer this question, a literature study was conducted. The main findings is this studies were that modern open source botnets can easily be created and traditional methods of taking down these botnets no longer suffice. Take-downs have proven to often be ineffective, due to the fact that attackers are not being caught and they can relatively easy rebuild their botnet. Also, many countermeasure are being criticised by the security industry.

The second research question was: "What is the average attacker response to a botnet take-down". A quantitative analysis has been proposed to give an answer to this question. Using the dataset from the ZeuS Tracker and the information about three botnet take-down operations B71, B54 and Tovar we evaluated this analysis.

Our hypothesis for the second question was that the average response delay for an attacker was less than a week. This turned out to be two weeks, thus we estimated this too low. It was also hypothesized that the average growth of botnets after a take-down could be expressed as at least a linear function, which turned out to be true, according to the results. As the dataset contained insufficient information, our third hypothesis (the average time a botnet reaches its original size is less than six months), remains inconclusive.

Finally some limitations were listed that constrained this research. There are limited botnet trackers available and the data that they often is not always reliable, accurate or complete. For further research, better botnet tracker need to be developed for this specific purpose or contact needs to be established with other organizations such as *abuse.ch* to conduct research in a joint effort.

References

[1] abuse.ch. Feodo tracker. https://feodotracker.abuse.ch/. Accessed: 2-11-2015.

[2] abuse.ch. Zeus tracker. https://zeustracker.abuse.ch/. Accessed: 2-11-2015.

[3] Christian Czosseck, Gabriel Klein, and Felix Leder. On the arms race around botnets-setting up and taking down botnets. In *Cyber Conflict (ICCC), 2011 3rd International Conference on*, pages 1–14. IEEE, 2011.

[4] F-Secure. A quick guide to botnets - what they are, how they work and the harm they can cause. https://www.f-secure.com/en/web/labs_global/botnets. Accessed: 4-11-2015.

[5] Fox-IT. Critical analysis of microsoft operation b71. http://blog.fox-it.com/2012/04/12/critical-analysis-of-microsoft-operation-b71/. Accessed: 5-11-2015.

[6] Ahmad Karim, Rosli Bin Salleh, Muhammad Shiraz, Syed Adeel Ali Shah, Irfan Awan, and Nor Badrul Anuar. Botnet detection techniques: review, future trends, and issues. *Journal of Zhejiang University SCIENCE C*, 15(11):943–983, 2014.

[7] SC Magazine. Botnet takedowns: are they worth it? http://www.scmagazineuk.com/botnet-takedowns-are-they-worth-it/article/428021/. Accessed: 4-11-2015.

[8] Trend Micro. Simda: A botnet takedown. http://blog.trendmicro.com/trendlabs-security-intelligence/simda-a-botnet-takedown/. Accessed: 2-11-2015.

[9] Yacin Nadji, Manos Antonakakis, Roberto Perdisci, David Dagon, and Wenke Lee. Beheading hydras: performing effective botnet takedowns. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 121–132. ACM, 2013.

[10] Krebs on Security. Spyeye, zeus users target tracker sites. http://krebsonsecurity.com/2011/03/spyeye-zeus-users-target-tracker-sites/. Accessed: 7-11-2015.

[11] The Register. Zeus tracker shrinks takedowns from days to minutes. http://www.theregister.co.uk/2010/02/05/zeus_tracker/. Accessed: 8-11-2015.