WM0824TU Economics of Cybersecurity
Malware Droppers Assignment 2

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

October 8, 2018

Contents

1. Introduction

Internet and cyberspace are things that have spread themselves into a lot of the main and most relevant areas in today's economy. 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.[5] 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] The dataset[2] contains timestamps and urls, so the time and place of where the malware droppers were downloaded from are known.

We have analyzed the dataset and came up with security metrics that can be used to measure malware droppers data. In order to do that we looked at what security issues the data speaks to. After that we discussed the ideal metrics for security decision makers and found out which metrics exist in practice. Finally we defined the metrics we can design from the dataset and evaluated them. We thus came up with the following three metrics: Downloader Count, Time Difference and Domain Count.

Now that we have knowledge about the security issues and the metrics that can help measure them and their impact, we will look into identifying the actors involved with these security issues and their strategies to deal with it. In the first section we describe the problem owner of the security issue. Next we look into what relevant differences in security performance our metric reveal. After that we sum up risk strategies that the problem owner can follow to reduce the security issue. We also come up with other actors that can influence the security issue. Then we identify the risk strategies that the actors can adopt to tackle the problem. Finally we calculate the Return on Security Investment (ROSI) for one of the risk strategies from the previous section, using the malware droppers dataset.

2. Who is the problem owner of the security issue as measured in your first assignment?

The security issue related to our data is the access to the malicious links, that when clicked may install malwares or steal personal data using phishing. Thus, the key requirement for this security issue is access to the internet. These problem owners begin with small or large private and government organizations or a single user able to access these links. The stakeholders of the company, partners and other connections of these primary owners gets involved as secondary owners based on the nature of the malwares.

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

[2] https://surfdrive.surf.nl/files/index.php/s/MZbaZl2fF0SD2QV

In this report, we will consider private organizations and its employees to be our main actor and the problem owners.

3. What relevant differences in security performance does your metric reveal?

Domain count metric, as explained in the previous assignment, reveals the number of different times that particular domain was visited. Clearly, a high value of this metric reflects the success rate of that particular malicious link.

The domain count can be easily used to evaluate the security performance of an organization. Consider a scenario, where a company has highly invested in an antivirus software to avoid these malicious domains. This metric can be used to validate the quality of this software. If a domain is deemed not malicious by the antivirus software but a high domain count metric might suggest otherwise.

For example, Figure 1 shows the top 10 domains for malware droppers in the month April of 2014. Here we can clearly see that *download.goobzo.com*, for instance, is the most frequently occurring url for malware droppers. This domain count can be used, to see if any risk strategy has a positive or negative effect on the security performance of the organization. If after applying the risk strategy, the domain count for a domain drops, we can assume that the risk strategy is working and thus security performance is enhanced. Of course it could also mean that the domain is not working properly. That's why we look at the top domains, so we see an overall drop of these domain counts if the risk strategy is working. In case it's not working, the domain count for the top domains should be similar or slightly higher.

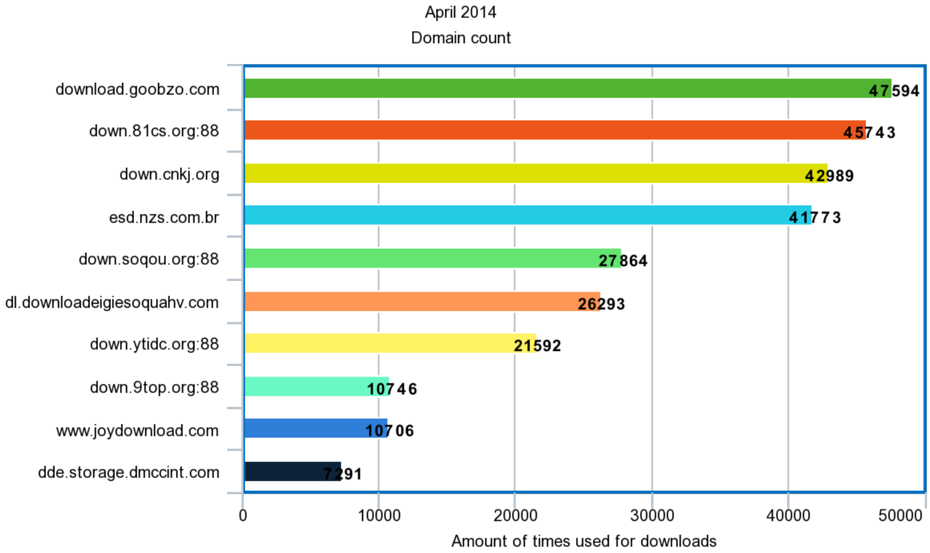

Figure 1: Top 10 domains used in April 2014

Thus, the above metric can be used as the extra validation tool to evaluate the security performance of an organization. Although, this largely depends on the quality of the domain list provided in the dataset. As it is assumed to be our ground truth dataset.

4. What risk strategies can the problem owner follow to reduce the security issue as measured in your first assignment?

A **Invest in a quality antivirus**
A good quality antivirus that can help the users detect and ban the malicious links based on their large database and algorithms used to detect malicious links. This antivirus has to be installed on all the computers of the organization's network. New unknown malware and malicious links can however not be dealt with by the antivirus, until they are known and added to the antivirus database.

B **Run Daily and Update Daily**
It is a good practice to check your system daily for any malicious content. By daily updating your antivirus tool, it keeps the user safe from new and latest malicious links created recently. Doing this regularly can help keep the set of unknown malware as small as possible for the antivirus. This is of course a bit of an hassle to do on all the computers of an organization. It's therefore good to keep this in the daily routine of the employees, so they get used to it.

C **Monitor & Block Internet Traffic**
Blocking known malicious websites helps against malware infiltrating the network and computers. Monitoring internet traffic inside the organization can help find suspicious behaviour of potential malware infected equipment. This monitoring and blocking can be done by using firewalls and/or have specialized personnel do it manually.

D **Don't click on email links or attachments**
This is the most common and important strategy as it is the easiest way to get in contact with a user. It is always strongly advised avoid clicking links that seems fishy. Knowing which email are fishy, is however hard. Proper tools and/or training are needed to ensure that employees don't click on links or attachments. False positives and negatives will occur, so it's important to have the right tool and/or training to keep those as low as possible.

E **Surf smart**
In the end, it is majorly a user decision that decides to visit these malicious links. Thus, an organization can offer day trainings for their employees teaching them basics of surfing smartly and make them aware of the risks available online. A paper by Kumaraguru et al. [2] showed that training users in the real world for phishing trained them to identify phishing scams, no matter if the user has a

technical background or not. Phishguru (tool used for training against phishing) helps train users to avoid giving information to phishing websites,does not retain users on clicking valid mails and users retain knowledge from Phishguru even after 28 days.[1]

5. What other actors can influence the security issue as measured in your first assignment?

The actors associated to the security issue can be divided into two general categories, that is, victim or problem owners and the attackers. As discussed above, the problem owners can be any user or organization that is impacted by the use of these malicious links. The different types of actors that represents attacker category can be described as follows: [3]

A **Professional criminals**
As the term professional indicates, there is usually a monetary benefit behind these attacks. The attacks can be carried out in order to gain some private information that could be used for extortion or there is already a buyer who is willing to pay for that personal information. Other motives might include damaging the resources of the organizations in exchange of money. One famous example of this is WannaCry, where attacker would encrypt the victim's hard drive in exchange of Crypto Currency.[3]

B **Terrorists**
The main motivation of this group of actors is to create a social upset or imbalance, instead of monetary gain. As everything is moving online and is being controlled online, the role of this actor will get only more significant. It could also involve stealing secret information from various government organizations to gain useful insights.

C **Cyber vandals and script kiddies**
It refers to the amateurs who carries out basic attacks/small sized attacks with the use of widely available scripts and tools. It is mostly done to demonstrate their abilities or as a challenge or prank.

D **Competitors**
The problem owning organization might have competition from other organizations. They will try to keep ahead of the problem owner. This can be done in several ways, like trying to create bad publicity for the problem owner, attack their assets, come up with better product/service, etc.

The different types of actors that represents victims or defenders are:

A **ISPs**
ISPs can influence the security issue as well, by blocking known domains and urls

[3] https://english.nctv.nl/binaries/CSAN%202016_def_tcm32-145252.pdf

with malware. This way websites with malware can be blocked nationwide. This comes of course with other issues, like censorship. For instance restricting freedom of the ISP users who do want to visit these websites.

B **NGOs**

These are organizations that are not the government, but actively try to improve society according to their objectives. Mostly non-profit, so if these organizations are compromised, it would mean that the adversaries are doing it out of political reasons. This could have all sort of political and international consequences.

C **Governments**

Governments have the power to come up with laws that can help protect the problem owner. They can force ISPs to block certain domains, which are known to have malware. Not only can they help defend, they could also become a victim. Many adversaries will always try to attack governments, in order to get classified information about countries, cities, etc.

6. Identify the risk strategies that the actors can adopt to tackle the problem.

The risk strategies stated in section 4 are primarily for protecting the problem owner's (or NGO) organization and its assets. ISPs could use the monitor and block strategy to block certain websites nation wide, whereas governments could help make laws in order to help ISPs to do so legally. All these 5 strategies would reduce risks over time.

The attacking actors, on the other hand, have of course completely different risk strategies. Their problem is that they want to infiltrate organizations with their malware. Even though we established four different type of attackers in the previous section, their risk strategies are mostly the same. Their strategy would be to have their malware installed in the organization's network, by using social engineering, phishing mails, fake websites and fake files and media. Then they wait till someone from the organization takes the bait.

The professional criminals and terrorists might even go so far as physically appearing and infiltrating in the organization to plant their malware. This can be done by someone from the inside, social engineering or just breaking and entering. The reason being them having a higher cause then the cyber vandals and script kiddies, who do it just for sports. Their malware could therefore cause more harm, compared to malware by the cyber vandals and script kiddies. Thus these professional criminals and terrorists have more to lose (in case of failure) and gain (in case of success).

Competitors can try attacking the problem owner them self or hire any of the other type of attacking actors to do the job for them.

Any of their strategies would increase the risks over time for the problem owner.

7. Pick one of the risk strategies identified previously and calculate the Return on Security Investment (ROSI) for that particular strategy.

Looking at the risk strategies from section 4, we pick the **Surf smart** strategy. We choose this one, because we think it's best to train personnel to avoid these websites. This way there will be more awareness among employees and not just among a small group of people like security decision makers and tech guys. Also it's better to prevent and avoid, these malwares, then to cure.

The benefits of this risk strategy can also be measured with our metric, domain count, by looking how often these domains are accessed by any of the users in the organization. If it less after training, then that means that the training is effective.

To see how well this risk strategy would work, we calculate the **Risk on Security Investment (ROSI)**[4]:

$$ROSI = \frac{(Risk\ Exposure \cdot \%Risk\ Mitigated) - Solution\ Cost}{Solution\ Cost}$$

In order to estimate the costs and benefits involved with the surf smart strategy, we use the given dataset for the malware droppers. Figure 2 shows that the top most malware urls are intact for a year, so that means that these malwares can harm the organization for a whole year. This also means that employees can be trained to avoid these malwares in that same year. Looking at Figure 1, you can see that the top domain with malware was downloaded almost 50.000 times in one month. By creating awareness among employees, this can be avoided.

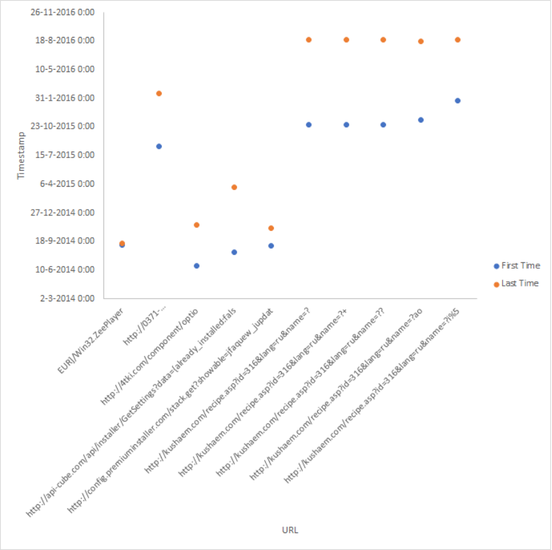

Figure 2: First & Last time of top 10 download urls

There are three values needed to calculate ROSI:

1. **Risk Exposure:** The annual cost in damage and lost productivity due to exposure of the malware. Figure 3 shows the average annual cost companies spend on malware attacks is almost 2.4 million dollars.[4]

2. **Risk Mitigated:** The percentage of attacks catched. In this case the amount of malware that can be avoided by training staff. Looking at Phishguru, the tool used to train people to avoid phishing, the website[5] states that it reduces over 80% in susceptibility to attacks. Having Phishguru been proven to work in the previous section.

3. **Solution Cost:** The costs of implementing the risk strategy. Security education has an average cost of $290,033 per year.[6].

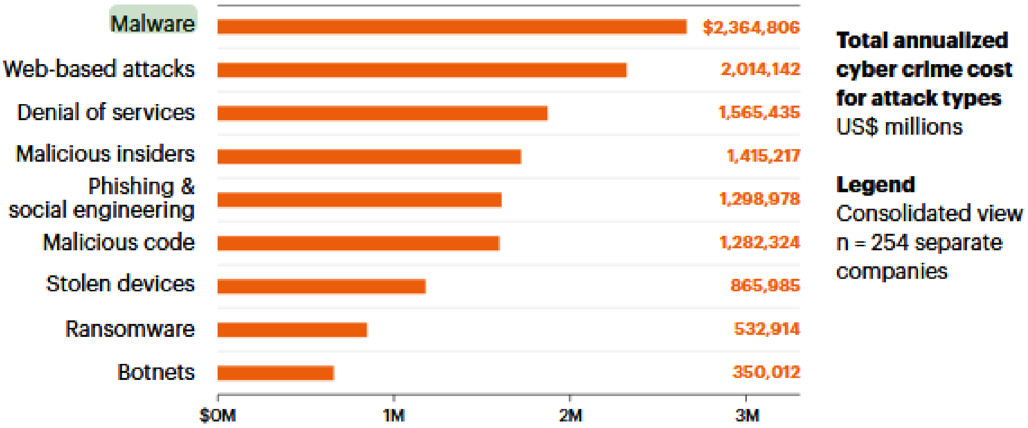

Figure 3: Annual cyber crime costs per attack type

In order to calculate the ROSI, we'll be using a probability distribution. This because we don't have solid values for each of the variables, thus a probability distribution helps giving an overview of the estimation.

In order to do so, first the **Annualized Expected losses (ALE)** has to be calculated

[4] https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

[5] http://www.resoftco.com/phishguru

[6] https://www.infosecurity-magazine.com/news/cost-of-user-security-training/

for both the original and secured scenarios:

$$\begin{aligned} Unitary\ Impact &= \$1\ -\ \$2364806/incident \\ Frequency(annual) &= 1\ -\ 2461933\ incidents/year \\ ALEo &= Unitary\ Impact * Frequency(annual) \\ Probability(annual) &= 0.01\ -\ 0.20\ incidents/year \\ ALEs &= Unitary\ Impact * Probability(annual) \end{aligned}$$

After that **EBISs** can be calculated:

$$\begin{aligned} EBISs &= ALEo - ALEs \\ &= \$XXXXXX/year \end{aligned}$$

Figure 4 shows its distribution.

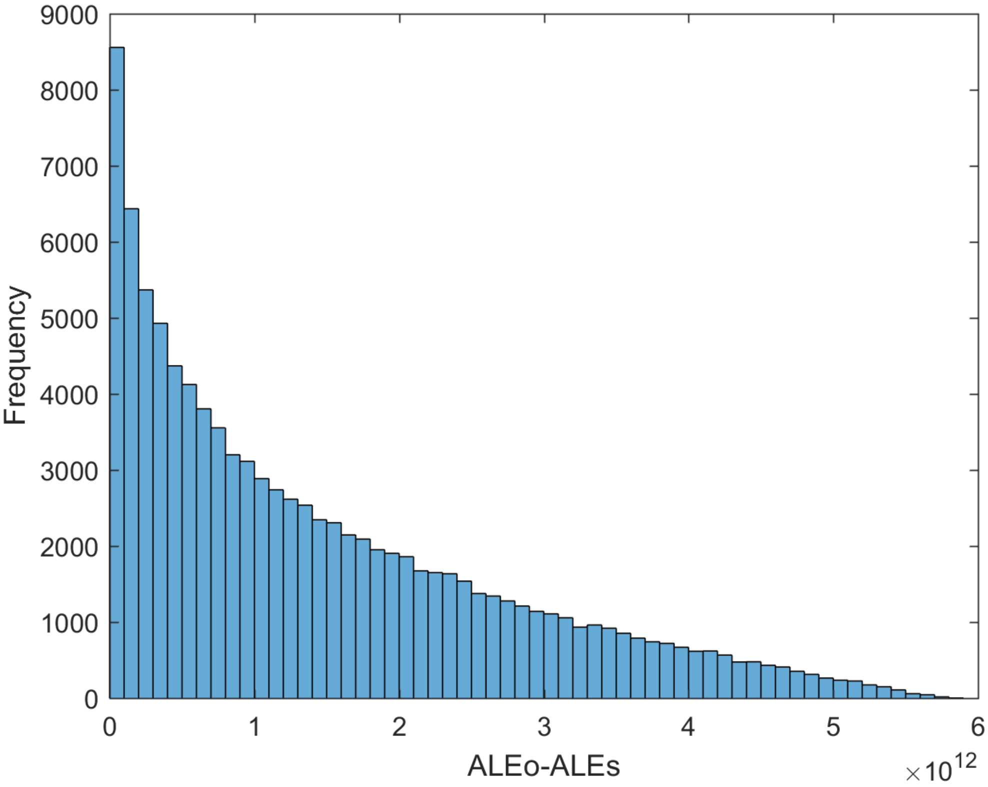

Figure 4: EBISs

Now that we have the EBISs distribution and the cost of investment, the ROSI distribution can be calculated:

$$\begin{aligned} ROSI &= \frac{EBISs - Solution\ Cost}{Solution\ Cost} \\ &= \frac{EBISs - 290033}{290033} \end{aligned}$$

The final ROSI distribution can then be found in Figure 5.

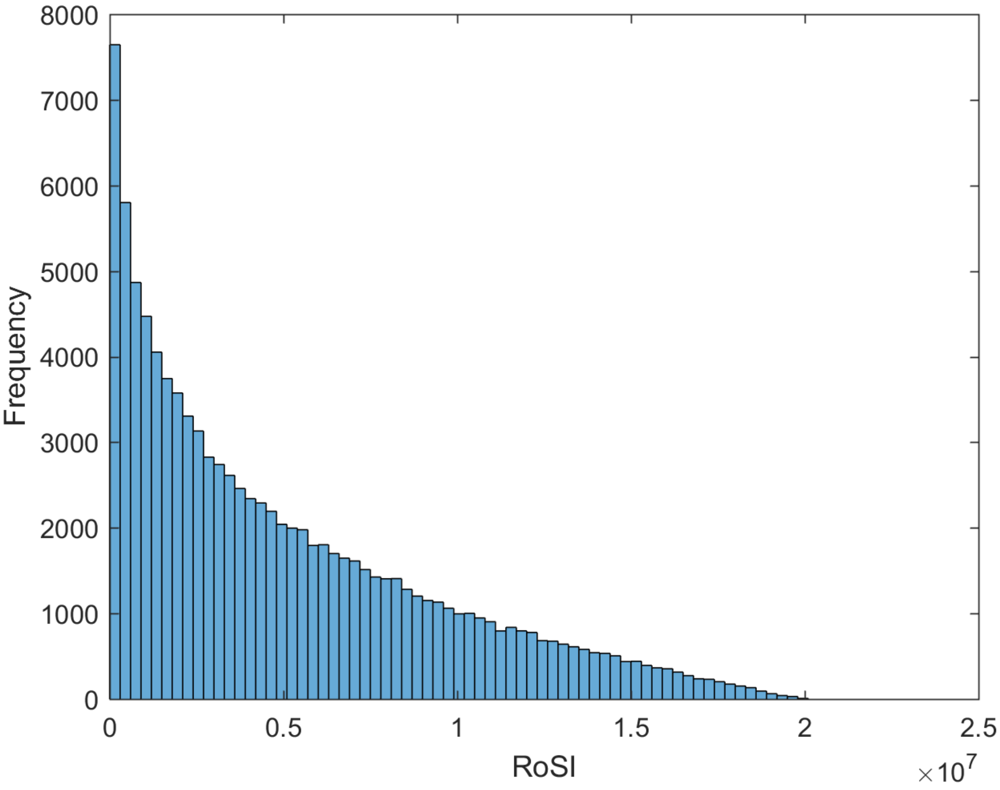

Figure 5: ROSI

Here we see that the ROSI is likely to be 0, with an average of $0.5x10^7$.

8. Conclusion

So after defining security metrics for the malware droppers, we haven chosen the domain count metric as the main metric. This because it can be easily used to evaluate the security performance of an organization.

Now we have also looked at the actors and risk strategies. Four different types of attacker actors were defined, with their own motives and thus their own risk strategies.

Having private organizations and its employees as our problem owner, we came up with four risk strategies for them. Surf smart seemed the most promising, for it avoids and prevents instead of cures. Calculating ROSI for this risk strategy, we see that the average makes it worth to invest.

The results of training employees can then be validated, by looking at domain count for the malware droppers. If the training is going well, the domain count should then be lower.

References

[1] P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M. A. Blair, and T. Pham. School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, page 3. ACM, 2009.

[2] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong. Lessons from a real world evaluation of anti-phishing training. In *eCrime Researchers Summit, 2008*, pages 1–12. IEEE, 2008.

[3] S. Mohurle and M. Patil. A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, 8(5), 2017.

[4] W. Sonnenreich, J. Albanese, B. Stout, et al. Return on security investment (rosi)-a practical quantitative model. *Journal of Research and practice in Information Technology*, 38(1):45, 2006.

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