Draft - Assignment block 2

Economics of Security

20/9/2015

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

Introduction

In order to make clear where this project is about, some basic information about ZeuS and Feodo is given in this section. Besides that, the purposes of the ZeuS Tracker and Feodo Tracker are shortly described.

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 which contains 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 virus 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 virus sends the information to its servers.

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.

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 config 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.

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 you to block Feodo botnet C&C traffic.

Methodology

This section contains the methodology and the steps that will be followed to solve the assignment.

In order to understand what this project is about, information about Zeus and Feodo must be found and the purpose of ZeuS and Feodo Tracker must be clear. ZeuS and Feodo tracker have both different kinds of data available, this data should be collected and understood. The data should be exported, so it can be used in R, for that reason the data should be clear and readable. When the data is understood, the first question of this assignment can be answered, namely: what security issue does the data speak to. To measure the security issue, some ideal metrics must be found. Unfortunately, there is not data for all kind of metrics, so only the metrics can be used where data is available for. Finally, the metrics should be defined, graphics 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 in practice;
- Design a definition of the metrics from the dataset
- Create graphics in R;
- Evaluate results;

Preliminary results

This section contains the preliminary results of this assignment.

Security issues

Below are several issues which relate to the data and the ZeuS and Feodo virus.

1. **<u>The virus improves over time</u>**
   When the virus improves over time it will be harder to detect the virus and remove it. More on this below.

2. **<u>It is hard to detect the virus with antivirus programs</u>**
   This may be a security issue, because people and organizations do not know they are infected and when the antivirus program also does not know that the computer is infected, credentials can easily be stolen.

3. **<u>There are multiple mutations of the virus</u>**
   Everybody can change and distribute the virus since it is Open Source. So there will be new versions of the virus, which makes it harder to detect the virus. Besides that, the older versions will still be distributed.

4. <u>People/Organizations may not know that their computer or server is infected</u>
   When people/organizations do not know that their computer or server is infected, they do not know anything about it and their credentials and so on can be stolen easily.

5. <u>It is not known how many C&C servers the trackers are unable to track</u>
   The trackers give an approximation towards how many C&C servers there are. There is no way to know the exact number of C&C servers. So, the problem may be much larger than is thought.

6. <u>There is no awareness about social engineering</u>
   When people or organizations are not aware about social engineering they may for example click on the phishing mails and then their computer or server will be infected. So, the virus will be distributed faster.

The data speaks to several security issues, these are discussed above. From these issues it is possible to combine the first three issues (the issues in bold). The other issues can be deducted from the description of the viruses, however cannot be directly seen from the dataset made available. The first three issues combine to produce the following more general security issue. The issue, the data set also speaks to, is that the virus mutates over time (as a result of reprogramming) and thereby it goes under the radar of antiviruses. The dataset makes it possible to measure a possible “improvement” of the virus. In this context the word improvement is lightly spoken of: improvement usually means that it becomes “stronger”. However, in case of the ZeuS and Feodo virus, strength or improvement cannot be measures with simply a single metric. What does it actually mean for the ZeuS and Feodo viruses to improve? There are too many factors involved in performing a ZeuS or Feodo ‘attack’, that not a single answer can be given. A successful ZeuS or Feodo comprises the following steps.

1. Setting up a Command and Control server.
2. Spreading the virus to victims and successfully installing them on the victim’s computer without being detected.
3. Picking up the credentials of victims through dropzones.

Notice how, ‘Making the victim enter their credential on a false site’, is not included in the list. Viewing things from the perspective of the virus, this is a step which is not in the control of the C&C host (or the virus).

Technically speaking, the virus itself is only the binary file on the victim’s computer. An improvement then refers solely to this file. However, if we suppose that this file is incredibly sophisticated, it still does not mean that there will be many cases of the virus, because it may be very difficult to spread the virus, or set up a Command and Control server. Therefore, in determining the strength or improvement, we must take into account all the three steps described apart.

An improvement of the ZeuS or Feodo virus means that any of the above steps is easier to perform and/or that the resistance thereof, by victims or security specialists, is more difficult.

Some may argue that measuring step 1 is not necessary and has nothing to do with the virus. However, we must take into account that when the number of C&Cs increase, there may be a possibility that the number of infections also increase. Simply because the malicious servers are not found, does not mean that the C&C is not active, it may very well be that the C&Cs are very active, but that it is better at staying under the radar. Keeping track of the C&Cs is therefore important, and plays a part in the overall attack.

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. The metrics which are made bold are metrics which can be used to analyse the security issue regarding the improvement of the virus. The others are interesting metrics to measure, but refer back to security issues which were mentioned in the previous section and which not made bold.

Hosts infected with ZeuS or Feodo and which mutation of the virus

- as percentage of hosts per country over time
- as percentage of hosts per nameserver over time
- as percentage of hosts per registrar over time
- as percentage of hosts per isp over time
- as percentage of hosts per 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 is 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 is needed to say something about the security issue that there are multiple mutations of the virus. Tracking the mutations over time over several criteria might reveal how the virus has changed and how improvements are taking place. This may reveal information such as, to what degree is the virus still effective and whether the security measures are improving.

Percentage of infected hosts that are free web hosts

This metric can be used to see if free web hosts are a vulnerability. Namely, when web hosts are free there are no/less costs for criminals to host the virus. If they have to pay for hosting the threshold to spread the virus may be higher.

Percentage of C&Cs that are hacked

Not all servers which contain dropzones route ZeuS and Feodo information with the permission of the host.

Expanding rates per month (how many more C&Cs are set up every month?)

This metric says something about the spread of the virus, whether there are more infected hosts. However this does not allow a conclusion that the virus is more effective or less effective, for such conclusions this metric needs to be coupled with, for example, user awareness or antivirus detection rates.

Note: this metric relates to the measuring the improvement of the virus. However, whether the virus spreads fast or slow does not necessarily means it is improving or not. Take for example the Stuxnet virus. Let us suppose the the spread suddenly took an exponential growth after two weeks of its release, this does not mean the virus has improved, because it still remains unactivated on all personal devices/computers. The virus in itself has never changed. Conclusions about data form regarding this metric is therefore not easy to draw.

Percentage of active files over time

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

Percentage of online files over time

Not all C&Cs are online at all times. This metric gives an overview of how the C&Cs change from online to offline. I am not sure we can use this metric, because this pattern would not tell us much.

Success rate of ZeuS or Feodo phishing mails

ZeuS and Feodo are mainly spread through phishing mails. This metric tells 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 matter, necessarily, for what reason these phishing mails are more or less successful, they give an idea of effectiveness of spreading techniques.

Banks that are targeted

ZeuS and Feodo target specific banks. Knowledge about which banks are targeted may provide information about in which countries the infection is larger or what type of banks are targeted more.

Banks that are targeted, but are uninfected

There are several reasons why banks may remain unaffected. For example, the customers of these banks are aware of phishing. It may also be that these banks have better security measures. Coupling this metric with others may reveal some of that information .

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 analyse what type of people spread the virus. This metric is needed to analyse 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. According to our definition, it then means that the virus is improving.

Uptime

How long is every C&C online and is there a trend in this? This informs us on the average lifetime of a C&C. However, if the trackers think that a C&C has gone offline, does not necessarily mean it has been disabled. It is thus not so easy draw conclusions from the metric.

Metrics that do (not) exist in practice

Of the abovementioned metrics, not all metrics also exist in practice. The following metrics cannot easily be measured, and therefore no or limited data is available.

1. *Hosts infected with the virus.* The trackers are capable of measuring C&Cs, even though it is not exactly clear how, but it is not easy to measure which victim's computers are infected with the virus and therefore contain a malicious binary file. The virus will obviously try to stay hidden, and therefore the victim may never find out his/her computer is infected. The only way to find out information about the number of infection is the count the number of reported cases. Data on this is very limited however, without any sources.
2. *Success rate of ZeuS or Feodo phishing mails.* It is not known how many phishing mails are sent out every day or in total. From that it is also not known how many of these mails are successful. A reason for this latter is that when phishing mail are successful, by the nature of phishing mails, the victims themselves are unaware. This makes it a very difficult metric to measure.
3. *Profile of the owner of the C&C hosts over time.* It is not known exactly who sets up C&Cs and what type of people they are. Therefore it not easy to create a profile. However, looking into the mechanics of how to set up a C&C may reveal something about the difficulty level, and therefore what type of people may be associated with them, or at least what their technical background is.

The remaining metrics can be measured. Data is readily available and this data now needs to be processed so that it fits the metrics and so that the data can be visualized.

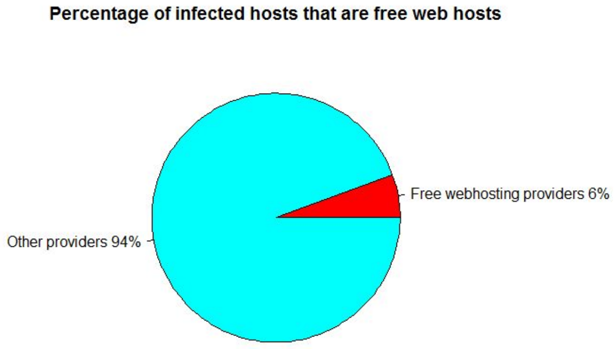
Percentage of infected hosts that are free web hosts

This metric will be used to see if free web hosts are a vulnerability. Namely, when web hosts are free there are no/less costs for criminals to host the virus. If they have to pay for hosting the threshold to spread the virus may be higher. Unfortunately, this metric can only be used for ZeuS, since there is no data available for Feodo.

Evaluation

According to the data 6% of infected hosts are free web hosts. So, for those hosts there are no costs for the criminals.

This metric does not give a clear view on some points: free web hosting could also involve shared hosting, so you might have several malicious URLs hosted in the same IP address. Besides that, a higher number of infected host under a certain provider does not necessarily imply that they are worse, as they can mitigate the infected hosts faster despite having a higher amount than in dedicated hosting.



Percentage of infected hosts that are hacked
Existing web hosts possibly have all kinds of vulnerabilities. This issue can be exploited by hackers to distribute the ZeuS or Feodo viruses. This metric is important to give us insight on whether regular hacking exploits are playing a big part in the expansion of the virus. This metric can only be used for ZeuS, since there is no data available for Feodo.
Evaluation

Percentage of infected hosts that are free- or hacked web hosts over time
Since the bare amount of hacked or free infected web hosts is not sufficient to show what is a recent development when distributing this malware. Therefore, it is rational to plot these metrics opposed to time (over the past 4 years). This also can only be done for ZeuS.
Evaluation

Expanding rates per month
This metric says something about the spread of the virus, whether there are more infected hosts. However this does not allow a conclusion that the virus is more effective or less effective, for such conclusions this metric needs to be coupled with, for example, user awareness or antivirus detection rates.
Evaluation

Percentage of active files
Not all C&Cs are still active or have related dropzones. This metric explains how many of the total C&Cs are still have active binaries and dropzones.
Evaluation

Percentage of online files over time

Not all C&Cs are online at all times. This metric gives an overview of how the C&Cs change from online to offline.
Evaluation

Uptime
How long is every C&C online and is there a trend in this? This informs us on the average lifetime of a C&C.
Evaluation

Sources:

ZeuS Tracker: https://zeustracker.abuse.ch
Feodo Tracker: https://feodotracker.abuse.ch