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 [17]. 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 [23]. Malware droppers are a piece of software that is used to infect devices with

the threat which the author wants to spread [29]. 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, 13, 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 [16].

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 [19], 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 [20]. 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	[16]
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)	[19]
13	Incident date	
14	Time until discovery	
15	Time until recovery	
16	Number of new vulnerabilities in the past thirty days	[20]
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	[14]
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.

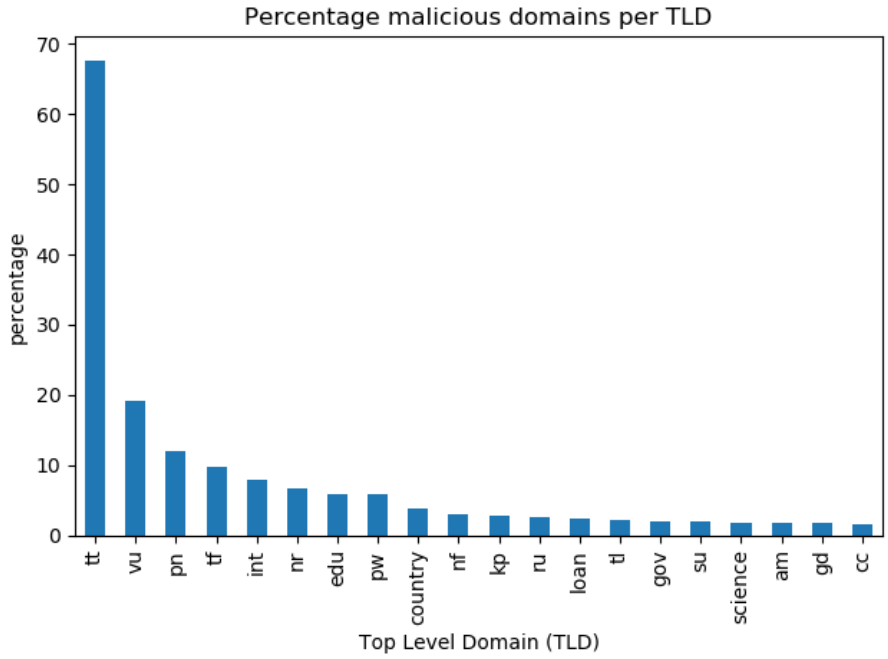

Figure 1: Percentage of malicious domains per TLD

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.

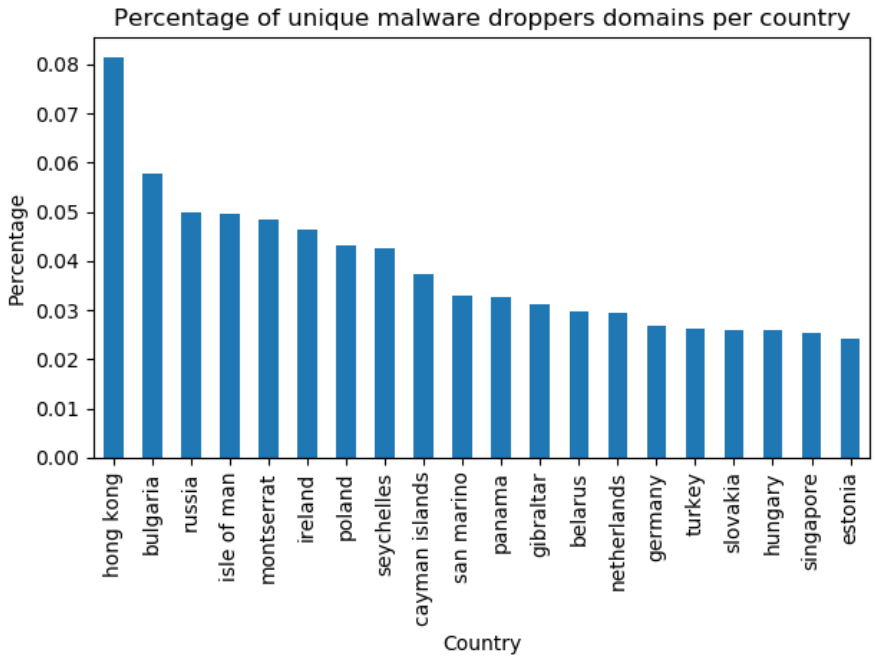

Figure 2: Percentage of malicious domains per country

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).

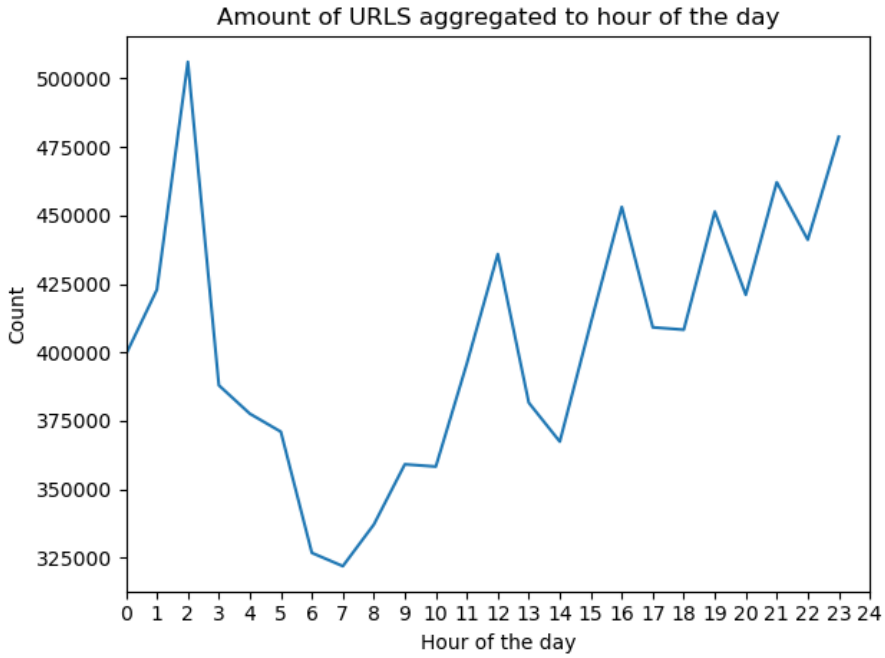

Figure 3: Amount of malware dropped per hour of the day

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

To make a good security investment, one must be able to quantify risks. 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 number of average clicks for each hour of the day. In this report, the security metric of the percentage of malicious domains per TLD will be further explored. This metric can be used by companies to sharpen their firewall rules or IDS alerts which helps with the battle against malware infections.

In section 7 the problem owner mentioned in the previous report will be clarified. After this, section 8 will describe the exposure and differences in security performance of the metric about the percentage of malicious domains per TLD. section 9 will discuss other actors that might influence security decisions that need to be made. Then, section 10 will give an overview of possible strategies that companies can use to mitigate the risk of malware droppers. Finally, in section 11 two risk strategies will be further elaborated and the return on investment for these strategies will be calculated.

7 Problem Owner

In this section, the primary stakeholder affected by malware droppers will be analyzed. This stakeholder will be considered the problem owner for the malware droppers case.

The most affected actors by malware droppers are companies. Therefore, we will consider companies the primary stakeholder. The malware obtained by droppers can potentially result in the company missing out on revenue by being offline, and thus not able to operate. Aside from companies being affected themselves, the customers of these companies can also be affected by the malware droppers without having downloaded any malware. Companies can store sensitive data of customers, such as financial and medical data, which malicious entities could

obtain using malware. This could additionally lead to fines of up to 4% of the companies worldwide annual revenue, as a result of violating the GDPR[28].

Companies, therefore, have a lot to lose, both financially and in other unquantifiable goods (e.g. reputation), when they are hit with a malware infection. The WannaCry cyberattack 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 the WannaCry cyberattack [27]. 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, adding up to the total cost.

For these reasons, we consider companies to be our problem owner. Other stakeholders that can also have an effect on the problem of malware droppers 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. This section will focus specifically on the security performance differences that the metric "percentage of unique malware dropper domains per TLD" highlights. First, the generation process of this metric is given. Then, the resulting metric is shown. Finally, possible implications of the results of the metric are discussed.

The data set was first parsed such that the TLD and domain variables of every entry are given. After the TLD and domain variables were extracted, the number of unique domains per TLD was calculated. After this calculation, the percentage of unique domains for every TLD, normalized over the whole data set could be calculated. However, this metric on itself does not give any meaningful information because it does not take the exposure of each TLD into account. This means the total amount of unique domains per TLD on the internet is not included within the calculation.

To remedy the problem of not taking into account the exposure of each TLD, the percentages were not normalized on the size of the data set but the count of domains of each TLD. This takes the exposure of each TLD into account where the exposure is the total size of each TLD. The information for the count of domains per TLD was extracted from Domaintools [8]. Using the number of domains per TLD on the internet and the number of domains per TLD from the data set, the percentages of malicious domains per TLD could be calculated. These percentages are visualized in Figure 4.

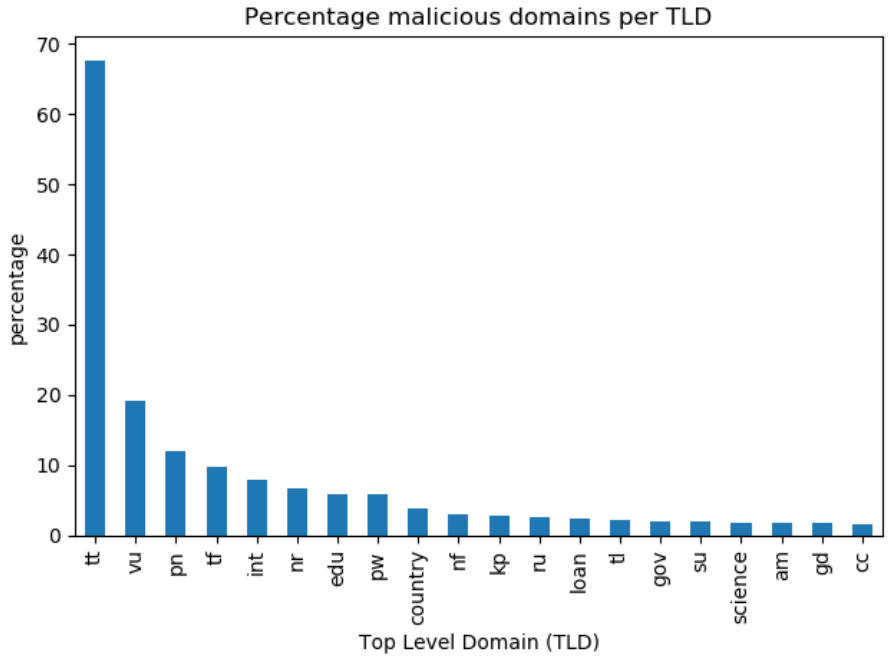

Figure 4: Percentage of malicious domains per TLD

From Figure 4 the TLDs with the highest percentages of malicious domains are visualized. We can see that the tt TLD has a very high percentage of malicious domains. This means that the security performance of the tt TLD is lower than, for example, the com TLD.

The metric of the percentage of malicious domains per TLD could be used by companies to, for example, set firewall rules or IPS rules that are stricter for these domains than for domains with a higher security performance.

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 malware blocking themselves. An example of this is the Dutch internet provider XS4ALL that introduced a malware

blocking service in May of 2019[30]. 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 the malware dropper domains that they host offline. This should make it harder for threat actors to spread their malware as they would need to keep switching between hosting providers.

9.3 Threat actors

Depending on the type of company, threat actors will be different as well. For 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 not a wise decision to pick their risk strategy to account for such a risk as protecting against state-sponsored actors increases the cost of security significantly while it does not secure them against a lot of actors.

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 etcetera). Using the metrics generated in the first report 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 [5]. 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. 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 need these resources to do their job. By doing this, the risk is lowered. This would, however, create policy obstacles for employees that might hurt business operations and employee morale. This would still not effectively deal with the risk as the employees that have access could still click a malicious link that infects the company's systems.

10.1.2 Risk mitigation

The second strategy that might be a good option is that of risk mitigation. To mitigate risk, a company can employ different technologies to lower their risk during their business activities. The most straightforward solution for this would be a firewall (or to upgrade their existing firewall). This firewall should make use of an up-to-date blacklist of malicious domains such as [21]. This will lower the amount of risk as any malicious link that is clicked and blocked by the firewall will no longer result in a malware infection.

Another technology that a company can employ is anti-virus software. This will catch most of the malware that is not blocked by the firewall and should lower the risk even further.

Another option a company has to mitigate the risk of malware infection is 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 number of malicious links clicked increases towards the end of the day. Thus, these training sessions could 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.

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 the malware attacks in the same period of time.

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 [15].

10.1.4 Risk acceptance

The last strategy that could be taken is that of risk acceptance. Using this strategy, the company does nothing concerning 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 are lower than the estimated investment 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 anti-virus software and firewalls) 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 concerning 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 because only in recent years the concept of insuring against malware attacks has become a possibility.

11 Final Strategy

For the final risk strategy, the mitigation of risk was chosen. In this chapter, both technical and operational options will be discussed that can be employed to mitigate the risk that malware droppers pose to a company. For both options, the return on security investment (ROSI) will be calculated and a recommendation will be made as to if the strategy should be implemented by the problem owner (a company).

For this risk strategy, calculations will be made for a small, medium and large-sized company. This is done to make this report useful for as many companies as possible and hopefully, help them improve their security.

A small company is a company with around 50 employees, a medium-sized company is a company with around 500 employees and a large company has around 10,000 employees. To keep this strategy applicable to as many companies as possible it is assumed that the companies do not do business with the government to avoid the elevated security risk that comes with this. Furthermore, it is assumed that they do not do business with educational institutions as there is a .edu TLD in our dataset and blocking .edu domains is not a very practical solution in that case. The small company has a yearly revenue of $5M, the medium-size company a revenue of $50M and the large company a revenue of $2B. An overview of the company profiles is given in Table 2.

Company type	Employee count	Yearly revenue
Small	50	$5,000,000
Medium	500	$50,000,000
Large	10,000	$2,000,000,000

Table 2: Companies used in Risk strategy calculations

Each of these types of companies will have a different cost per security inci-

dent, as a larger company has more to lose than a smaller company in terms quantifiable and unquantifiable goods, such as personal data and reputation. Additionally, the companies also have differing amounts of attacks hitting their infrastructure per year, under the assumption that a larger company is more often targeted by cyber attacks. These numbers have been based on information found for small companies, as exact numbers are not publicly available for different company types[26, 22, 6].

Company type	Incidents per year	Cost per incident
Small	3	$10,000
Medium	10	$100,000
Large	50	$2,000,000

Table 3: The costs associated with each security incident per company type

11.1 Firewall

From the previous report on security metrics, one can learn that many top level domains consist of mainly malicious activity. A firewall can be used to block these domains and mitigate the risk of malware dropers the company faces. For example, from Figure 4 one can see that almost 70% of all domains in the tt TLD are malicious.

Using the metric of "percentage of malicious domains per TLD" one can decide which domains to block. In this case, the top 10 most malicious domains will be blocked by the firewall. This means that the following domains will be blocked by the firewall:

- .tt
- .vu
- .pn
- .tf
- .int
- .nr
- .edu
- .pw
- .country
- .nf

For each domain, it is necessary to calculate the reduction of malicious infections when blocking these domains. To quantify this, a table was generated from the data set that shows how much of the data set is represented by each top level domain.

Name	Percentage of data set
.tt	0.047666%
.vu	0.004595%
.pn	0.001022%
.tf	0.004161%
.int	0.000485%
.nr	0.000248%
.edu	0.012474%
.pw	0.415082%
.country	0.000423%
.nf	0.000382%

Table 4: Domains relative to the size of the data set

From Table 4 it follows that blocking these 10 domains will lower the amount of malware installed by 0.49%.

$$\begin{aligned} \textit{Mitigation percentage} = {} & 0.047666 + 0.004595 + 0.001022 + 0.004161 + 0.000485 + \\ & 0.000248 + 0.012474 + 0.415082 + 0.000423 + 0.000382 \\ = {} & 0.486538\% \end{aligned}$$

Thus, assuming that each malicious click in the data set is possible with the same likelihood, this will result in a mitigation rate of $\frac{487}{100000}$.

Different costs come with a proper firewall. First of all, there is a purchase and setup price. This is usually a one-time cost. The price for this differs based on the size of a company. During the ROSI calculations, these different prices will be discussed. After this, there are also variable costs that come with a firewall. Some firewalls use subscriptions for extra firewall features such as VPN connections or web caching. For the sake of keeping this calculation somewhat applicable to most companies, we will only use VPN connections as a feature that has recurring costs. $15 seems like a reasonable price per VPN connection per month according to [4]. We will assume that 50% of employees will make use of such a VPN connection for each company.

When blocking entire top level domains it is unavoidable that this will influence business operations as well. Thus, this option comes with an opportunity cost as some websites might be unavailable to employees, hindering their ability to do their jobs. Given the fact that the domains that we block are all domains that have fairly low usage, we will calculate their usage by dividing the total amount of domains registered for that TLD[8] to the total amount of domains registered[12]. This can be seen in Table 5:

Name	Size of TLD	Percentage of global TLDs
.tt	3985	0.001132745%
.vu	1602	0.000455372%
.pn	735	0.000208925%
.tf	3018	0.000857873%
.int	204	0.0000579874929%
.nr	296	0.0000841387152%
.edu	7508	0.002134167%
.pw	393568	0.111872654%
.country	960	0.000272882%
.nf	1090	0.000309835%

Table 5: Domains relative to the size of all TLDs

Assuming that these percentages also reflect the percentages of actual use of these domains for each company, that means that communication will no longer work with the following percentage of potential customers:

$$\begin{aligned} \textit{Unreachable customers} = {} & 0.001132745 + 0.000455372 + \\ & 0.000208925 + 0.000857873 + \\ & 0.000057987 + 0.000084139 + \\ & 0.002134167 + 0.111872654 + \\ & 0.000272882 + 0.000309835 \\ = {} & 0.1173865792\% \end{aligned}$$

From this, we estimate that the opportunity cost would be a drop in company revenue of roughly 0.12%. For each company, we will use a profit margin of 10% as that is the average across different industries[18]. This will result in an opportunity cost of $0.12 * 0.1 = 0.012\%$ of company revenue.

11.1.1 Small company

In the scenario of a small company the costs for making use of a firewall will be as follows:

A license for a firewall for a small company costs approximately $3,500 per year according to [11]. This includes setup and service of the firewall.

VPN subscriptions for a small company will cost $\frac{1}{2} * 50 * \$15 * 12 = \$4,500$ per year.

The opportunity cost for a small company will be $0.00012 * \$5,000,000 = \$600$ per year.

From these numbers, the Cost of solution (per year) can be derived.

$$Cost\ of\ solution = \$3,500 + \$4,500 + \$600 = \$8,600$$

The annual loss expectancy (ALE) can be derived from the statistics mentioned earlier in this chapter.

$$ALE = Single\ loss\ expectancy * Annualized\ rate\ of\ occurrence = \$10,000 * 3 = \$30,000$$

With these numbers we can calculate the ROSI:

$$ROSI = \frac{ALE * mitigation\ ratio - Cost\ of\ solution}{Cost\ of\ solution}$$

$$ROSI = \frac{\$30,000 * \frac{487}{100,000} - \$8,600}{\$8,600} = -0.98 = -98\%$$

As we can see for a small company it is not worth it to implement a firewall that blocks malicious domains as their yearly investment will be almost twice the cost of the expected damage caused by malware.

11.1.2 Medium-sized company

In the scenario of a medium-sized company the costs for making use of a firewall will be as follows:

A license for a firewall for a medium-sized company costs approximately $5,000 per year according to [4]. This includes setup and service of the firewall.

VPN subscriptions for a medium-sized company will cost $\frac{1}{2} * 500 * \$15 * 12 = \$45,000$ per year.

The opportunity cost for a medium-sized company will be $0.00012 * \$50,000,000 = \$6,000$ per year.

From these numbers, the Cost of solution (per year) can be derived.

$$Cost\ of\ solution = \$5,000 + \$45,000 + \$6,000 = \$56,000$$

The annual loss expectancy(ALE) can be derived from the statistics mentioned earlier in this chapter.

$$ALE = Single\ loss\ expectancy * Annualized\ rate\ of\ occurrence = \$100,000 * 10 = \$1,000,000$$

With these numbers we can calculate the ROSI:

$$ROSI = \frac{ALE * mitigation\ ratio - Cost\ of\ solution}{Cost\ of\ solution}$$

$$ROSI = \frac{\$1,000,000 * \frac{487}{100,000} - \$56,000}{\$56,000} = -0.91 = -91\%$$

From this, we learn that it is also not worth it to purchase a TLD blocking firewall for medium-sized companies.

11.1.3 Large company

In the scenario of a large company the costs for making use of a firewall will be as follows:

A license for a firewall for a large company costs approximately $25,000 per year according to [4]. This includes setup and service of the firewall.

VPN subscriptions for a large company will cost $\frac{1}{2} * 10,000 * \$15 * 12 = \$900,000$ per year.

The opportunity cost for a large company will be $0.00012 * \$2,000,000,000 = \$2,400,000$ per year.

From these numbers, the Cost of solution (per year) can be derived.

$$Cost\ of\ solution = \$25,000 + \$900,000 + \$2,400,000 = \$3,325,000$$

The annual loss expectancy (ALE) can be derived from the statistics mentioned earlier in this chapter.

$ALE = Single\ loss\ expectancy * Annualized\ rate\ of\ occurrence = \$2,000,000 * 50 = \$100,000,000$

With these numbers we can calculate the ROSI:

$$ROSI = \frac{ALE * mitigation\ ratio - Cost\ of\ solution}{Cost\ of\ solution}$$

$$ROSI = \frac{\$100,000,000 * \frac{487}{100,000} - \$3,325,000}{\$3,325,000} = -0.85 = -85\%$$

From this, it follows that for large companies it is also not a valid strategy to invest in a TLD blocking firewall.

11.1.4 Discussion

From the previous sections, it follows that no company size actually benefits from a TLD blocking firewall. This is due to the extremely low mitigation ratio. From this, we can conclude that blocking malicious TLDs is not a good security investment. If a firewall is implemented that makes use of blacklists consisting of data sets like the one used for this study then the mitigation ratio

will be much higher which would result in a positive ROSI. In the next section, we will give an alternate solution, not necessarily based on the data set, that could also be employed to lower the risk of malware infections.

11.2 Operational Options

Blocking all domains using a firewall would be unfeasible, as this would result in the company simply being cut off from the internet, making them unable to do business. For the remainder of unblocked domains, the employees of the companies could be able to use their judgment to determine whether an URL is potentially malicious or not. This judgment could be trained through security awareness training sessions. After the employees have been trained, an additional layer on top of the firewall is placed, to reduce the number of infections even further.

When considering the total costs for security training, the hourly wage for an employee has to be considered in addition to the cost of the training session itself. The cost of security awareness training sessions varies wildly for each type of training. Mobile applications are on the cheap side of the spectrum at less than one dollar per employee, while training sessions in person can be up to $75 per employee[25]. We will only consider training sessions in person now as these sessions have a clear start and end, allowing us to calculate the total costs more accurately. The mobile applications could be used whenever, making it very hard to estimate the hourly wage used on the application.

The median weekly earnings of a full-time worker in the United States is $908 in the second quarter of 2019, according to the Bureau of Labor Statistic[24]. If we assume that a full-time worker works 40 hours a week, we get a median hourly earning of $22.70. The most popular cyber security awareness training sessions take up an entire day, resulting in a total cost of $22.70 * 8 = $181.60 in wages per employee. This is in addition to the cost of the training session itself, which we estimate at $75 based on the most popular cyber security training sessions available[25]. This adds up to a total cost of $181.60 + $75.00 = $256.60 per employee.

As there is no way to precisely measure the impact of cyber security awareness training sessions on the number of clicks on malware droppers, we have to estimate this number. In the data set, it can be seen that most, if not all, of the malware droppers are downloaded through fairly obscure URLs to foreign domains, suspicious executables, and other URLs which have nothing to do with the day-to-day operations of a company. We, therefore, believe that if the security awareness training is performed successfully, and the employees are indeed more security-aware, the number of infections through these URLs will drastically decrease. Based on the entries in the data set and what was mentioned earlier about the URLs, we will assume this number of infections mitigated to be 20%.

11.2.1 Small company

In the scenario of a small company the costs of security awareness training will be as follows:

As the only costs for training sessions are costs per employee we can directly calculate the cost of solution using that. We make the assumption that for these training sessions to be effective they need to be done once a year.

From these numbers, the Cost of solution (per year) can be derived.

$$Cost\ of\ solution = 50 * \$256.60 = \$12,830$$

The annual loss expectancy (ALE) can be derived from the statistics mentioned earlier in this chapter.

$ALE = Single\ loss\ expectancy * Annualized\ rate\ of\ occurrence = \$10,000 * 3 = \$30,000$

With these numbers we can calculate the ROSI:

$$ROSI = \frac{ALE * mitigation\ ratio - Cost\ of\ solution}{Cost\ of\ solution}$$

$$ROSI = \frac{\$30,000 * \frac{2}{10} - \$12,830}{\$12,830} = -0.53 = -53\%$$

From this, we learn that security training for employees is not worth it for a small company.

11.2.2 Medium-sized company

In the scenario of a medium-sized company the costs for security training will be as follows:

$$Cost\ of\ solution = 500 * \$256.60 = \$128,300$$

The annual loss expectancy (ALE) can be derived from the statistics mentioned earlier in this chapter.

$ALE = Single\ loss\ expectancy * Annualized\ rate\ of\ occurrence = \$100,000 * 10 = \$1,000,000$

With these numbers we can calculate the ROSI:

$$ROSI = \frac{ALE * mitigation\ ratio - Cost\ of\ solution}{Cost\ of\ solution}$$

$$ROSI = \frac{\$1,000,000 * \frac{2}{10} - \$128,300}{\$128,300} = 0.56 = 56\%$$

For medium-sized companies, it is still not recommended to do the training if it has a mitigation rate of 20% as the training will cost more than the damage that it will prevent.

11.2.3 Large company

In the scenario of a large company the costs for security training will be as follows:

$$Cost\ of\ solution = 10,000 * \$256.60 = \$2,566,000$$

The annual loss expectancy (ALE) can be derived from the statistics mentioned earlier in this chapter.

$$\begin{aligned} ALE &= Single\ loss\ expectancy * Annualized\ rate\ of\ occurrence \\ &= \$2,000,000 * 50 \\ &= \$100,000,000 \end{aligned}$$

With these numbers we can calculate the ROSI:

$$ROSI = \frac{ALE * mitigation\ ratio - Cost\ of\ solution}{Cost\ of\ solution}$$

$$ROSI = \frac{\$100,000,000 * \frac{2}{10} - \$2,566,000}{\$2,566,000} = 6.79 = 679\%$$

From this, we find that for large companies security awareness training sessions are a very good investment. On top of that, somewhere between the medium and large company, there is a tipping point in revenue and amount of employees where it starts becoming a profitable investment.

12 Conclusion

In this document, we analyzed the actors involved in the security issues around malware droppers. Furthermore, the security performance and exposure of the metric "the percentage of malicious domains per TLD" have been identified and discussed. After the security performance differences and the other actors, several risk strategies have been looked at for the problem owner. Finally, the risk strategy of risk mitigation has been further analysed for the problem owner. From this, we learned that blocking top level domains is not a viable way of mitigating the risk of malware droppers for any sized company. This is because the mitigation ratio is very low. A firewall using a blacklist of malicious URLs will have better performance.

After concluding that blocking TLDs was not a valid option, the risk mitigation strategy of employee training was explored. For small and medium-sized companies, employee training is still not a valid option as it will not provide a good return on security investment. However, for a large company employee training proves to be a very good investment. Thus, when a company is growing it will eventually reach a point where employee training starts to be a good investment to deal with the problem of malware droppers.

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] *Choosing a firewall*. [Online; accessed 6. Oct. 2019]. 2019. URL: http://techgenix.com/choosing_a_firewall/.

[5] *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.

[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] *How much does a firewall cost*. [Online; accessed 6. Oct. 2019]. 2019. URL: https://www.manxtechgroup.com/how-much-does-a-firewall-cost/.

[12] *Internet Grows to 351.8 Million Domain Name Registrations in the First Quarter of 2019*. [Online; accessed 6. Oct. 2019]. 2019. URL: https://finance.yahoo.com/news/internet-grows-351-8-million-202000514.html.

[13] *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.

[14] 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.

[15] 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.

[16] 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.

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

[18] *Profit Margin: Formula and What Makes a Good Profit Margin*. [Online; accessed 6. Oct. 2019]. 2019. URL: https://www.fundera.com/blog/profit-margins.

[19] 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.

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

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

[22] *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.

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

[24] *USUAL WEEKLY EARNINGS OF WAGE AND SALARY WORKERS SECOND QUARTER 2019*. [Online; accessed 6. Oct. 2019]. July 2019. URL: https://www.bls.gov/news.release/pdf/wkyeng.pdf.

[25] *Vergelijk 28 Security awareness trainingen en cursussen – Springest*. [Online; accessed 6. Oct. 2019]. Oct. 2019. URL: https://www.springest.nl/automatisering-ict/security-awareness.

[26] Ivana Vojinovic. "30+ Fear-Inducing Cyber Security Statistics". In: *SmallBizGenius* (Aug. 2019). URL: https://www.smallbizgenius.net/by-the-numbers/cyber-security-statistics.

[27] *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.

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

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

[30] *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/.