Final - Assignment Block 2

Economics of Security (WM0824)
Group 1

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

September 27, 2015

1 Introduction

This paper is about the assignment of block 2 of the course Economics of Security. In block 2 the importance of measuring cyber security and the challenges to create meaningful metrics is learned and this knowledge is applied on two topics (ZeuS Tracker and Feodo Tracker) during this assignment.

This papers is structured as follows. Section 1.1 and 1.2 provide some basic information about ZeuS and Feodo. Besides that, the purposes of the ZeuS Tracker and Feodo Tracker are shortly described (see section 1.3). The general information is followed up by a description of the methodology, which includes a roadmap of how the assignment will be solved (see section 2).

Sections 3 to 7 are about answering the five questions of the assignment:

1. What security issue does the data speak to? (see section 3)
2. What would be the ideal metrics for security decision makers? (see section 4)
3. What are the metrics that exist in practice? (see section 5)
4. Define definitions of the metrics that can be designed from the data-set. (see section 6)
5. Evaluate the defined metrics using graphical representations of the metrics. (see section 7)

Finally, the conclusion of the assignment is given in section 8.

1.1 ZeuS

ZeuS is foremost a crimeware kit with botnet capabilities. The main purpose of ZeuS is to steal digital banking login credentials of users of infected hosts. ZeuS was designed by Eastern Europeans, however nowadays it is hard to attribute ZeuS crimes to a single organization. This is because the ZeuS software - the ZeuS Builder toolkit - is easy to install and can thus be used by non-professionals. The ZeuS Builder toolkit does not require the user to have in depth technical knowledge of computers, this makes it accessible to a larger audience.

ZeuS consists of several different parts. The ZeuS builder creates a binary file, which makes the botnet and a configuration file that contain the botnet settings. The configuration file contains the information such as how often an attack should take place, which servers to connect to and which banks to target. When an infected host visits certain banking websites, the ZeuS Trojan will alter the website, by hijacking the session, such that the web page asks the victim for more information than is required. After submitting, the Trojan sends the information to its servers (TrendMicro [2010]).

1.2 Feodo

Feodo is a Trojan which is similar to ZeuS. The Feodo Trojan spreads by copying itself to removable devices on infected machines. It then creates access points or backdoors so that new malware can potentially be downloaded. When users of infected hosts visit banking sites, Feodo redirects the victim to a similar fake website. After the victim enters his/her personal credentials, Feodo sends these credentials to its own servers (FireEye [2010]).

1.3 Trackers

For both, ZeuS and Feodo, trackers are available. The ZeuS tracker provides the possibility to track ZeuS Command & Control servers (C&C) and malicious hosts which are hosting ZeuS files. ZeuS hosts, the associated configuration files, binaries and dropzones are captured and tracked by ZeuS tracker. It is even possible for system administrators to block well-known ZeuS hosts and to avoid and detect ZeuS infections in their networks (zeustracker.abuse.ch [2015]).

The Feodo tracker is less extensive than ZeuS tracker, but tracks currently four versions of Feodo. This tracker also offers various types of blocklist, which allows to block Feodo botnet C&C traffic (feodotracker.abuse.ch [2015]).

2 Methodology

In order to understand what the assignment is about, information about Zeus and Feodo must be found and the purpose of ZeuS and Feodo Tracker must be clear. The ZeuS- and Feodo trackers have different kinds of data available, this data will be collected and comprehended. The data will be exported, so it can be used in R. For that reason the data needs to be clear and readable. After the data and the purpose of the data has been understood, the first question of this assignment can be answered: what security issue does the data speak to? To measure the security issue, some ideal metrics must be acquired. Unfortunately, not all ideal metrics feature available data, therefore this project is limited to the disposable data-set. Finally, the metrics should be defined, graphs of the metrics should be made in R and the results should be evaluated. The steps can be summarized as follows:

- Finding information about ZeuS and Feodo;
- Understand the purpose of ZeuS and Feodo Tracker;
- Collecting data with the Zeus and Feodo Tracker;
- Understanding what the data is about;
- Export data;
- Finding security issues;
- Finding ideal metrics;
- Finding metrics that exists in practice;
- Design a definition of the metrics from the data-set;
- Create graphics in R;
- Evaluate results.

When working on this assignment it was concluded that some extra data was needed to solve this assignment properly, for that reason some external data sources were used to evaluate the metrics defined in section 6.4, 6.5 and 6.6.

3 Security Issue

The security issue that the data-set speaks to differs per point of view. In this assignment the defender's perspective is taken into account. To be more specific the organizations that defend themselves against financial malware as the ZeuS and/or Feodo Trojan.

For organizations it is hard to defend themselves against the Trojans. Trojans evolve over time. Certain versions of the Trojans, for example ZeuS, are Open Source. Consequently, everybody can change and distribute the Trojan. Besides that, there are multiple mutations of the Trojan, which results in multiple new versions of the Trojan, while the old versions are still distributed. Evidently, this makes it hard for malware protection programs to detect the Trojans. When organizations or employees do not know that their computer or server is infected, their credentials can easily be stolen. Furthermore, the employers and employees of an organization are susceptible to social engineering. Companies have a limited budget and therefore it is not possible to, for example, train everyone to defend themselves against social engineering.

This all together results in the following security issue from an organizational point of view:

- Organizations have to protect themselves against ever adapting financial malware and methods of spreading financial malware.

4 Ideal Metrics for Security Decision Makers

There are several metrics that could be ideal metrics for security decision makers, even if the data needed for this metrics is not available.

4.1 Hosts infected with ZeuS or Feodo

This should be measured including the mutation/version of the Trojan as percentage of hosts per:

- country over time;
- nameserver over time;
- registrar over time;
- ISP over time;
- IP over time.

It is not enough to measure the number of the infected hosts per criteria. For example, measuring the number of infected hosts per country does not tell anything about the top infected countries. To rank countries according to infections, the data still needs to be normalized. The number of infected hosts needs to be divided by the total number of hosts. Therefore, if the infected hosts are taken as a percentage of the total number of hosts, it is possible to make a ranking based on country, nameserver etc. This allows for an analysis, for example, of where the spread of infection is faster or larger, when the data is plotted against a time.

This metric tells something about the percentage of infections in a certain population. When this percentage is higher it means that the certainty of having the Trojan is higher. This directly links to the issue described in the section 3.

4.2 How many more C&Cs are set up every month

This metric should be measured per:

- country;
- name server;
- registrar;
- ISP;
- IP.

This metric says something about the spread of Command and Control servers. This does not allow a conclusion that the Trojan is more effective or less effective, for such conclusions this metric needs to be coupled with, for example, user awareness or antivirus detection rates. If the number of C&Cs increases, it can be said that more efforts will be made at spreading the Trojan. More people will come into contact with the an effort at spreading, and this increases the certainty of an infection.

4.3 Percentage of active and online files over time

Not all C&Cs are still active or have related dropzones. This metric explains how many of the total C&Cs still have active binaries and dropzones. If certain mutations of the Trojan have very few active files, it may tell us something about the effectiveness of the Trojan. It would mean that C&C masters have lost interest in their mutation of the Trojan. Of course there may be several reasons why files have gone offline. However, if there is a general trend towards certain mutations of the Trojan, there usually is a common reason behind it.

4.4 Profile of the owner of the C&C hosts over time

The profile of the owner could be for example the skills of the owner and the budget. This metric is needed to analyze what type of people spread the Trojan and the difficulty of setting up a C&C. If the trend shows that, for example, the technical background of people setting up a C&C server is decreasing, it means that less knowledge is required and that it is easier to set up a C&C. If there is a general trend towards the number of C&Cs increasing, it may mean that more organizations are more often confronted with the Trojan.

4.5 The number of mutations and their code

Since the ZeuS and Feodo Trojans always keep evolving, it is useful to measure how many mutations there are. This metric could give an idea about the real percentage of Trojans detected by antivirus software. In practice this is very difficult, because there exists an open source version of ZeuS and thus anyone can replicate the Trojan with ease.

4.6 Different versions and their use over time

With this metric it is possible to create a trend of which versions are most popular during which periods of time. When the trend changes, it may indicate that companies have to protect themselves against upgraded versions of the Trojan.

4.7 Percentage of employees trained against social engineering and the effectiveness

If the percentage of trained employees is higher, it means that the organization is less susceptible to being infected. But, this is only the case if the training has its desired effect, so the effectiveness of those training should be measured too. If the spread of the Trojan is high and is increasing, it may also mean that attackers may use different methods of spreading the Trojan, it is then important that employees of organizations are well equipped to handle these attacks.

4.8 Success rate of ZeuS or Feodo phishing mails

ZeuS and Feodo are mainly spread through phishing mails. This metric describes what percentage of the phishing mails sent out are actually successful. This is needed to measure whether spreading methods are still effective. It does not necessarily matter what the reason behind the success of these phishing mails are, they will still give an idea of effectiveness of spreading techniques. Also, if the phishing mails are more effective, the probability of being infected is higher.

4.9 Percentage of devices using up-to-date antivirus

Having an up-to-date and professional antivirus program on devices gives a good first line of defense against financial malware. As a company, it is useful to know how many of your devices are protected with such software.

5 Metrics That Exist in Practice

It is hard to find the metrics that organizations use to measure the security issue described in section 3. On the other hand, it is much easier to find solutions that organizations use or should use (according to scientific papers) to protect themselves against financial malware. These solutions could be used to obtain which metrics were possibly used in practice. The metrics mentioned below can also be used on Feodo, but the information that can be found on Feodo is sparse.

5.1 Antivirus program

Firstly, it is recommended to install an up-to-date version of a highly rated antivirus or -malware program, that could detect viruses or Trojans (Arshad et al. [2013]). But, still 77% of the ZeuS infections are not detected by antivirus programs (Riccardi et al. [2013]). This could lead to the following metrics:

- *Percentage of devices within an organization that have an antivirus program.*
  There is still a percentage of Trojans that is detected by the antivirus programs, so organizations can make sure that every computer within the company is equipped with an antivirus program.
- *Percentage of up-to-date antivirus programs.*
  Since the Trojan evolves in multiple ways, organizations should measure if their antivirus programs are up-to-date.

5.2 Training

Besides that, security experts advise training to teach users to not click on unfriendly or doubtful links in spams or on the websites with regularly updated antivirus (Arshad et al. [2013]). This can lead to the following two metrics:

- *Percentage of employees that followed a social engineering training.*
  To create higher awareness on social engineering it is better when more employees followed a training on that subject.
- *Effectiveness of a social engineering training.*
  In order to know if the training was effective,

the effectiveness should be measured, for example by sending fake non-malware phishing emails to all employees and see how many of the employees still click on the links. When every employee did a training, but still 90% of the phishing mail are clicked on the training was not that useful at all.

5.3 Operating system

Security analysts of big companies as Scotia bank agree that companies have to protect their customers by increasing knowledge and standard prevention methods for example updating their OS (backinfosecurity.com [2012]). Companies like Microsoft and Apple keep patching security issues that they find, therefore outdated versions of an OS cause vulnerabilities. This can lead to the following metric:

- *Percentage of OS being up-to-date.*
  The Trojan has many different versions and configurations. This causes big OS-providers to continuously patch vulnerabilities in their software.

5.4 Blocklists

The ZeuS and Feodo Trackers also provide blocklists, so system administrators have the possibility to block well-known ZeuS or Feodo hosts and to avoid and detect ZeuS or Feodo infections in their networks. This is a good solution, but there is no direct metric for organizations which relates to this solution. Counting the number of IPs or Domains on the blocklist does not reveal much.

6 Metrics designed from the data-set

In section 4 several ideal metrics have been described, but from these metrics not all can be derived from the available data-sets. So, new metrics have been defined in this section, which were derived from the available data-sets. The data for the last three metrics (6.4, 6.5 and 6.6) was obtained through external sources.

6.1 Increase/decrease of C&Cs every month

The data-set allows us to view the number of different C&Cs online every month. It is then possible to take a difference between the number of C&Cs which have gone offline and the number of C&Cs which have newly appeared.

This metric resembles the ideal metric of obtaining the number of new C&Cs being set up (metric 4.2). The data-set does not exactly provide this. This metric can be used to analyze the spread of C&Cs and as this spread is higher, companies and organizations will have to face more attacking efforts. Each new C&C will have a new configuration of the ZeuS or Feodo Trojans.

6.2 Percentage of active and online files over time

The data-set shows how many files are online per C&C. It is then possible to plot this against different time intervals. This allows us to track whether the number of active and online files becomes larger. This also means that with every new C&C a new version of the Trojan has been released. This in turn means that organizations and companies need to defend against newer versions.

6.3 Different versions and their use over time

Metric 4.5, "the number of different mutations", is not directly deducible from the data-set. The data-set does provide which C&Cs makes use of which version of the Trojan. It is then possible to generate a trend of which versions are most popular during which periods of time. When the trend then changes, it indicates that companies may need to protect against upgraded versions of Trojans.

6.4 Percentage of devices using up-to-date antivirus software

The data for this metric is readily available from various sources. Many companies have the policy that employees should bring their own devices. For this reason, it is useful for security decision makers to know how many devices run up-to-date antivirus software. The difference with not up-to-date antivirus software is that up-to-date versions protect against newer versions of the Trojans.

6.5 Success rate of phishing emails

One of the major ways in which the Trojans are spread is via phishing mails. Sources provide data on success rates and effectiveness of phishing mails. Combining this metric with, for example, the spread of C&Cs may provide valuable information. For instance, if the number of C&Cs increases every month, but the percentage of phishing mails decreases, it may indicate that the method of spreading the Trojans has evolved or changed.

6.6 Percentage of employees trained against social engineering and the effectiveness

The Trojans may also be spread through other means of social engineering. In case of social engineering however, the version of the Trojan is not relevant. An increase in the percentage of security aware employees means a higher level of protection against different versions and mutations of Trojans. To make sure that the training is effective, this should be measured too.

7 Evaluation of the metrics

For the evaluation of the data, the metrics of section 6 are used. Since the data-set of Feodo is much smaller than the data-set of ZeuS, not all metrics could be done for the Feodo data-set.

7.1 Increase/Decrease of C&Cs every month

Figure 1 shows that mid 2011 the number of newly detected ZeuS C&Cs is still relatively small. There are two small spikes at the end of 2013. This did not immediately indicate a general increase, since the months after that the numbers dropped again. From 2014 and onward a general increase can be seen, with a top in September 2015.

Over time more and more ZeuS C&Cs are being set up, this means that the number of newer versions of the ZeuS Trojans are rapidly increasing.

This is slightly different regarding Feodo (see figure 2). For starters, only data of 2015 is available. However, the popularity of Feodo peaked in May and June, and afterwards it slowly decreased again. Towards the end of 2015 ZeuS seems produce more newer versions of their Trojan, as opposed to Feodo.

7.2 Percentage of active and online files over time

From the ZeuS Tracker the number of online C&C's and the number of active files can be obtained. Unfortunately, only data from the past 60 days can be gathered. From figure 3 it can be seen that the number of dropzones, config files and active domains follow the same trend. In mid-august, there was a slight peak in the amount of active files. During the rest of the past two months, these remain approximately the same. From this, it can be concluded that even though more C&C's are found, approximately the same amount disappear or go offline.

The Feodo data-set does not contain information about the online and active files, therefore it was not possible to evaluate this metric for that dataset.

7.3 Different versions and their use over time

In figure 4 it can be seen that in 2011 and 2012 generally speaking only one version of ZeuS was being used, namely 'regular' ZeuS. There was one small time period where suddenly three versions where being used, Citadel and Ice IX, however this did not continue. Only in mid 2013 did the popularity of Citadel suddenly rose. It can be seen Citadel from 3013 onward has been consistently used. The popularity of the KINS version suddenly spiked since the beginning of 2015. From the middle of 2015 also the VMZeuS version got into play from then onward 4 different versions had continually been deployed.

Figure 5 shows that only two versions of the Feodo Trojan have been tracked over 2015. Over this period version D has been consistently thriving. Version C was popular during May 2015, but has not been detected since July 2015. This pattern corresponds to figure 2, which shows that there is a decrease in the number of new Feodo C&Cs.

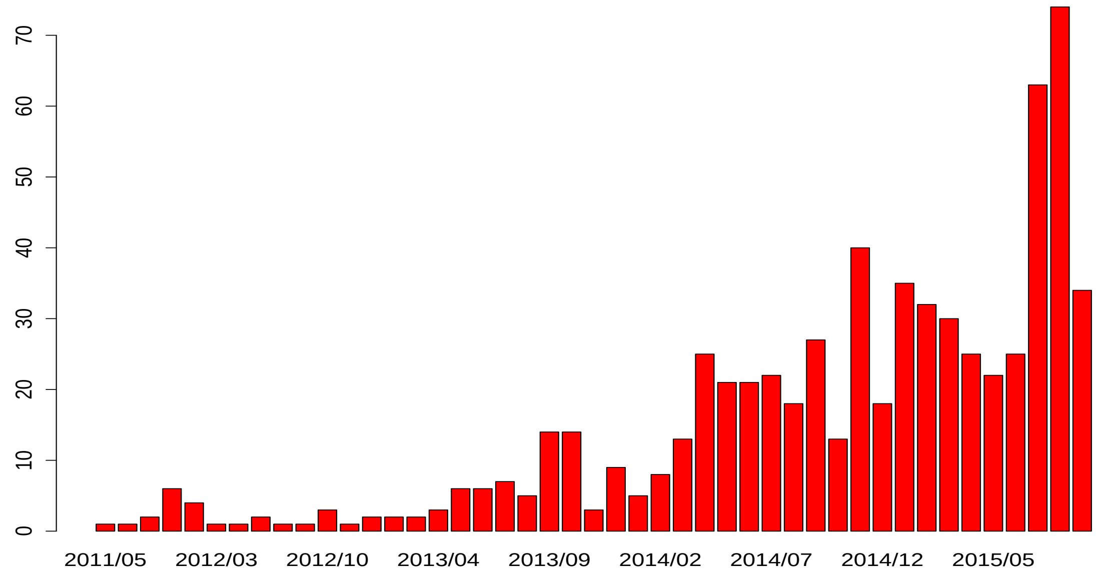

Figure 1: Number of C&C's detected by ZeuS Tracker per month

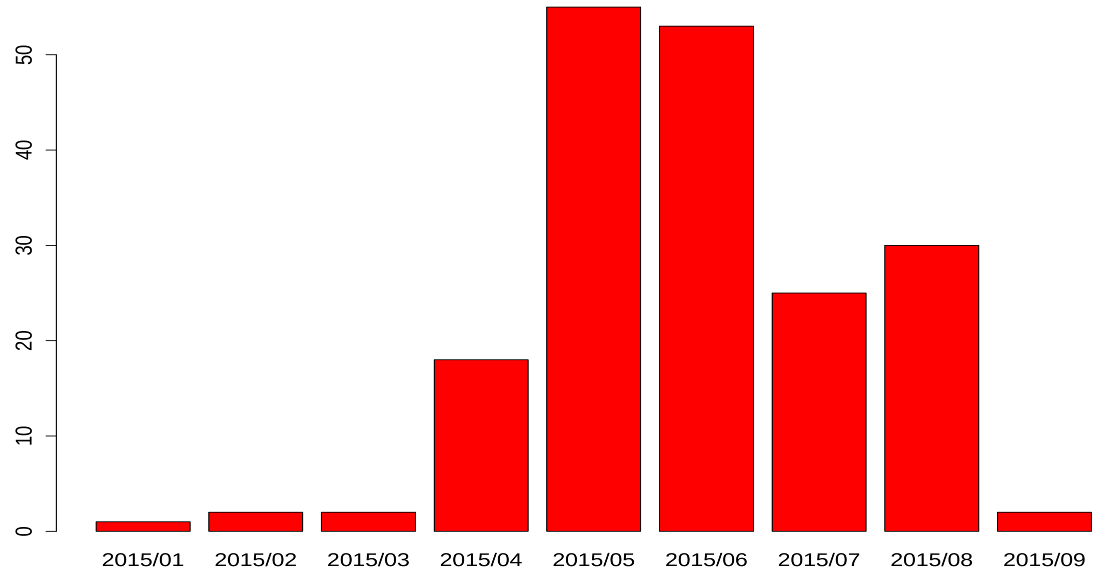

Figure 2: Number of C&C's detected by Feodo Tracker per month

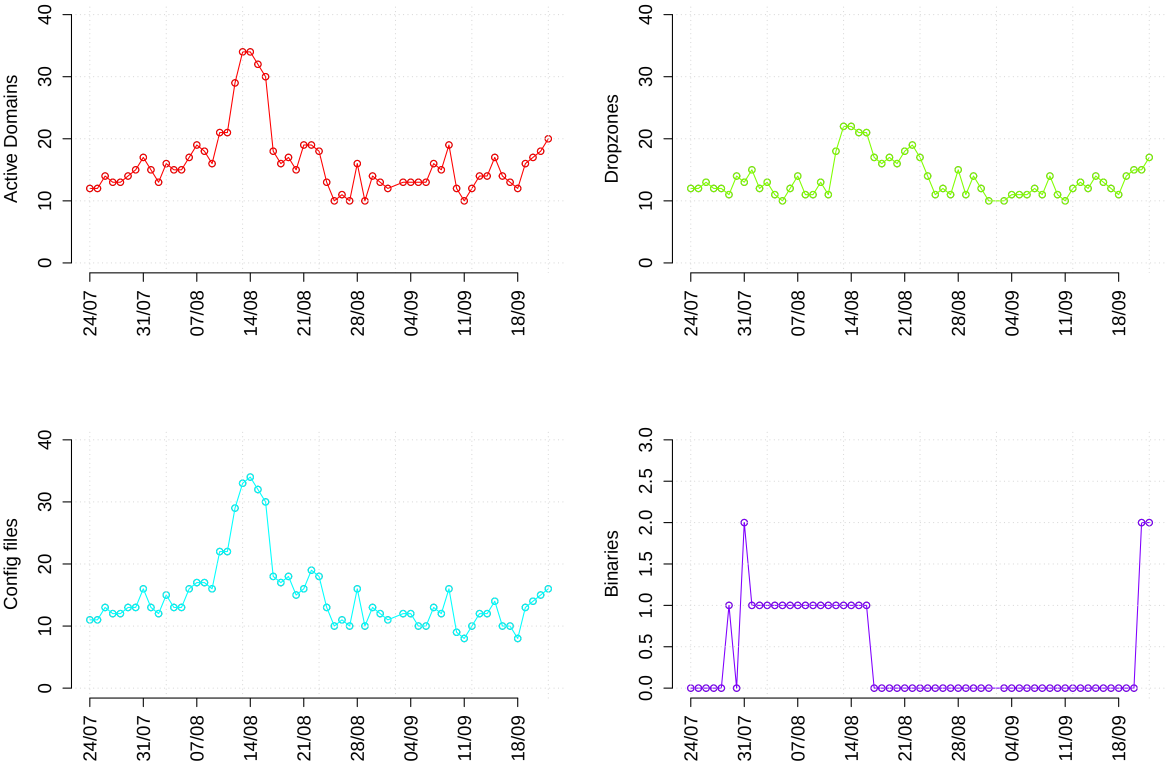

Figure 3: Number of online ZeuS C&C's and their active files in the last 60 days

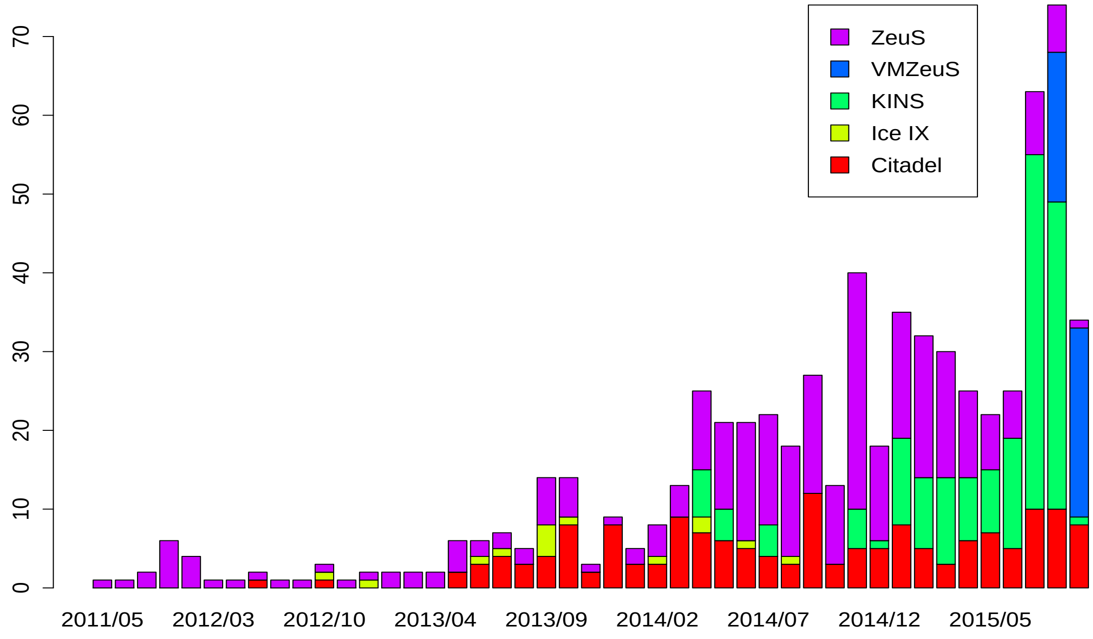

Figure 4: Versions of ZeuS tracked by ZeuS Tracker over time

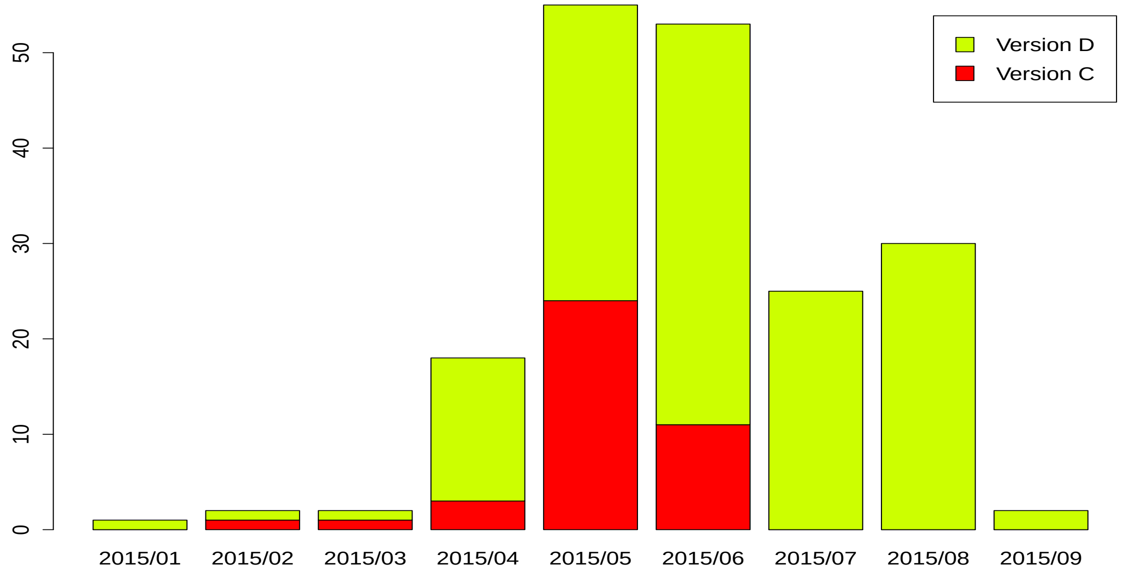

Figure 5: Versions of Feodo tracked by Feodo Tracker over time

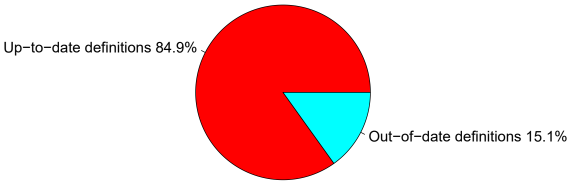

Figure 6: Devices using up-to-date antivirus software

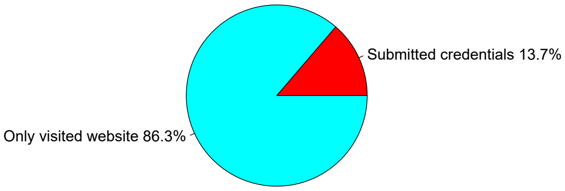

Figure 7: Success rate of phishing emails

7.4 Percentage of devices using up-to-date antivirus software

According to OPSWAT [2015], 84,9% of the devices with an antivirus program have up-to-date definitions. But 15,1% have out-of-date definitions, which are at least three days old (see figure 6).

This means that nearly 85% of the people using antivirus software will be able to defend against versions of the Trojans, which have been added to the antivirus. However, this means that, given that 77% of the time antiviruses do not detect the ZeuS virus, antiviruses will have an even harder time since the number of new ZeuS C&Cs increases.

7.5 Success rate of phishing emails

When researchers analyzed a data-set of 5.000 phishing emails provided by Google, they found that 13,7% of the people that visited phishing websites also filled in their details (see figure 7). They did this by dividing the amount of HTTP-POST requests by the amount of HTTP-GET requests. However, this is only an average. Broken down by individual pages they observed a huge variance in success rate, with the most successive page having a success rate of 45% opposed to a lowest rate of 3% (Bursztein et al. [2014]).

Given the fact that the number of ZeuS C&Cs is increasing, a larger number of ZeuS phishing mails can be expected. The number of people still visiting phishing websites is still large; security decision makers can expect a larger number of mails and may opt to provide training for people who they deem necessary.

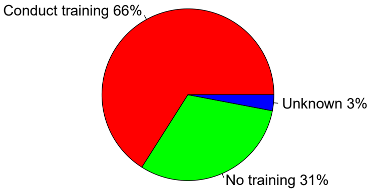

Figure 8: Percentage of organizations that conducted a user awareness training

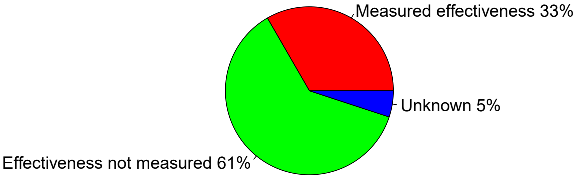

Figure 9: Percentage of organizations that measured the effectiveness of the training

7.6 Percentage of employees trained against social engineering

RAPID7 [2013] did a research on user awareness training based responses from IT professionals representing more than 550 organizations. One of the results was that 66% of the organizations conducted a user awareness training, and of those organizations only 33% actually measured the effectiveness.

It is not exactly known what percentage of people actually have undergone training. However, this metric shows that only 33% of the companies tested the effectiveness of the training. From the majority of the people it is not known whether the training has been effective.

8 Conclusion

In this paper the results of the analyzed data provided by the ZeuS and Feodo trackers was described. A security issue have been derived which was analyzed using the provided data-set. The security issue has been formulated as follows: organizations have to protect themselves against ever adapting financial malware and methods of spreading financial malware.

We then looked at all the metrics which would ideally help us analyze the security issue. Section 4 lists all these metrics and how they relate to the corresponding issue. The focus has been mainly on the growth rate, antivirus usage and social engineering. Section 5 and 6 have revealed that not all these metrics are applied in practice, or are obtainable from the data-set. The metrics then to be slightly altered, or dropped altogether. For example ideal metric 4.2, "how many more C&Cs are set up every month", had to be changed to "increase/Decrease of C&Cs every month" (metric 6.1).

Section 7 reveals visual data regarding every metric and discusses how they can be interpreted. We have seen that the number of new Feodo C&Cs has decreased in the past several months, whereas the number of new ZeuS C&Cs have increased. Surprisingly, the number of active and online files, or its trend, has remained the same though. Companies can use this data to further analyze financial malware. For example, the fact that less online files are detected, might mean that malware is better at hiding. The metrics regardfing antiviruses and social engineering give companies an idea of their own defense against financial malware and helps them identify their weak points.

In conclusion, this paper analyzed metrics which help evaluate the security issue defined in section 3 and also evaluated the data corresponding to these metrics. The visualized data can be used by companies and other parties to make informed decisions about how financial malware is evolving and how it is spreading.

References

Sobia Arshad, Shahid Mehmood, Nida Yasir, and Maria Arshad. Botnets: Zeus botnet detection and its removal. *International Journal of Computer Applications*, 84(17), 2013.

backinfosecurity.com. Zeus: How to fight back, 2012. URL `http://www.bankinfosecurity.com/interviews/zeus-i-1592/op-1`. Accessed: 2015-09-29.

Elie Bursztein, Borbala Benko, Daniel Margolis, Tadek Pietraszek, Andy Archer, Allan Aquino, Andreas Pitsillidis, and Stefan Savage. Handcrafted fraud and extortion: Manual account hijacking in the wild. In *Proceedings of the 2014 Conference on Internet Measurement Conference*, pages 347–358. ACM, 2014.

feodotracker.abuse.ch. Feodo tracker, 2015. URL `https://feodotracker.abuse.ch`. Accessed: 2015-09-15.

FireEye. Feodo - a new botnet on the rise, 2010. URL `https://www.fireeye.com/blog/threat-research/2010/10/feodosoff-a-new-botnet-on-the-rise.html`. Accessed: 2015-09-15.

OPSWAT. Antivirus and compromised device report: January 2015, 2015. URL `http://www.opswat.com/resources/reports/antivirus-and-compromised-device-january-2015\#antivirus-usage`. Accessed: 2015-09-29.

RAPID7. The threat within: securing user risk, 2013. URL `http://www.rapid7.com/docs/riskrater-user-risk-survey.pdf`. Accessed: 2015-09-29.

Marco Riccardi, Roberto Di Pietro, Marta Palanques, and Jorge Aguil Vila. Titans revenge: Detecting zeus via its own flaws. *Computer Networks*, 57(2):422 – 435, 2013. ISSN 1389-1286. doi: http://dx.doi.org/10.1016/j.comnet.2012.06.023. URL `http://www.sciencedirect.com/science/article/pii/S1389128612003556`. Botnet Activity: Analysis, Detection and Shutdown.

TrendMicro. Zeus: A persistent criminal enterprise, 2010. URL `http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_zeus-persistent-criminal-enterprise.pdf`. Accessed: 2015-09-15.

zeustracker.abuse.ch. Zeus tracker, 2015. URL `https://zeustracker.abuse.ch`. Accessed: 2015-09-15.