EoS - Security Metrics

Noël Keijzer (s1602349)
Tom Leemreize (s1745506)
Joost Prins (s1723545)

September 2019

1 Introduction

With the rapid growth in digitalisation of the world, the importance of digital security has grown significantly. With the rise in importance of digital security, a need for measuring the digital security of an individual or entity has grown as well. Measuring digital security starts with having data about your security. Thus it is very important to keep logs of your digital activity. In this assignment we are tasked to analyze such data and draw conclusions from them. Our group analyzes the malware droppers data set that is provided by the course.

In this document, the analysis will be divided into different sections to make sure it is correct and easy to follow. First, in section 2 malware droppers and the data contained in the data set will be explained. Second, section 3 gives an overview of the ideal metrics regarding malware droppers such that all the different variables can be precisely defined. Third, section 4 discusses the actual metrics that can be retrieved from the given data set and which variables can be estimated from these metrics. Fourth, section 5 gives the actual metrics that are retrieved from analysing the data set. Finally, section 6 gives the analysis of the retrieved metrics and draws conclusions from them.

2 Malware droppers

Malware droppers are a piece of software that is used to infect devices with the threat which the author wants to spread. This can be ransomware, a remote administration tool (RAT) or any other piece of malware. The data that is provided contains date-time stamps along with URLs. A snippet of the data is given in Listing 1.

Listing 1: Snippet of malware dropper data

```
,2013-08-24 07:42:04,http://www.intro2seo.com/-.php
```

```
,2013-09-10 16:00:26,http://www.kostazoo.pl/onas.html
,2013-10-08 22:00:39,http://firstcomp2004.hu/index-4.html
,2013-10-11 03:00:13,http://www.senegalair.sn/charter.html
,2013-10-19 13:30:09,http://www.mm.pl/%7Efotobk/rocz/target16.html
,2013-10-23 18:30:06,http://www.brmkozmetik.com.tr/cvv.html
```

The data appears to be an access log containing when infected computers download the payload of the dropper. We have not yet figured out the security issues that this data speaks to, because we simply do not know how to interpret the data yet.

3 Ideal Metrics

The ideal metrics are metrics that can be used to quantify the costs, the level of security as well as the benefits of a security measure that has to be taken to deal with the issue mentioned in the previous chapter. There are three variables that one must measure to make a security decision. The security cost being the first. This involves the cost of setting up and maintaining a security solution for the issue.

The second variable that needs to be measured is the security level. This is the degree in which all direct and indirect costs have mitigated the risks faced by the organization.

The third variable that one wants to measure is the benefits of the security. This can be quantified as the reduction of losses that would have been incurred.

Using these three variables as metrics one can make a decision as to which security solution is the most optimal economical solution.

4 Practical Metrics

The metrics mentioned in the previous chapter are metrics that may not be applicable to the data provided. There are however a lot of practical metrics that can be used to quantify the metrics mentioned in the previous chapter. In this chapter we will be going in to each metric and how one can use practical measurements to quantify it.

4.1 Security cost

4.2 Security level

4.3 Benefits of security

5 Metrics that follow from the dataset

As far as how we currently understand the dataset there are very few metrics we can design from it. The dataset consists purely of date, time and a link to a website. A metric that might be possible is the amount of droppers. This can be used to quantify the benefits of security as it shows us the amount of threats.

6 Results

Unfortunately we do not have any results yet.