WM0824TU Economics of Cybersecurity

Malware Droppers Assignment 1

Kanav Anand 4712870
Dinesh Bisesser 1512250
Philip Blankendal 1547682
Richard Vink 4233867

September 24, 2018

Contents

1. Introduction **2**

2. What security issue does the data speak to? **2**

3. What would be the ideal metrics for security decision makers? **2**

4. What are the metrics that exist in practice? **4**

5. A definition of the metrics you can design from the dataset **5**

6. An evaluation of the the metrics you have defined. This should include graphical representations of the metrics (e.g., histograms, scatter plots, time series, bar charts) **5**

6.1 Url Count 5

6.2 Time Difference 7

6.3 Domain Count 7

1. Introduction

Internet and the cyberspace is something we cannot live without these days. It is as important as other utilities like water and electricity. With more and more companies being digitalized, adversaries are increasing and becoming more active. Thus cyber security is becoming more important in order to protect not only data but also services, communication and users.[6] Implementing cyber security is hard, for there are allot of factors that need to be accounted for. One of these factors is economy. The economics of cyber security deal with economic concepts, measurement approaches and data analytics in order to make better security decisions.

For this assignment we will look into a dataset of malware droppers: **A Trojan that installs some malware on a target machine**.[1]

We will analyze the dataset and come up with security metrics that can be used to measure malware droppers data. In order to do this we first look into what security issues the data speaks to. After that we discuss the ideal metrics for security decision makers. Next we find out which metrics exist in practice. Finally we define the metrics we can design from the dataset and evaluate them in the last section.

2. What security issue does the data speak to?

The security issue here relates to unsafe links. Once clicked, the user will download a small piece of malware. The data consists of a set of database files. The files contain malicious links for a specific month. A malicious link can be used for different goals. One of which is installing a trojan horse [2]. Another goal is phishing [3]. The complete dataset relates to a time interval between: April 2014 until September 2016. There are two types of actors when malware droppers are used. These actors are: victims and attackers. The victims are the ones who got malware installed on their device by a malware dropper. The attackers are the ones who created the malicious software.

3. What would be the ideal metrics for security decision makers?

As seen in the lecture[2] there are four types of security metrics:

- **Controls:** measures you take to mitigate risks.
- **Vulnerabilities:** (un)known weaknesses in the controls.
- **Incidents:** events where security is compromised.
- **(Prevented) Losses:** mapping (prevented) incidents to (prevented) losses.

[1] https://en.wikipedia.org/wiki/Dropper_(malware)

[2] http://delftxdownloads.tudelft.nl/EconSec101x-EconomicsCybersecurity/Week%202/EconSec101x-2b-slides.pdf

Most security assessments only use controls for metrics. This is easier to measure and risk of failure is at the buyer side instead of at the security company. However this is not enough and ideal. Figure 1 shows that in order to make proper security decisions, all four type of metrics needs to be used. That way the threat environment is included in the measurement and metrics are then both action and event driven, so that an overall security level can be established for the company.

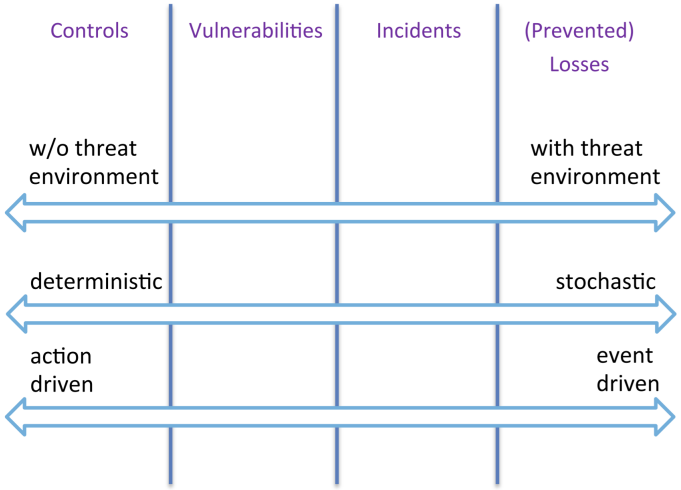

Figure 1: Types of metrics

The following different levels of security decision makers exists:

1. **Organizational**

   As an organization you want to use all four type of security metrics to ensure the highest level of security within the organization. However depending on costs this might be hard to accomplish.[1] Looking at the malware droppers dataset it can be interesting for an organization to see what urls are mostly visited in order to block connections to them. Another interesting metric is to check in which periods or time malware is most active.

2. **Local**

   Local or regional wise it is interesting to see whether multiple users in the region are affected by these malware droppers.

3. **National**

   Nationwide it is important to see if multiple users and companies are affected by the malware droppers. ISPs can check if and when certain websites are visited that corresponds with the dataset. This way it will be clear if the national might be under a cyber attack or not.

4. **International**

   International is hard to measure cyber security. Different countries have different rules. However in case of the malware droppers, it might be possible that multiple countries have similar problems. In order to check that, countries need to exchange strange behavior like what the ISPs can check nationwide. This way the source might be traced and stopped.

4. What are the metrics that exist in practice?

Malware droppers are known to be active for over two years [5] due to the difficulty in determining their maliciousness. They are known to downloads other programs or files, combining malicious files with trusted software to hide their true identity. Thus usual metrics used for detecting malware do not give promising results for droppers. It comes as no surprise that the current state of the art metrics used for detecting these malware droppers is majorly dependent on data generated from download history. The Figure 2 shows how two files with the same name and downloaded from the same domain can be differentiated as malicious using the download data. [4]
Below we present few of the metrics currently being used to detect malware droppers.

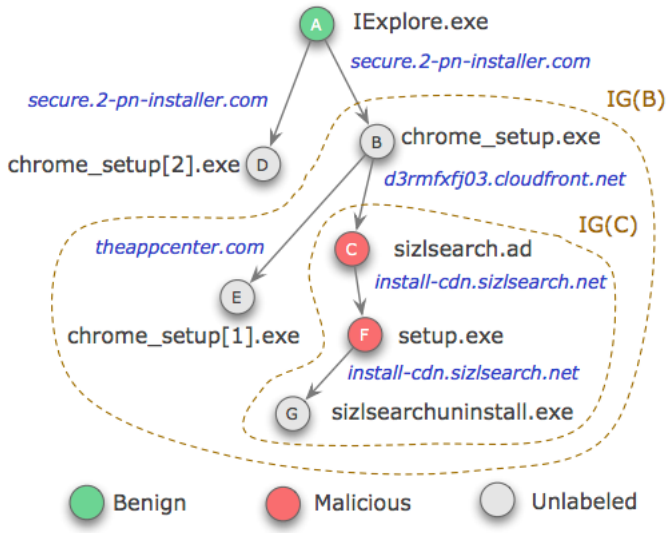

Figure 2: Same file showing different download history data

Metric	Definition
DownloadFrequency	Number of downloads by a downloader or possible dropper
DownloaderCount	Number of times the downloader has been downloaded
TimeDifference	Time difference to capture how quickly a downloader tends to download other executables
TrustScore	Downloader trustability i.e file signature, publisher information, and reputation of certificate authorities
UrlRank	URL it is downloading from i.e Alexa rank
DomainCount	Number of downloads from the specific link

Table 1: Metrics to detect malware droppers

5. A definition of the metrics you can design from the dataset

As we can see in Table 1, several metrics are named. This dataset contains a set of malicious links. We can design DomainCounts out of these links, namely the number of downloads from a specific link. We are also able to design TimeDifference as a metric, because this dataset contains a set of time stamps before noting the malicous download. Furthermore, we could have designed the DownloaderCount; the number of times the downloader has been downloaded. Unfortunately the source url of the malware droppers is not provided. However we can use a similar metric with the given requested urls. This way we can see the number of times a specific url has been requested.

6. An evaluation of the the metrics you have defined. This should include graphical representations of the metrics (e.g., histograms, scatter plots, time series, bar charts)

In the following subsections we evaluate each metric defined in section 5 seperatly. We also use some form of graphical representation of the data concerning these metrics in some of our analysis. In order to evaluate the metrics we used a dataset of malware droppers urls that were clicked during August 2013 to September 2016.[3] Information about the dataset can be found on our Github repository.[4]

6.1 Url Count

The data-set shows the requested url by the malware or the downloader. To obtain the number of times a certain url was requested we simply check the amount of times that url occurs in our dataset. We plotted the top ten urls along with the time of its first occurence

[3] https://surfdrive.surf.nl/files/index.php/s/MZbaZl2fFOSD2QV
[4] https://github.com/richie-v/Malware-Droppers

in the data set along with its last occurence. Figure 5 shows the top 10 requested urls by the malware droppers, whereas Figure 4 shows the first and last time these urls were requested. This information could help in detecting and blocking malware droppers and their url requests, by blocking the most requested urls.

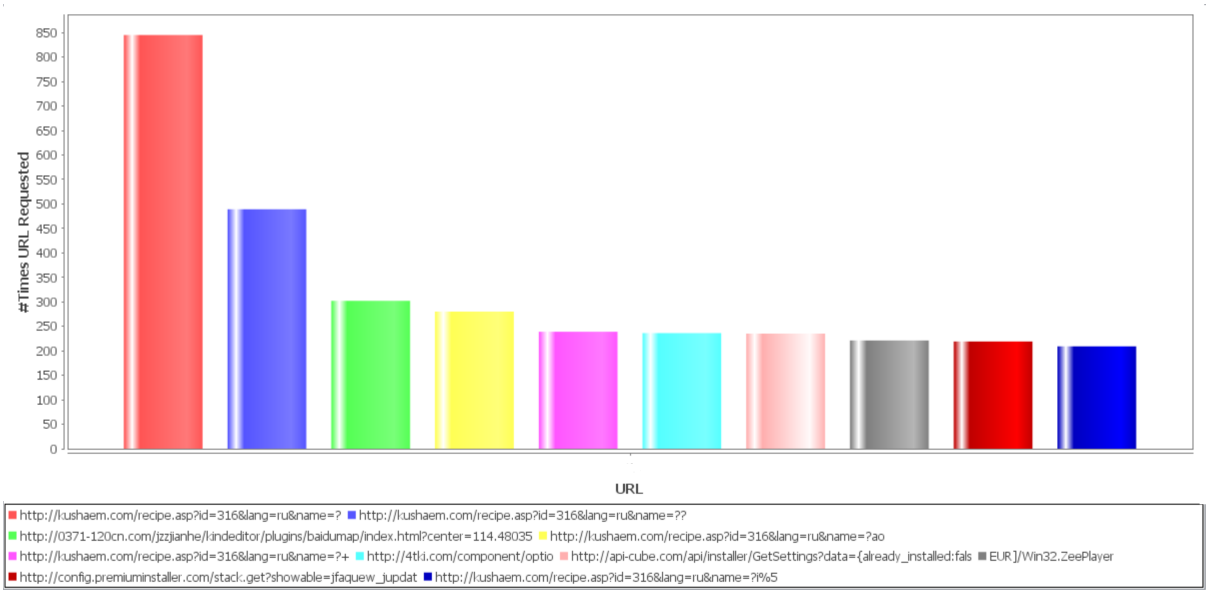

Figure 3: Top 10 requested urls

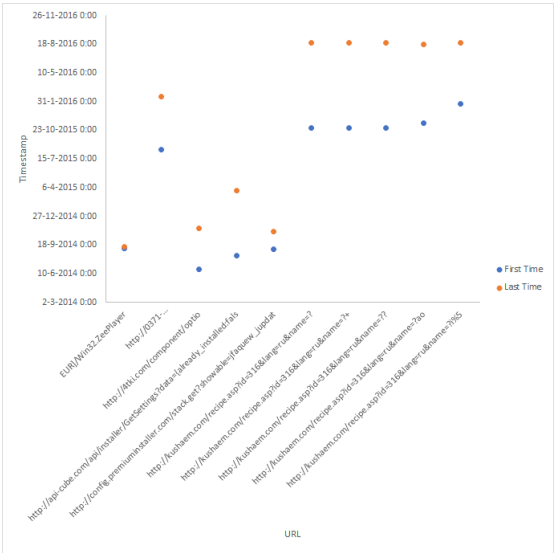

Figure 4: First & Last time of top 10 url request

6.2 Time Difference

In order to plot the time difference we simply check the time between two occurences of the same url, here we then plot the average time, the fastest time, the slowest time as wel as the median in order to gain some insight on the reaction time of the downloader (malware dropper).

As we can see in the files; most files are downloaded between days. For example http://000.lzong.cn/cssfzxfabu/ is being downloaded on september 13 2016 and on september 14 2016. Both downloads were done at 18:30.

6.3 Domain Count

The Domaincount can easely be computed by only taking the first part of the url (e.g. hosntame) into consideration and ignoring the URI parth of the path. We can achieve this by splitting each string on '//' and '/'. We plotted the top ten occuring hostnames/domains from april 2014 in the (bar chart) below.

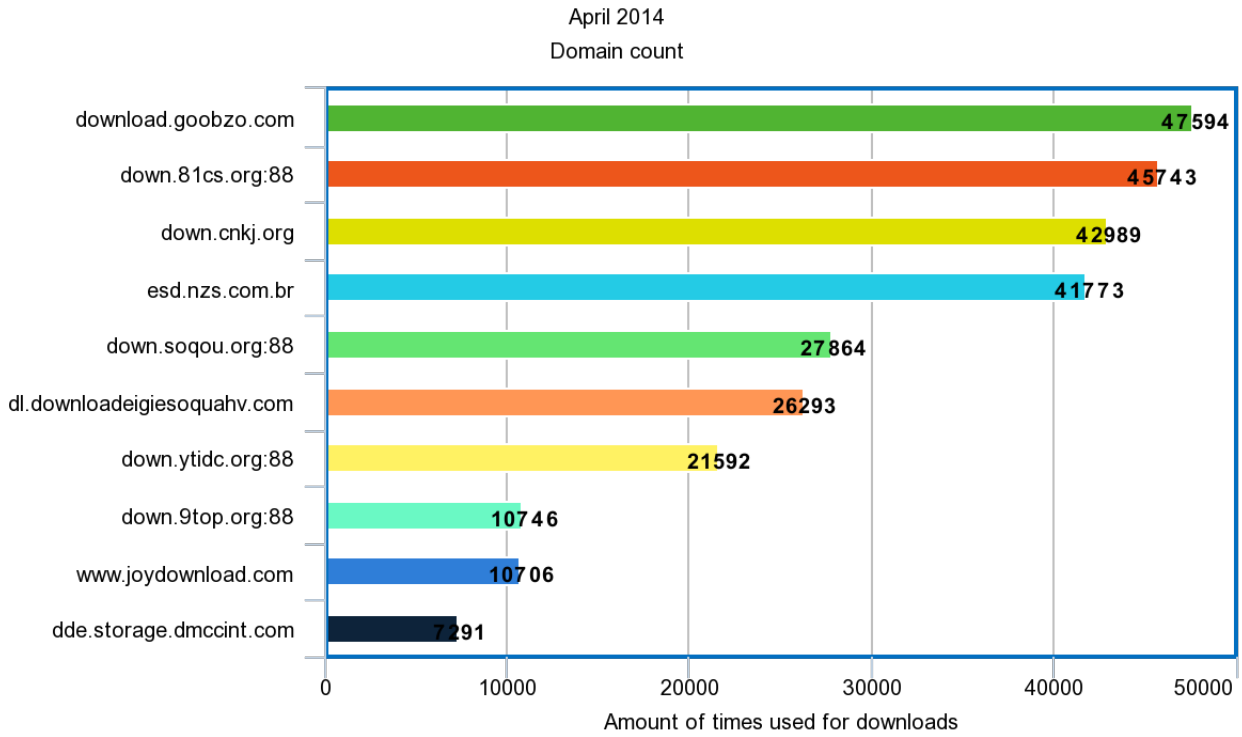

Figure 5: Top 10 domains used in April 2014

In the above plot (figure 5) we observe that the domain "download.goobzo.com" was used 47594 times in total, followed closely by "down.81cs.org:88". This makes them the 2 most frequently used malware servers in April 2014.

References

[1] R. Böhme. Security metrics and security investment models. In *International Workshop on Security*, pages 10–24. Springer, 2010.

[2] F.-G. Deng, X.-H. Li, H.-Y. Zhou, and Z.-j. Zhang. Improving the security of multiparty quantum secret sharing against trojan horse attack. *Physical Review A*, 72(4):044302, 2005.

[3] R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pages 581–590. ACM, 2006.

[4] B. J. Kwon, J. Mondal, J. Jang, L. Bilge, and T. Dumitras. The dropper effect: Insights into malware distribution with downloader graph analytics. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 1118–1129. ACM, 2015.

[5] C. Rossow, C. Dietrich, and H. Bos. Large-scale analysis of malware downloaders. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 42–61. Springer, 2012.

[6] R. Von Solms and J. Van Niekerk. From information security to cyber security. *computers & security*, 38:97–102, 2013.