EoS - Actors and Security Strategies

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

October 13, 2019

1 Introduction

In this assignment, different actors and their security strategies against the security issue of malware droppers are discussed. Then, the security metric that we have chosen in the previous assignment will be further analysed and statistical tests will be performed.

Section 2 identifies three different actors regarding the security issue of malware droppers. For each actor, a countermeasure and their consequences will be further analysed. Then, in section 3 different factors causing the variance in the metric will be given and a statistical test for this factor will be calculated. Finally, section 4 draws conclusions and summarizes the report.

2 Actors Involved in the Security Issue

The actors we have chosen that are involved with different aspects of the security issue of malware droppers are:

- Companies being targeted by malware droppers (problem owner)
- Domain registrars
- Hosting providers

These actors were chosen as they are all affected by the security issue of malware droppers, but on different levels. Since they are all affected on different levels, each of these actors will also have a different mitigation strategy for the security issue. The companies are those being targeted by the droppers and receiving the actual malware, while domain registrars never even touch the malware. Nevertheless, according to the metrics, the domain registrars do play an important role in malware droppers. Lastly, the hosting providers are the actors serving the actual malware themselves, and thus they could also play a role in preventing malware droppers from existing by not offering their services to malicious

entities.

2.1 Companies

2.1.1 Concrete Countermeasure

From the previous report, it follows that the best countermeasure that companies can take is to do yearly security training with their employees. This will give companies with more than 100 employees a positive return on security investment and will reduce the risk that their company is exposed to. Because the return on security investment is positive, the benefits for the company outweigh the costs for the company.

2.1.2 Distribution of Cost and Benefit Analysis for Different Actors

If the companies implement the security awareness training countermeasure into their business, less infections will spread through the company network onto their websites. This leads to the fact that there are less infections on the side of the hosting providers where these companies host their websites. Therefore, the hosting providers have a benefit when companies implement the security awareness training countermeasure. Furthermore, like the hosting providers, the domain registrars have fewer malicious domains assigned to their name if the companies utilising that registrar implement the security awareness training countermeasure.

2.1.3 Incentive to Take Countermeasure

Medium and large-sized companies have a monetary incentive to take the countermeasure of investing in security awareness training for their employees. This claim is backed by the previous assignment where the ROSI for medium and large-sized companies is positive. The ROSI took all the potential costs and potential losses regarding the security issue of malware droppers into account.

As security awareness training sessions can have a big impact on the security issue while being one of the cheapest options a company can take, this countermeasure does not have any drawbacks when considering the returns. The ROSI calculations shown in the previous report confirm this.

2.1.4 Reflection of Externalities Around the Security Issue

A negative externality when a company is hit with a malware attack is the loss of reputation. When a company gets hit with a malware attack and it impacts personal data, they must report that to the people or companies that are affected by the malware. This will present the company in a negative light. Therefore, the externality of loss of reputation plays a role in the decision process for companies to consider making more information security investments.

2.2 Domain Registrars

2.2.1 Concrete Countermeasure for Each Actor

Since certain TLDs are more commonly used for malware droppers than others, the domain registrars for those TLDs could start verifying the identity of their customers as a way to prevent malware droppers. Registering a domain is currently being done by simply filling in an online form, without any verification of whether the details filled in are legitimate. So, domain registration is in actuality an anonymous process. By verifying the identity of those who register a domain, a blacklist can be created for those who use the domain for their malware droppers. Additionally, the fact that domain registration is no longer an anonymous process might scare malicious actors away.

2.2.2 Distribution of Cost and Benefit Analysis for Different Actors

The benefits for domain registrars are mostly reputational, as domains that are currently primarily used for malware will be used for their intended purpose instead. This can, in turn, increase the trust into these domains, and might make managers of firewalls remove these domains from their blacklist, as was proposed in the previous report. Customers from these countries belonging to the TLDs might then consider using the TLD for their companies instead of alternatives such as `.com`, as they are now able to do business using their own TLD as well.

Costs for the domain registrars are due to lost customers that will no longer use their services as a result of the loss of privacy that follows from the extra verification, and loss of customers intending to use it for nefarious purposes. Additionally, the company will have to spend extra resources on verifying the customers' identity. The domain registrar also has to take into account the rules of the GDPR when processing personal information, to avoid getting fined[3, 5].

Identity verification will result in the same costs for companies as for regular customers of the domain registrar, which is that they have to give up a certain amount of privacy by giving the registrars their personally identifiable information. For this report, we assume that the domain registrars will not abuse this information for purposes such as identity fraud, as this will bring in a whole lot of other consequences and issues.

The benefit for regular companies is that they can remove the domains corresponding to a previously bad TLD from the blacklist of their firewall. This allows them to do business with the companies using those TLDs, resulting in potentially higher revenue, as was shown in the previous report.

Hosting providers will not notice much from this countermeasure. Those who want to have a location to host their website or files will do it regardless of which TLD, as a TLD is a separate component of a web service, on top of the server where the website is hosted.

2.2.3 Incentive to Take Countermeasure

The incentive for the domain registrars to take the countermeasure of verifying the identity of their customers is related to the reputation of that domain registrar. By verifying the identity of their customers, the percentage of malicious domains on that registrar will drop. This will result in a better reputation of that registrar because they have less malicious domains under their name. So, there is an incentive for domain registrars to take this countermeasure.

The drawback from this countermeasure for the domain registrars is the fact that they generate extra workload for their employees without directly creating extra profit. This means adding extra costs to implement the security measure while the benefits might only come later in the form of extra customers.

2.2.4 Reflection of Externalities Around the Security Issue

An externality regarding domain registrars is the number of malicious domains registered with their registrar. This can attract or discourage potential new customers for registering a domain with them. If there is a low percentage of malicious domains with a specific registrar, they can use that to boost their publicity and reputation advertising themselves as a secure registrar. If there is a high percentage of malicious domains with a specific registrar, it will reflect badly on the registrar as it will result in people considering them malicious.

2.3 Hosting Providers

2.3.1 Concrete Countermeasure for Each Actor

The most concrete countermeasure that hosting providers can take to combat the problem of malware droppers is to implement a solution that automatically takes malicious websites offline. This takes care of the root of the problem: the fact that threat actors can host their malware on servers provided by hosting providers.

2.3.2 Distribution of Cost and Benefit Analysis for Different Actors

This solution will cost the hosting providers money as the malicious actors will no longer pay them for their domain.

It will benefit the hosting providers as an automatic solution will save them a lot of human work. Taking a more pro-active approach towards malware will result in less pressure from the government and possibly fewer fines.

This countermeasure will also benefit companies as there will be fewer malware droppers online and thus the chances of a company employee clicking an active malicious link will in turn also be lower.

This countermeasure will also benefit domain registrars as they will have to take fewer domains offline. If the hosted service behind a malicious domain gets

taken offline it is no longer necessary for domain registrars to act upon that domain.

2.3.3 Incentive to Take Countermeasure

There is no real monetary incentive for hosting providers to take malicious domains offline as that results in a loss of income.

There is however an incentive for hosting providers with regards to their reputation. If they are known to be a very reliable hosting provider that deals with malware very well then they will most likely obtain more legitimate customers, which will indirectly also benefit them.

A drawback of the countermeasure would be the fact that the implementation introduces extra costs for the company. They have to set up an automatic service for detecting and shutting down malicious websites. Furthermore, automatically shutting down malicious websites might take down legitimate websites. This will put the hosting provider in a negative light, which could cause them to lose clients to competitors.

2.3.4 Reflection of Externalities Around the Security Issue

The externality for hosting providers is that their reputation will depend on the number of malicious websites they are hosting. If they host a high amount of malicious domains, it will reflect badly on their security performance and their reputation as a secure hosting provider. If they host a low amount of malicious domains, it will reflect positively on their security performance and their reputation as a secure hosting provider.

3 Actor's Security Performance According to the Security Metric

This section will analyze the security performance that is highlighted with the metric that was chosen in the previous assignment. First, the metric and a brief explanation is given. Then, factors causing the variance in the data will be discussed. Next, data backing these factors will be given. Finally, a statistical analysis is performed to give the impact of these factors on the metric.

The metric that will be used in this assignment and was analysed in the last assignment is *the percentage of malicious domains per TLD*. The metric is given in Figure 1.

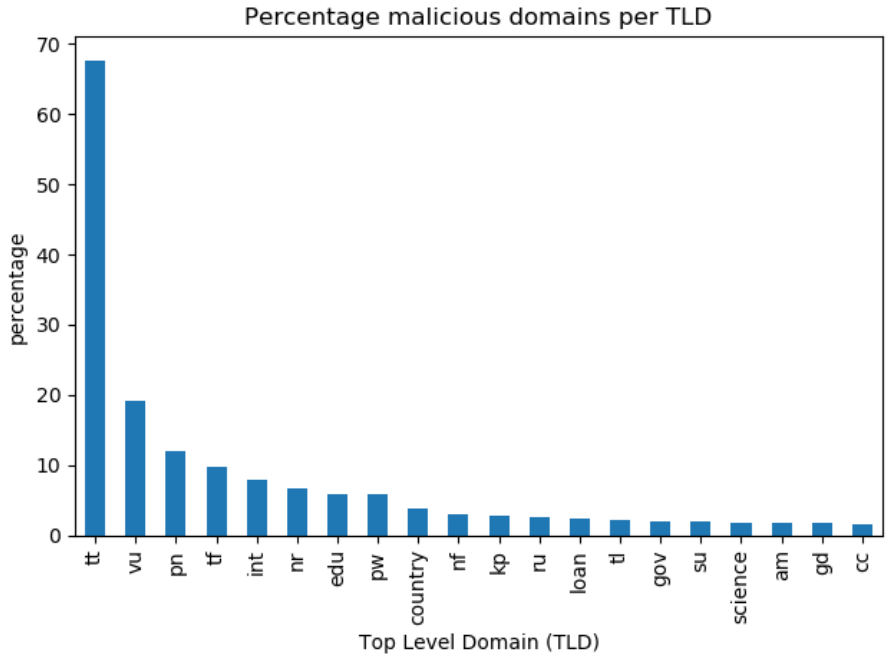

Figure 1: Percentage of malicious domains per TLD(normalized over TLD size)

The metric is generated by counting the number of unique domains for each TLD in the dataset and dividing it by the number of unique domains registered to that TLD. The information for the total amount of domains per TLD is gathered from Domaintools [2].

3.1 Factors Explaining the Variance in the Metric

From the metric, we can learn that mainly small top level domains are used for malicious activity. One characteristic of these domains that might explain the variance in the metric is the price of such a domain registration. A low price of domain registration will most likely lead to more malicious activity on that top level domain. Thus, a top level domain with a low average price might indicate more malicious actors on that domain.

On top of this, it might be possible that threat actors make use of domain registrars that are more lenient with regards to the information necessary to register a domain. Therefore, there might be a correlation between registrars used for a specific TLD and the malicious activity on that TLD.

From the metric, it is hard to determine if the malware droppers are still active on the domain or if the domain has since been cleared of malware. As a result of

this, it might be possible that a domain occurs in the data set quite a lot but is cleared of malware fast. The data set does not show when domains are cleared of malware droppers so unfortunately we are not able to account for this.

3.2 Data collection of these factors

To find out whether the domain price drives the usage of domains by malicious actors the average domain price per TLD was collected from [1]. This data can be found in Table 1. We decided to use the average domain price instead of the cheapest domain price as this would give us a data set that would not be heavily influenced by one registrar. For example, if a domain registrar currently has a discount on one of the domains this would heavily influence a data set based on the lowest price per domain. Therefore, the average domain price is used over as many registrars as we could find to reduce the impact one single registrar has on the data set. A price of `N/A` means the top level domain is not available for purchase by regular consumers, and is reserved for special organizations (e.g. `.edu` for educational institutions).

TLD	Average domain price
tt	$723.02
vu	$109.90
pn	$197.29
tf	$17.55
int	N/A
nr	$738.89
edu	N/A
pw	$17.47
country	$31.76
nf	$855.61
kp	N/A
ru	$23.58
loan	$21.94
tl	$98.78
gov	N/A
su	$34.19
science	$23.12
am	$71.18
gd	$46.08
cc	$20.86

Table 1: Average TLD price

3.3 Statistical Analysis

For the statistical analysis, the Spearman rank correlation test will be used to analyze the relationship between the price of a domain and the amount of

relative malicious activity on that domain. The Spearman test was chosen as it is a non-parametric test that does not carry any assumptions about the distribution of the data. The Pearson test assumes that the data is normally distributed, which in the case of percentages is not true, which is why we decided to opt for the Spearman rank correlation test instead of the Pearson correlation test.

The Spearman rank correlation test was performed using Python with the `Scipy` package. The code can be found on the GitHub repository of this project[1].

The data that will be used for this analysis is displayed in Table 2. Since the `.int`, `.edu`, `.kp` and `.gov` domains do not allow any registration these domains have been removed from the data set used for calculation.

TLD	Malicious percentage	Average domain price
tt	0.676	$723.02
vu	0.191	$109.90
pn	0.120	$197.29
tf	0.097	$17.55
nr	0.067	$738.89
pw	0.059	$17.47
country	0.039	$31.76
nf	0.029	$855.61
ru	0.026	$23.58
loan	0.023	$21.94
tl	0.021	$98.78
su	0.019	$34.19
science	0.018	$23.12
am	0.017	$71.18
gd	0.017	$46.08
cc	0.016	$20.86

Table 2: Data used for statistical analysis

For the Spearman test we assume the following:

H_0 = There is no correlation between the average price of a domain and the maliciousness of that domain.

H_1 = There is a correlation between the average price of a domain and the maliciousness of that domain.

From the Spearman calculation we get the following result:

$$Rho = 0.33$$
$$pval = 0.21$$

[1] `https://github.com/joostprins/EoS-malware-droppers/blob/master/actors-and-security-strategies/scripts/spearman_test.py`

From the Rho value, we find that there is a weak correlation between the average price of a domain and the maliciousness of that domain. However, as we have a P-value of (a lot) more than 10% there is very weak to no evidence that we should reject H_0 in favour of H_1[4]. Thus, we can conclude that there is no correlation between the average price of a domain and the maliciousness of that domain.

A scatter plot of the data was made to visualize the relationship between the popularity of a malicious TLD and the average price said TLD can be purchased for. This visualization can be seen in Figure 2. This visualization also shows that there is no clear positive or negative correlation between the two variables.

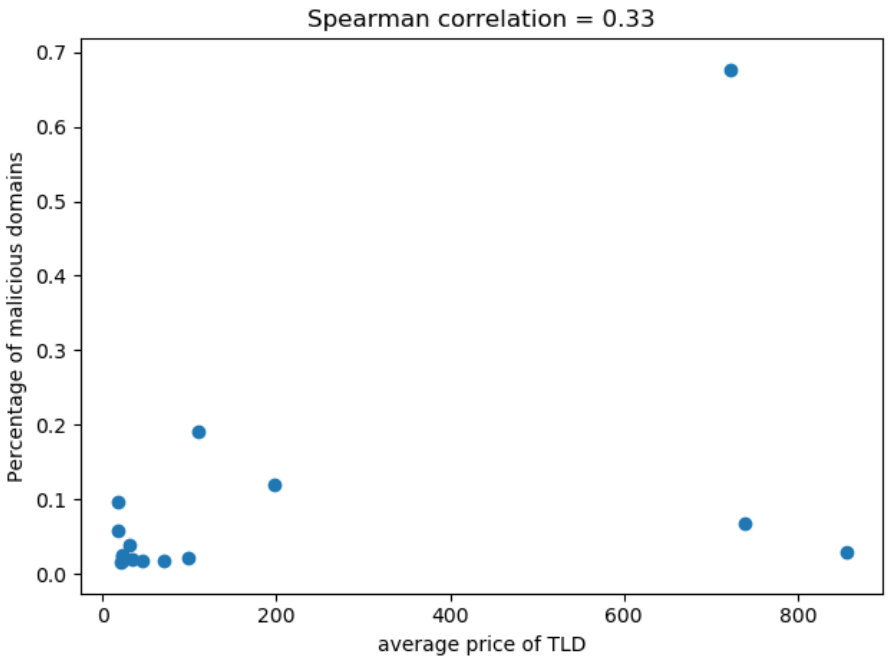

Figure 2: Scatter plot of the percentage of malicious domains per TLD against the average price of a domain for that TLD

4 Conclusion

In this report, we have analyzed the metric of malicious activity per TLD. Three actors surrounding the security issue have been analyzed and the possible countermeasures they could take as well as their motives for taking them have been analyzed. After this, the security performance of the metric was analyzed and we tried to find an explanation of the variance in the metric. We expected

that the variance in this metric would be explained by the price of the top level domain. From the statistical analysis, we found that there is no correlation between the price of a domain and the malicious activity on that domain. We suspect this is because most malicious activity is not performed by the owner of the domain but by a malicious actor that has compromised the website that the domain refers to.

References

[1] *Compare Prices of All Top-Level Domains | TLD List*. [Online; accessed 13. Oct. 2019]. Oct. 2019. URL: `https://tld-list.com`.

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

[3] *GDPR compliance checklist - GDPR.eu*. [Online; accessed 10. Oct. 2019]. Oct. 2019. URL: `https://gdpr.eu/checklist`.

[4] *Spearman's Rank Correlation Coefficient Rs and Probability (p) Value Calculator*. [Online; accessed 13. Oct. 2019]. Oct. 2019. URL: `https://geographyfieldwork.com/SpearmansRankCalculator.html`.

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