EoS - Security Metrics

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

September 23, 2019

Important notice

The first two deliverables have been merged into one deliverable, allowing us to reference to our old metrics and citations. The second deliverable, about risk strategies, can be found on page 9.

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 its security issue is defined. Second, section 3 gives an overview of the ideal metrics regarding malware droppers that were discovered during a literature review. Third, section 4 discusses the actual metrics that are retrieved from the given data set and which variables can be estimated from these metrics. Finally, section 5 concludes the research.

2 Malware droppers

According to Naval et al. malware has become a major threat to the cyberspace [15]. Contemporary anti-malware solutions are often able to detect malware before they can cause damage to systems, however by utilising malware droppers, these infections can still take place, regardless of anti-malware solutions [20]. Malware droppers are a piece of software that is used to infect devices with

the threat which the author wants to spread [23]. Malware droppers can deliver ransomware, a remote administration tool (RAT) or any other piece of malware. Malware can cause damage to the reputation of companies as well as resulting in financial losses [1, 11, 7]. This directly implies that malware droppers are a threat as well, as they can deliver a malware payload onto a target machine without detection.

The security issue that malware droppers speak to is that of malware infection itself. As mentioned above, malware infection is a problem that can have major consequences for companies and individuals. In order to mitigate this problem a company can implement both technical as well as organizational measures. An example of a technical measure could be the deployment of anti-malware solutions, or a blacklist for unknown domains. Organizational measures include training employees to recognise suspicious e-mails, which could potentially include links to malicious programs, such as malware droppers.

3 Ideal Metrics

In this section the ideal metrics are described. The ideal metrics for malware droppers are distilled from a literature study that was done on the topic of security metrics in combination with malware droppers. An overview of the ideal metrics found in the literature study is given along with further explanation of these metrics. A summary of the literature study is given in Table 1.

Miani *et al.* looked at different metrics that could be retrieved from IDPS's and found that metrics 1, 2, and 3 from Table 1 were the most telling for the security of an entity [14].

In [2] the results of 46 papers are combined to produce the best metrics to identify the security of an entity. These resulting metrics are metric 4, 5, and 6 in Table 1.

Ahmed *et al.* listed several cybersecurity metrics for use in healthcare IT systems, however these metrics could be applied to other IT systems as well [3]. Metrics 7 and 11 could be used to spot data exfiltration, which is especially important with laws such as the GDPR. GDPR violations could result in both financial loss due to fines, and damage of the company's reputation. Depending on the organization, metric 8 could also provide a lot of insight into malware droppers. Organizations which do not have servers outside their geographical area should not connect to IP addresses in those areas. If this is the case, it could indicate a security hazard.

In [16], Skopik *et al.* described several metrics, including the financial loss caused by the incident and the time until the incident was discovered, which provide insight into the severity of an incident.

Takamura *et al.* did a study into the definition of security of NASA mission operation centers (MOCS). In a NASA MOC, security is of utmost importance

because it is the critical element in NASA's space missions [17]. Takamura *et al.* Describe Metric 16, 17, 18 of Table 1 as the most important metrics to have in such an environment.

Metrics 19 and 20 are related to the domain names and registrars used for the malware droppers. Hao *et al.* found that 46% of spam domains come from two registrars, so this information could prove vital in blocking domains used for malware droppers, and thus preventing infection [10].

Metric Nr.	Metrics	Study
1	Number of (distinct) attackers per week	[14]
2	Number of (distinct) objectives per week	
3	Number of (distinct) signatures per week	
4	Current number of untrusted network connections	[2]
5	Total number and number of unsuccessful connection attempts to authenticate devices communicating via untrusted networks per week	
6	Number of access retries associated with a source address recorded by each access point	
7	Volume of outbound traffic	[3]
8	Volume and number of IP addresses connecting to your network from outside of your geographical area	
9	Number of simultaneous logins by the same user from different locations that has not been detected by the network security tools	
10	Number of unknown accounts with elevated privileges found on compromised systems	
11	Number of hosts communicating with external networks on non-standard ports	
12	Damage of attack (in euros)	[16]
13	Incident date	
14	Time until discovery	
15	Time until recovery	
16	Number of new vulnerabilities in the past thirty days	[17]
17	Number of open vulnerabilities in the past thirty days	
18	Number of closed vulnerabilities in the past thirty days	
19	Number of malicious domains per registrar	[12]
20	Number of malicious domains per TLD	

Table 1: Literature overview of ideal metrics

4 Practical Metrics

This section describes the metrics that can be gathered from the provided data set. First, the data set will be explained. Then, the different metrics from section 3 that are applicable to this data set are measured. Finally, visualizations

will be given of these metrics.

The data that is provided is an access log containing when infected computers download the payload of the dropper. The access log is in the format of 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
,2013-11-05 13:30:09,http://www.007museum.com/movie.htm
,2013-11-24 00:00:15,http://solariumibg.com/novi.html
,2013-11-24 00:30:04,http://paw.compnet.com.pl/h1l.html
,2013-11-24 01:00:09,http://www.doucetpol.net/taille.html
```

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 over each metric applicable to the data, and how one can use practical measurements to quantify it. Additionally, we will provide metrics of our own.

Many of the metrics described in section 3 are not applicable to the data as not enough information is available. Metrics 1 through 3, for example, cannot be applied to the data as we cannot tell what was targeted or by whom the attacks were executed. Other metrics, such as metric 8, cannot be executed as no data is available of the targets themselves, so nothing can be said about the geographical location of the target. Because of the lack of available data, most of the metrics can unfortunately not be applied.

Even though no data was available on the attackers, metric 1 can still be applied when looking at the different URLs. This also holds for metric 16, where a new vulnerability can be seen as a new URL in the logs. By making these small modifications, some metrics found in literature can still be applied on our limited dataset. Additionally, metrics 13 and 20 were also applied on the dataset. For metric 20 some extra processing of the dataset had to be done, as the TLD for each domain had to be separated and compared to the list of total domains for that TLD. Aside from the metrics of the literature, we also looked at the country to which the IP address of URL belongs, as this might indicate that some countries host more servers serving malware. This information can in turn be used in blacklists or other technical countermeasures.

After processing the data set and extracting IP addresses, Top Level Domains (TLDs) and countries of origin it was possible to analyze a few of the metrics described above. In Figure 1, one can see the distribution of the TLDs used by droppers between 2014 and 2016. This distribution was made by summing up the amount of unique domains in the dataset and grouping them by TLD. It was then normalized by dividing each TLD by its sum of total assigned domains[8].

This results in a dataset that shows the percentage of malicious users on a certain domain.

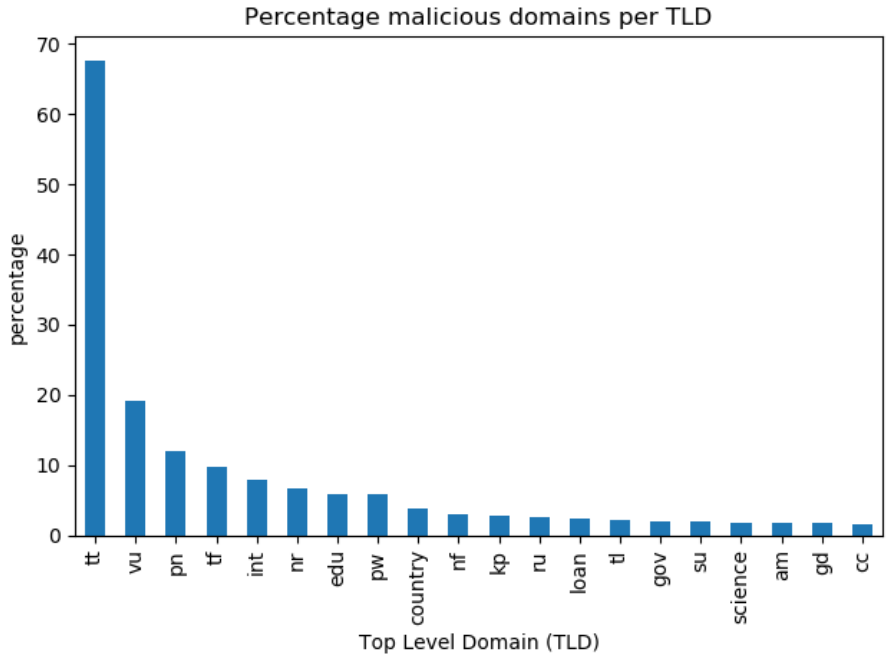

Figure 1: Percentage of malicious domains per TLD

As one can see from Figure 1 there are some TLDs for which the percentage of malicious domains is very large. For example for the .tt domain, malicious domains from the dataset used in this assignment make up almost 70% of the domain space. From this we can conclude that there are several TLDs that pose a particularly high risk to users, which should be avoided. This information can be used when informing employees of companies about malware. When giving a training one could mention that links from these particular TLDs often contain malware and thus that the employees should take extra care when clicking links from these domains. When taking more precautions a company could opt to block these TLDs altogether.

In the histogram in Figure 2 one can see the percentage of unique IP addresses used by malware droppers per country relative to IP address space of that country[9]. From the histogram one can see that compared to other countries Hong Kong has a reasonably high percentage of dropper domains. However this is still only 0.08%. Thus, it is not really feasible to mark Hong Kong domains as potentially dangerous. We learn from this that there is not one single country

that is preferred by malicious actors to host their malware, instead it is more of a global epidemic.

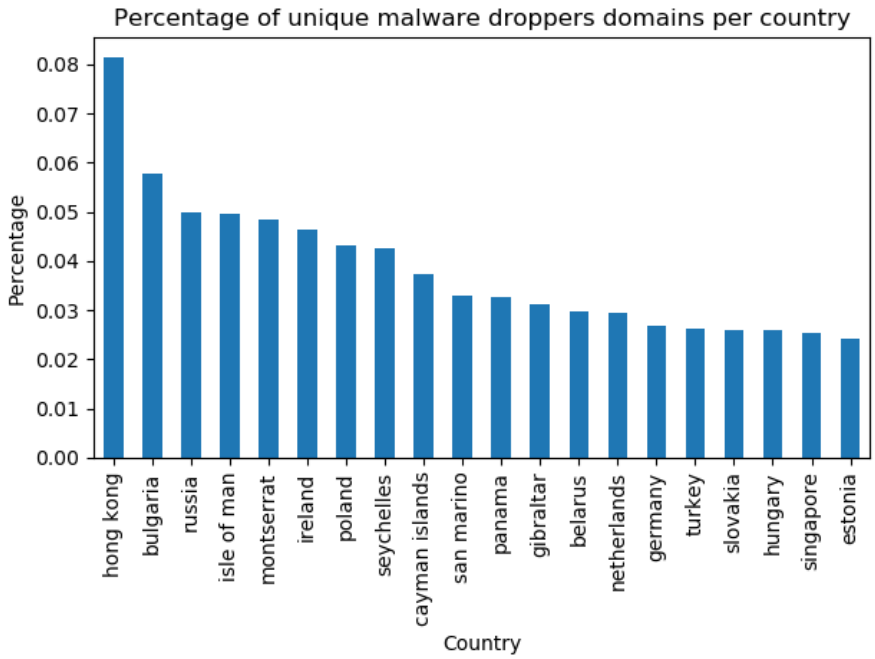

Figure 2: Percentage of malicious domains per country

In order to get better insight into when most malware infections occur, a plot was made showing the amount of clicks aggregated per hour of the day. This plot can be seen in Figure 3. In this plot it can be seen that the most amount of infections actually occur during the evening and at night. Thus, it is more likely that an employee of a company clicks on a malicious link during the night than during work hours. Using this data one can better inform employees that they need to pay attention, especially as the day goes on (and when they work at home during night time).

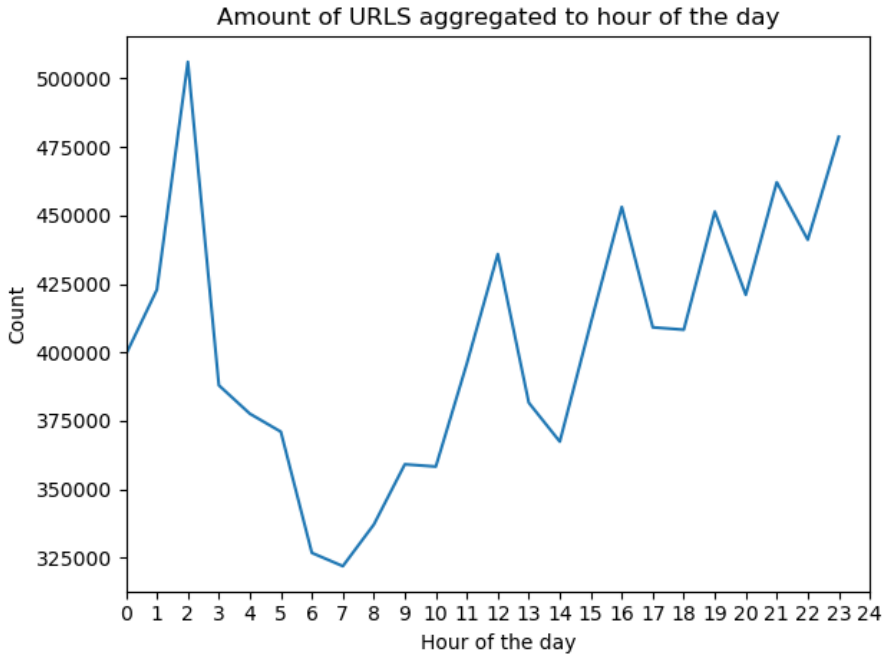

Figure 3: Amount of malware dropped per hour of the day

5 Conclusions

This article reports about the research that was done on malware droppers. The research shows that malware droppers are the source of a lot of malicious behavior. From a literature study we have learned which ideal metrics that one can use.

The literature has shown several metrics security decision makers could use in order to find the areas that need more attention. These ideal metrics can, however, not always be applied, depending on the data that is available. For the malware droppers data set very few of the ideal metrics could be applied. Those that could be applied did however prove useful, as they have indicated several areas with increased risk of malware droppers, such as the Top Level Domain of a website.

From the data set we have been able to derive some key metrics that can be used to make decisions about how to deal with the security issue. Firstly, there are several Top Level Domains that consist for a large part of malware droppers. Thus, these domains should be avoided or blocked whenever possible. Second, the malware droppers are spread quite evenly across countries. Thus, there is

not one single country that needs to address the issue, instead it is a global issue. Finally, we have learned that the amount of malicious clicks (and thus the likelihood that someone clicks a malicious link) increases as the day goes on and is highest during the night time. This data can be used to educate users on when and what to pay attention to and should attribute to enabling people to make safe use of their computers.

Security Investments

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

September 30, 2019

6 Introduction

In order to make a good security investment one must be able to quantify risks. In order to do this meaningful metrics will need to be derived from data. In the previous report this was done resulting in metrics on Top Level Domains, Countries hosting malware droppers and the amount of average clicks for each hour of the day. In order to make a better security investment a new metric has been added, the average amount of malicious clicks per day for each month of the data set. This metric can be used for companies to quantify the likelihood that an employee clicks a malicious link and all devastating consequences that accompany it.

In the next chapter the problem owner mentioned in the previous report will be clarified. After this section 8 will describe the differences in security performance that can be found using our metrics. section 9 will discuss other actors that might have an influence on security decisions that need to be made. After that will give an overview of possible strategies that companies can use to mitigate the risk of malware droppers. Finally in section 11 a risk strategy will be recommended and the return on investment for that specific strategy will be shown.

7 Problem Owner

In this section the stakeholders affected by malware droppers will be analyzed. The primary stakeholder, the actor that suffers the most from malware droppers, will be considered the problem owner for the malware droppers case. Three different stakeholders will be considered in this analysis:

- Companies
- Customers of affected companies
- Regular internet users

Companies

The most obvious affected actor by malware droppers are companies. The malware obtained by droppers can potentially result in the company missing out on revenue by being offline, or in them losing valuable customers data. This could additionally also lead to fines of up to 4% of the companies worldwide annual revenue, as a result of violating the GDPR[22].

Customers of affected companies

Aside from companies being affected themselves, the customers of these companies can also be affected by the malware droppers without having downloaded the droppers themselves. Companies can store sensitive data of customers, such as financial and medical data, which malicious entities could obtain by means of a malware infection. The effects from this range from the individuals receiving spam e-mails to identity fraud, so it's hard to estimate the impact for the customers.

Regular internet users

Lastly, we consider regular internet users: individuals that use the internet for purposes other than work. These users suffer from the same effects as the customers mentioned in the previous section. These users, however, suffer from these effects because of their own actions, and not those of a third party.

7.1 Conclusion

Taking the three previously mentioned stakeholders into consideration, companies suffer the most from malware droppers. Companies have the most to lose, both financially and in other unquantifiable goods, when they are hit with a malware infection. The WannaCry cyber attack in 2018 has shown that this is indeed an issue companies shouldn't ignore. The National Health Service, for example, lost 92 million British pounds as a result of WannaCry [21]. As mentioned earlier, the customers of these companies could also be affected by the company being infected, which in turn could result in major fines.

For these reasons, we consider companies to be our problem owner. The other stakeholders involved will be discussed in detail in section 9.

8 Security Performance Differences

In this section the security performance differences of the generated metrics in the last assignment will be discussed. Each metric will be highlighted and analyzed individually. Due to the fact that our dataset is focused solely on malware droppers, the security performance difference that is discussed in this section is based only on the security performance with regard to malware droppers.

8.1 Hour of the day

The metric that is given in Figure 3 gives an overview of the amount of malware droppers activated, aggregated over every hour of the day. Noticeably we can see that the amount of malware droppers activated is lower during office hours (9 - 17) than after office hours (17 - 2). This means that the security performance during office hours regarding malware droppers is higher than after office hours.

This metric for example says that companies should look at whether the security outside of office hours is sufficient.

8.2 Percentage of unique malware dropper domains per country

The metric that is given in Figure 2 gives the percentage of malicious domains that is registered to that country. We can see that the percentage of malicious domains Russia is higher than the percentage of malicious domains in the Netherlands. This means that the security performance of Russia is lower than the security performance of the Netherlands with regards to malware droppers.

This metric can be used by companies to for example tighten firewall rules for specific countries such as Russia.

8.3 Percentage of unique malware dropper domains per TLD

In Figure 1 the percentage of malicious domains per TLD is given. This metric tells us that the TLD tt has a very high percentage of malicous domains registered. This means that the security performance of the tt TLD is a lot lower than the security performance of the TLD com.

Like the metric about percentage of unique malware dropper domains per country, this metric can be used to tighten firewall rules for specific TLDs such as the TLD tt.

8.4 Amount of malware droppers distributed over every month of the year

In **??** the amount of malware droppers activated, aggregated over each month of the year is given. This metric tells us that, for example, month X has a higher security performance than month Y. This is because in month X the amount of security droppers activated is lower than in month Y.

This metric can help companies decide in which month security training for their employees gives the most effect.

9 Other Actors

In this chapter other actors will be discussed that could have an influence on the security issue at hand and thus influence the risk strategy that a company should take.

9.1 ISP

An internet service provider could prove to be very helpful when dealing with malware droppers. Some ISPs provide their own malware blocking. An example of this is the dutch internet provider XS4ALL that introduced a malware blocking service in May of 2019[24]. Thus the security issue of malware droppers can be reduced by using an ISP that provides such a service(and thus automatically blocks known malware dropper domains).

9.2 Hosting providers

Hosting providers could take more action against malware droppers by taking their droppers offline. This should make it harder for threat actors to spread their malware as they have to keep switching between hosting providers.

9.3 Threat actors

Depending on the type of company threat actors will be different as well. For the purpose of this research we will limit ourselves to companies that do not work with state secrets as this would completely change the risk strategy that would need to be used.

9.3.1 State-sponsored actor

A state-sponsored actor will most likely not focus their resources on a regular company that doesn't deal with the government in any way. Thus for a regular company it is probably not a wise decision to pick their risk strategy to account for such a risk as protecting against state-sponsored actors is most likely not feasible for a regular company.

9.3.2 Organized cyber criminals

The main actors that will influence the security issue mentioned in section 6 are organized cyber criminals. A new deployment of malware by cybercriminals will cause a huge increase in malware droppers and also in traffic to those droppers(due to spam campaigns etc). Using the metrics generated in the first report as well as the new metric mentioned in section 6 we will try to predict these patterns and incorporate them into the risk strategy.

9.3.3 Hacktivists and Competitors

Depending on the operations of the company they could be the target of hacktivists or of competing companies trying to use malware for corporate espionage. This could mean that company employees will be exposed to more targeted malware campaigns than employees of other companies. For this study that will not be taken into account.

10 Risk Strategies

In this section the different risk strategies a company can take to minimize the effect of malware droppers will be discussed. Furthermore, an overview of the different actors identified in section 9 along with their risk strategies will be given.

There are several risk strategies that one can take, namely: avoiding the risk, mitigating the risk, transferring the risk, and accepting the risk [4]. These strategies will be discussed more in depth for the problem owner of our security issue, namely companies.

10.1 Risk Strategies for the Problem Owner

10.1.1 Risk avoidance

The first strategy that could be implemented to deal with the risk of malware infection is that of risk avoidance. In order to completely avoid the risk a company would have to limit the access of its employees to the internet (as to not be exposed to malware at all). This clearly cannot work for modern-day companies as this would cease all business operations. However, it could be possible to avoid as much risk as possible by limiting access of employees to company resources/computers to only employees that absolutely need these resources to do their job. By doing this the risk is lowered as much as possible. This would however create policy obstacles for employees that might hurt business operations and employee morale. This would also still not effectively deal with the risk as the employees that have access could still click a malicious link that infects systems.

10.1.2 Risk mitigation

The second strategy that might be a good option is that of risk mitigation. In order to mitigate the risk of malware infection the company can choose to create new policies for employees to enable the reporting of possibly malicious situations. This will enable to company to deal with malware infections as swiftly as possible and should allow them to mitigate the damage that malware will do to their systems.

On top of this the company can train employees to recognize malicious links

and websites such that they do not get infected in the first place. For these training sessions the metrics from the previous assignment can be used. The metrics indicate that the amount of malicious links clicked increases towards the end of the day. Thus, these training sessions should notify employees of this pattern which should raise their awareness and lower the risk. The percentage of malicious domains per TLD can be used to warn employees of domains that pose a higher risk.

Besides training the employees to better deal with malicious domains the company can install security measures on their systems to mitigate the risk even further. The company should install a firewall that keeps an up-to-date blocklist of malicious domains such as [18]. This should mitigate the risk even further as all of the malicious clicks that are on the blocklist will no longer result in a malware infection.

Finally to mitigate the damage caused by a malware infection the company should install anti-virus software on all systems.

10.1.3 Risk transfer

The third strategy that a company can take is that of risk transfer. Risk transfer means the shifting of risk from one party to another. In the case of our problem owner, a company, this would mean insuring itself against malware droppers, and thus for malware and the damages caused by it. Risk transfer would only be a beneficial strategy if the cost of insuring yourself is lower than the estimated cost of being hit by a malware attack.

Insurance against malware also has downsides, You do not know in advance whether all the damages that you incur by being hit with a malware attack will be paid out. This is because it is very hard to say what exactly the total cost of a malware attack is. For example you do not know how much potential revenue was lost because the company image is damaged. Furthermore, there are also instances where the insurance simply does not pay out the damages that were done by the malware attack like was the case for Mondelez [13].

10.1.4 Risk acceptance

The last strategy that could be taken is that of risk acceptance. Using this strategy the company does nothing with regard to risk management. They accept that there is a risk of malware droppers infecting their systems. This means dealing with the effects of the malware droppers when the company gets hit with a malware dropper. This option would only be beneficial if the estimated costs of getting hit by malware infections is lower than the estimated investments costs to battle malware infections.

10.2 Other Actors With Different Strategies

The risk strategy for companies relies largely on the scale of the company. This means that a startup will use the strategy of risk acceptance rather than any other risk strategy. But a larger company will have multiple risk strategies in place when it comes to malware infections. This is because when a larger company gets hit with a malware infection the damages will be much higher than when a small startup company gets hit with a malware infection. Therefore different company sizes have different risk strategies when it comes to malware infections.

Furthermore, consumers will likely have the strategy of risk mitigation (with the use of an antivirus) and risk acceptance. This is because it is financially not feasible for an individual to adopt the risk transfer strategy.

10.3 Risk Strategy Change Over Time

The risk strategies with regard to malware infection have changed significantly over time. In the past all companies adopted the risk strategy of acceptance. But with the rise in malware infections and the rise in malware impact, the risk strategies of companies have shifted to either risk mitigation, risk transfer, or risk avoidance. Furthermore, the strategy of risk transfer has only been available in recent years. This is due to the fact that only in recent years the concept of insuring against malware attacks has become a possibility.

11 Final Strategy

For the final risk strategy the transfer of risk was chosen. In this chapter multiple risk transfer options will be shown for companies and the Return on Security investment will be calculated for this strategy. In order to do this one must first estimate the costs involved in following this strategy as well as the costs that follow from a malware infection. After this the benefits of the strategy will be calculated and a recommendation will be made as to what the optimal implementation of the strategy will be.

For this draft the security metric of average clicks per day has not yet been added to the report. However in order to write up this chapter we will make a few assumptions about the metric. We will assume that the chance that a person using the internet will have a 0.0001% chance to click on a malicious link per day, and that a click on a malicious link will always lead to an infection.

For the final strategy the strategy will be calculated for three different scenarios. Once for a small company of 10 employees, once for a company with 100 employees and once for a company with 5000 employees.

After doing literature research it was found that the average malware infection costs a company approximately €18.000[19, 6].

11.1 Small company

For a small company with 10 employees the likelihood of an employee clicking a malicious link in the time span of a month is $10 * 0.0001 * 365/12 = 0.03042\%$.

From the data set follows that the average amount of malware infections that occur is 0.0036 annually. The average cost of a malware infection for a small business is around $20.000 [5]. Thus the average cost of malware infections annually is 20.000 * 0.0036 = $72. The average cost of an insurance for a small business is around $1.000/year.

With these numbers we can calculate the ROSI:

$$ROSI = \frac{72 - 1000}{1000} = -0.928$$

From the ROSI we can conclude that it is not beneficial for a small business to acquire an insurance against malware attacks.

11.2 Medium company

For a medium company with 100 employees the likelihood of an employee clicking a malicious link in the time span of a month is $100*0.0001*365/12 = 0.3042\%$

The data set shows that for medium companies an average of $0.3042 * 12/100 = 0.036504$ infections occur a annually, while the average cost for an infection is $50.000. This results in an average cost of a malware infection being $0.036504 * \$50.000 = \$1.825,20$. Additionally, the cost of cyber insurance for a medium sized business is around $10.000/year.

This results in the following ROSI:

$$ROSI = \frac{1825.20 - 10000}{10000} = -1.1805$$

As was the case with small businesses, we can conclude from the ROSI calculation that it is also not beneficial for medium-sized businesses to acquire cyber insurance.

11.3 Large company

For a large company with 5000 employees the likelihood of an employee clicking a malicious link in the time span of a month is $5000*0.0001*365/12 = 15.2083\%$.

From the data set follows that the average amount of malware infections that occur is $15.2083 * 12/100 = 1.825$ annually. The average cost of a malware infection for a large business is around €18000[19]. Additionally, the cost of cyber insurance for a large sized business is around $20.000/year. ROSI = $\frac{18000*1.825-20000}{20000} = 0.6425$

12 Conclusion

In this document we analyzed the actors involved in the security issues around malware droppers. Furthermore, the security performance differences of the different metrics that were generated in the first assignment have been identified. After the security performance differences and the other actors, several risk strategies have been looked at for the problem owner. Finally, the best risk strategy has been further analysed for the problem owner. This risk strategy, that of transferring the risk to another party, has shown result in a high Return on Security Investment for the actors following this strategy.

References

[1] *"WannaCry" ransomware attack losses could reach $4 billion*. [Online; accessed 21. Sep. 2019]. Sept. 2019. URL: https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/.

[2] "2011 Future of Instrumentation International Workshop, FIIW 2011 - Proceedings". In: *2011 Future of Instrumentation International Workshop, FIIW 2011 - Proceedings*. 2011.

[3] Y. Ahmed, S. Naqvi, and M. Josephs. "Cybersecurity Metrics for Enhanced Protection of Healthcare IT Systems". English. In: *International Symposium on Medical Information and Communication Technology, ISMICT*. Vol. 2019-May. 2019. URL: www.scopus.com.

[4] *Common Examples of Risk Management*. [Online; accessed 29. Sep. 2019]. Sept. 2019. URL: https://www.investopedia.com/ask/answers/050715/what-are-some-examples-risk-management-techniques.asp.

[5] *Cyber Liability Insurance Cost - Estimates and Prices at Howmuch*. [Online; accessed 30. Sep. 2019]. Sept. 2019. URL: https://howmuch.net/costs/cyber-liability.

[6] *cyber-liability*. [Online; accessed 29. Sep. 2019]. Sept. 2019. URL: https://howmuch.net/costs/cyber-liability.

[7] *Cybersecurity Ventures Official Annual Cybercrime Report*. [Online; accessed 21. Sep. 2019]. Sept. 2019. URL: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

[8] *Domain Count Statistics for TLDs*. [Online; accessed 21. Sep. 2019]. Sept. 2019. URL: http://research.domaintools.com/statistics/tld-counts/.

[9] *DomainTools Internet Statistics - IP Addresses*. [Online; accessed 21. Sep. 2019]. Sept. 2019. URL: http://research.domaintools.com/statistics/ip-addresses/.

[10] Shuang Hao et al. "Understanding the Domain Registration Behavior of Spammers". In: *Proceedings of the 2013 Conference on Internet Measurement Conference*. IMC '13. Barcelona, Spain: ACM, 2013, pp. 63–76. ISBN:

978-1-4503-1953-9. DOI: 10.1145/2504730.2504753. URL: http://doi.acm.org/10.1145/2504730.2504753.

[11] *Is cybercrime the greatest threat to every company in the world?* [Online; accessed 21. Sep. 2019]. Sept. 2019. URL: https://www.csoonline.com/article/3210912/is-cybercrime-the-greatest-threat-to-every-company-in-the-world.html.

[12] M. Korczyński et al. "Reputation Metrics Design to Improve Intermediary Incentives for Security of TLDs". English. In: *Proceedings - 2nd IEEE European Symposium on Security and Privacy, EuroS and P 2017*. Cited By :6. 2017, pp. 579–594. URL: www.scopus.com.

[13] Kieren McCarthy. "Cyber-insurance shock: Zurich refuses to foot NotPetya ransomware clean-up bill – and claims it's 'an act of war'". In: *The Register* (Jan. 2019). URL: https://www.theregister.co.uk/2019/01/11/notpetya_insurance_claim.

[14] R. S. Miani et al. "A Practical Experience on Evaluating Intrusion Prevention System Event Data as Indicators of Security Issues". In: *Proceedings of the IEEE Symposium on Reliable Distributed Systems*. Vol. 2016-January. 2016, pp. 296–305.

[15] S. Naval et al. "Employing Program Semantics for Malware Detection". In: *IEEE Transactions on Information Forensics and Security* 10.12 (2015), pp. 2591–2604.

[16] F. Skopik et al. "Establishing national cyber situational awareness through incident information clustering". In: *2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2015*. 2015.

[17] E. Takamura et al. "Information security considerations for protecting NASA mission operations centers (MOCs)". In: *IEEE Aerospace Conference Proceedings*. 2015.

[18] *The block list project.* [Online; accessed 28. Sep. 2019]. Sept. 2019. URL: https://blocklist.site/.

[19] *The cost of cybercrime.* [Online; accessed 29. Sep. 2019]. Sept. 2019. URL: https://www.accenture.com/t20190305t185301z__w__/us-en/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf#zoom=50.

[20] *Trojan.Dropper | Symantec.* [Online; accessed 21. Sep. 2019]. Sept. 2019. URL: https://www.symantec.com/security-center/writeup/2002-082718-3007-99.

[21] *WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled.* [Online; accessed 26. Sep. 2019]. Sept. 2019. URL: https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled.

[22] *What are the GDPR Fines? - GDPR.eu.* [Online; accessed 28. Sep. 2019]. July 2018. URL: https://gdpr.eu/fines.

[23] *What is dropper? - Definition from WhatIs.com.* [Online; accessed 21. Sep. 2019]. Sept. 2019. URL: https://whatis.techtarget.com/definition/dropper.

[24] *XS4ALL introduceert als eerste provider malwarefilter in netwerk*. [Online; accessed 28. Sep. 2019]. May 2019. URL: https://blog.xs4all.nl/xs4all-introduceert-als-eerste-provider-malwarefilter-in-netwerk/.