WM0824TU Economics of Cyber Security

Assignment Block 4 Deliverables

Group 7

Darli Ciang / 4624211 Samuel Natalius / 4608380

Mathew Vermeer / 4216989 Thomas van Biemen / 4206827

October 2017

Introduction

Ransomware attack is one of the most popular topics of cybersecurity in recent times. In the ransomware attack, the attacker spreads a ransomware, a type of malware that locks the infected PC or blocks user access to specific files, and then requests a ransom payment to the victims in order to "solve" the problem. Ransomware attacks are one of the most popular topics of cybersecurity in recent times. In a ransomware attack, the attacker spreads a type of malware that locks the infected PC or blocks user access to specific files, and then requests a ransom payment to the victims in order to make these files usable again.

In our series of reports, the security issue of malware is assessed from the perspective of domain registrars, entities that are accredited to manage the reservation of domain names. While most of these registrars are legitimate in their goal of providing cheap and good domain services, some have been known to extort users or actively support the distribution of malware such as ransomware (see [1]). In our previous reports on this issue, we discussed the challenge of domain registrars to tackle **the exploitation of legitimate domain registrar service for ransomware hosting** in order to **protect the registrar's credibility**. We have also evaluated existing and proposed security metrics to analyze this challenge, investigated factors that influence the issue and evaluated the strategies that these actors can take to mitigate said risk.

The following report will further reflect on the previously mentioned challenge by analyzing countermeasures of three involved actors and reflecting on the costs and benefits that they bring in the next section. A further section will investigate different externalities and their influence on credibility losses due to the exploitation of legitimate domain registrar service for ransomware hosting.

Actors involved in the security issues

This section will investigate three concrete countermeasures that different actors can use to potentially mitigate the issue of domain registrar services being used for ransomware hosting: The domain registrars, regulatory body and domain owners. For each of these countermeasures, we will elaborate on the effects that the measure has on each of these actors.

Domain registrars

Domain registrars – unless being a hosting provider as well – offer a single service, namely to register domains for a customer. This service is partly why the World Wide Web has managed to achieve the popularity that it enjoys nowadays. This is because it enables users to access websites by a certain name, instead of its difficult-to-remember IP address. The fact that domain registration is the only service provided by these organizations means that there are only a few risk strategies that can be taken. However, the domain registrars could **implement an automatic check on infected domains**, just like websites like ransomware tracker [2] use to search for tracking infections. This automatic check can then be **linked to a system that notifies the domain owner**. If domain owners do not respond

to these notifications, domain registrars can automatically take down the link between a domain name and the domains infected IP address.

Creating this automatic checking and emailing system will probably not be very expensive for most domain registrars. The option to automatically unlink domain names and IP addresses should already be available for most registrars when reservation periods end or bills are not paid. This could benefit the domain registrar because a good ransomware-fighting reputation can bring in more business. Checking which IP addresses can also be done in an inexpensive manner by using third party domain lists such as the ransomware tracker feed that is updated every five minutes. The main costs for a registrar that implements this software will be from taking down false-positively detected domains, as this will mean no income from this business and possibly a bad reputation if too many domain owners have their domain -IP link blocked.

Businesses can also benefit from notifications of infected domains by the registrar as infections are bad for both reputation and website performance. But businesses will probably also make somewhat higher costs by subscribing to a hosting provider and/or domain registrar that has implemented this system. Governments do also benefit from fewer ransomware infections as these can incur high costs to businesses. Costs for government will be minimal to non-existing, only consisting of possible tax losses because of fewer hosted or registered websites in the country.

Because this countermeasure is not expected to be very expensive for any of the actors and might be of benefit to the domain registrar and businesses, there is an incentive to take this measure. This is especially true for the first registrar to successfully implement this measure and a small group of businesses that place high importance on online security. However, because rogue domain registrars are not obliged to implement this tool, the exploitation of registered domains for ransomware hosting is not expected to cease because of this measure..

Government/Regulator

A regulatory body is responsible in establishing a secure cyber environment for its people. Regulatory bodies have the power and right to force hosting providers under their legal coverage to shut down services and hosts that are proved to be malicious. Additionally, the domain registrars can be requested to take down the maliciously used domain name or hand over ownership and control of the domain name to them. This will in turn lead to a safer cyberspace which is very beneficial to governments. It might however be very hard and expensive to investigate all hosting providers that are active within the bodies legislative area and even harder to investigate domain registrars, as basic information such as the number of registered domains per registrar is not publicly available. Because the worldwide web is not restricted to physical legislative areas, it is pretty likely that most domain hosting and registration companies would leave the areas that are within the regulators reach, negatively affecting the government's economy and power over these companies.

Businesses would also suffer economically, both from implementing the mandatory security measures and sanctions if these are not installed correctly. If the measure would lead to fewer ransomware hosting sites, the rule would create lower ransomware costs for businesses (and government). But because hosting and registration companies will probably move to another location without these rules, these benefits will probably not materialized. Strict cyber security regulation on website hosting might be beneficial to domain registrars as domains that are linked to ip addresses within the regulators reach can be considered safe, leading to lower costs for checking these domains and lower risks for credibility hits because of infected domains.

Although this measure has potential to be beneficial for hosting providers, a government does not have an incentive to implement strict regulations in it’s own territory because offending companies can easily evade the rules by moving their business someplace else. This will immediately economically benefit the company while hurting the government's economy. This regulation is therefore only plausible if action is undertaken by (almost) all the world's governments. If the cost of ransomware attacks to governments and companies keep increasing, this might be a future scenario.

Businesses

Businesses buy domain names from registrars and rent hosting space from hosting companies to host their website or other online services. Business costs from malware attacks have been rising sharply in the past years, but in most businesses, employees are unaware of the risk of malware infections. To combat this security blindness, business can implement malware awareness training for their employees. For as little as £8 per employee, this can help protect the business' servers against malware, especially since most of infections rely on social engineering attacks such as spam emails, drive-by downloads and malvertising. Although most of the costs of the infections of ransomware servers are not for the host itself, these awareness training can help companies to protect against a wide range of attacks. This creates a low cost, high available reward situation for businesses to implement these training. The reward will be even higher if companies can get other companies to also invest in malware awareness measures.

The costs of these malware training is entirely paid for by companies, so the implementation of this countermeasure will not hurt domain registrars or the government. And because a safer cyberspace will be beneficial to both these actors, directly in a lower attack risk and indirectly because of a higher credibility, all three of them have an incentive for the countermeasure to be implemented. If the measure is proven to be effective, government and registrars might even help financing the measure. Please refer to our previous report for more information on the effectiveness of the countermeasures.

Table 1 summarizes the above explanation about the countermeasures for every actor together with their costs and benefits and also the incentives the actors have in order to take those countermeasures.

Externalities in the Security Issue

The countermeasure strategies from the actors in previous sections could not be separated from the socio-technical context of its implementation. Those actions provide positive and negative externalities, positive externality is benefit to third parties as a consequence of another's actions and negative externality is harm imposed on third parties as a consequence of another's actions.

Therefore, a whole range of externalities are also at play, such as:

- Automated check and notification for infected domain owner is beneficial to protect the integrity of domain registrar. However, it will give negative externalities of increasing subscription costs for the whole businesses that register in that domain registrar. It also provide positive externalities for government since there are lower infected domain under its jurisdictions.
- Government strategies to sanction/incentivize businesses to comply with security standards would strengthen the securities of whole countries and disincentivize ransomware attacks. The strategy presents positive externalities for domain registrar because the firms will have a better protected system which decrease the probability of infection. The negative externalities happens when these security standards are imposed indiscriminately, firms that are not really prone to the ransomware attacks (e.g. agriculture) are enforced to pay a high sum of security investments that are not really beneficial for them.
- The awareness training strategy from the business (victim) not only increase the firm's security awareness but also provide positive externalities for the general society since it hinder the spreading rate of ransomware. Governments could also comfortably engage the citizen to participate in a nation-wide security campaign when they already develop certain level of security awareness.

Table 1 Summary of countermeasures and distribution of costs and benefits

Actors	Countermeasure	Cost	Benefit	Incentives?
Domain registrars	Automated check the infected domains and notify the domain owner.	• **Domain registrar**: the cost incurred if domain registrars take down the false-positively detected domains, the investment costs for automatic detection and connect with a complete ransomware tracker. • **Business**: higher cost of subscription	• **Domain registrar**: Increasing trust and reputation • **Business**: lower productivity lost due to ransomware infection • **Government**: lower infected website under its jurisdiction	Yes, as long as the domain registrars are not bulletproof registrars. For "legitimate" domain registrars, the reputation on "secure registrars" is important so that the clients are willing to use their services. However, bulletproof registrars may ignore this reputation matter since they have different objectives and type of clients.
Government	Sanction/incentivize businesses to comply with security standards.	• **Government**: Cost of subsidies (incentivize), cost of compliance checks/audits (enforce) • **Business**: Cost of implementing security measures, legal/sanction cost when business can't comply to the security standards.	• **Society**: Creation of new jobs • **Government**: increase country's cybersecurity rating, which also affects country's reputation. • **Businesses**: lower infection rate due to the security strength of the national network (equally strong)	Yes, the ransomware incident already affect the national agency such as NHS in UK and strengthening the country-wide firms is one of the way to disincentive the creator of ransomware. However, the level of security compliance can be differentiated between sectors to lower the burden for smaller firms. For example, the critical and sensitive sectors such as: financial, medical, critical infrastructure, should have a stronger standard than agriculture, manufacture.
Business (victims)	Awareness Training	• **Businesses**: Cost of training, productivity costs (time for training, time to adopt security practices)	• **Businesses**: More secure environment, lowering the probability of ransomware attack ("network effect")	Depends on how the high-level management put the priority on the employee cyber activities. If the ransomware attack affects the company-wide network it will become a hazardous incidents. Therefore, the incentives on conducting awareness training is higher than the training cost and productivity lost for the training.

Factors explaining the variance in metrics

This section will look further a specific metric which is identified in the previous assignment, and try to analyse factors that influence the metric.

The Metric and factors

The metric that we want to look into is the ratio between the number of online and total ransomware-related hosts per country. The metric basically provides us with the insights about the effectiveness of a country in removing or

taking down the ransomware hosts. We assume that the countries can be represented by the actors whose security performance is visible in this metric.

We argued that there are several factors which can affect the metric. They are total population of a country, number of individuals in a country using internet and number of secure servers (servers using encryption technology in Internet transactions) in a country. Open Data from World Bank[1] corresponds to these factors are collected to support the analysis. From World Bank, we acquire data about total number of population (in number), individuals using the internet (in % of population) and secure internet servers (in number). In the figures, this data is called **SP.POP.TOTL**, **IT.NET.USER.ZS**, and **IT.NET.SECR** respectively. Furthermore, **freq.x** represents the total number of detected ransomware hosts per country, while **freq.y** represents the total number of ransomware hosts per country that are still online. Finally, **f** is the ratio between **freq.y** and **freq.x**.

The statistical analysis

First of all, we create the correlation matrix to see whether there are correlations between the metric and factor variables in the dataset. The correlation matrix can be seen in figure 1. Respectively, table 2 shows the p-value of the correlation matrix, which implies the statistical significance of the correlations.

From the correlation matrix we can see that there are weak negative correlation between variable **f** and the factor total number of population, and weak positive correlation between variable **f** and number of individuals using the internet. Interestingly, we find almost no correlation between variable **f** and the number of secure internet servers. The number of secure internet servers per country could be used as an representation of a country's security awareness. The lack of correlation corresponding to this variable may indicate that a country's security awareness will not have any effect on its effectiveness at removing ransomware hosts. However, since the p-values for those correlations are high (>0.1), the significance of this finding is doubted.

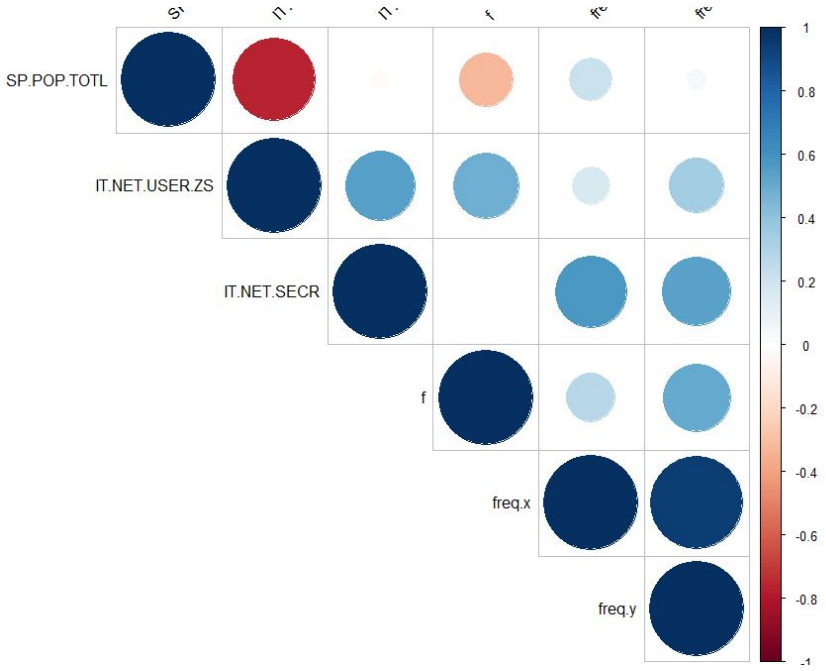

Figure 1 Summary of countermeasures and distribution of costs and benefits

[1] https://data.worldbank.org/

Table 2 Summary of countermeasures and distribution of costs and benefits

	SP.POP.TOTL	IT.NET.USER.ZS	IT.NET.SECR	f	freq.x	freq.y
SP.POP.TOTL	NA	**0.0093167**	0.942818	0.3600258	**5.54E-01**	**9.04E-01**
	IT.NET.USER.ZS	NA	0.1003136	0.1601705	**6.45E-01**	**3.36E-01**
		IT.NET.SECR	NA	0.9866123	**8.07E-02**	**1.12E-01**
			f	NA	**4.43E-01**	**1.33E-01**
				freq.x	NA	**2.66E-05**
					freq.y	NA

Beside the correlation matrix, we also performed the regression analysis of the dataset against the **f** variable. The result of the regression analysis is as shown below.

```
Coefficients:
                      Estimate     Std. Error   t value   Pr(>|t|)
(Intercept)           -3.787e-01   2.414e-01    -1.569    0.168
merged$IT.NET.USER.ZS 7.074e-03    3.090e-03    2.289     0.062 .
merged$SP.POP.TOTL    1.202e-09    7.640e-10    1.574     0.167
merged$IT.NET.SECR    -2.048e-06   1.078e-06    -1.900    0.106
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 0.07597 on 6 degrees of freedom
Multiple R-squared:  0.5225, Adjusted R-squared:  0.2838
F-statistic: 2.189 on 3 and 6 DF,  p-value: 0.1903
```

It can be seen from the result that the coefficient of the factor **IT.NET.USER.ZS** (percentage of the population that uses the internet) has a p-value under 0.1 which means it has confidence rate between 90-95% that the null hypothesis for this factor can be rejected. In other words, **IT.NET.USER.ZS** can be considered as a factor that influence the metric **f** (ratio between online and total ransomware-related hosts per country).

Conclusion

The security issues of "**the exploitation of legitimate domain registrar service for ransomware hosting"** can be addressed by several types of countermeasures. Each of this countermeasure is defined as an action by a certain actor which acts as part of a broader socio-technical context. Therefore, every actor and its action (countermeasure) presents externalities toward other actors in the system. These externalities affect the effectiveness of security measures, high positive externalities could discourage the actors to implement countermeasures since they do not gain direct benefits from the investment. On the other hand, high negative externalities discourage the actors to take action since they do not get the direct consequences of their negligence on implementing security measures.

From the regression analysis result, it can be seen that the factor ***individuals using the internet*** influences the security performance of a country with the significance between 90-95% (fairly high). This finding can be explained as below: higher fraction of individuals using the internet in a country, increase the attractiveness of the country for

the attackers and also the higher chance that the attackers come from that country. These may result in more ransomware hosts evident under the country's IP address. Therefore, it presents a bigger challenge for domain registrar and hosting provider to take down the infected hosts due to the sheer number of websites hosted in the country.

However, some limitations in the analysis need to be considered while interpreting the result. The fact that only 10 countries, which represents 10 data points, are considered in the analysis affects the accuracy of the regression model. This is reflected in the R-squared value of the model, which is not high. Having more data into the analysis may help to create better regression model and also better interpretation of the factors influencing the metric.

Additional Note

This report and R files for dataset analysis can also be found on GitHub:

https://github.com/mathewvermeer/econ-cs/tree/master/Block_4

References

[1] D. Bradbury, "Testing the defences of bulletproof hosting companies," *Network Security*, vol. 2014, no. 6, pp. 8–12, 2014.

[2] "Ransomware tracker CSV feed." [Online]. Available: https://ransomwaretracker.abuse.ch/feeds/csv/