WM0824TU Economics of Cyber Security

Assignment Block 3 Deliverables

Group 7

Darli Ciang / 4624211
Samuel Natalius / 4608380
Mathew Vermeer / 4216989
Thomas van Biemen / 4206827

October 2017

Introduction: Revisiting Previous Assignment

Problem Owner

In this report, the ransomware security issues are being assessed from the perspective of **domain registrars**. The ransomware tracker website provides information to the public regarding the existence of various ransomware servers (e.g. Command & Control servers, Distribution servers, and Payment servers) on the internet. That information precisely tracks the location of the hosted servers through its IP address and domain registrars, and the status of the servers (online/offline). The domain registrars hold a pivotal position on countering the spreading of ransomware since they can mitigate the ransomware infection by taking down the malicious servers hosted in their domain[1]. Therefore, the credibility of domain registrars in front of public opinion is deeply related to its ability to prevent and mitigate the exploitation of its registers by malicious hosts thus the security issue in this report is stated as "**the exploitation of legitimate domain registrar service for ransomware hosting**".

The domain registrars can not take every malicious domain hosted in its registrar without any consideration since the servers do not only consist of servers that have been explicitly registered by the ransomware owner but also legitimate servers that are being compromised and used as the ransomware hosts [2]. In that sense, the domain registrars capabilities to swiftly and precisely differentiate between the legitimate and illegitimate hosts are important. If the domain registrars fail to develop the abilities and took down every malicious host indiscriminately, it will result in the disruption of service for the legitimate website owner.

On the other hand, the regulatory body sees the unresponsiveness of domain registrars as the participation in unlawful activities of ransomware. Several domain registrars are specially created as "bulletproof domain registrar", which are very lenient on the utilisation of its service by the customer and rarely comply with the takedown request on the domain it hosts[3]. In this case, the law enforcement could take down the domain registrar by force, for example, the Russian-based PROXIEZ-NET bulletproof hosting is forcibly taken down from the internet routing tables resulting in the inability of its downstream nodes to communicate [4].

Relevant differences in security performance

As explained in the previous section, our report focusses on **the exploitation of legitimate domain registrar service for ransomware hosting** and the credibility of domain registrars in face of this issue. Our last assignment report has already been written to investigate metrics that could help to measure this exploitation and the difference between domain registrars in their ransomware host removal-efficiency and thus credibility. Although serious limitations still exist, these metrics do point out relevant differences in the security performance of registrars:

1. The threat-removal effectiveness of registrars shows the percentage of known threats that are offline. Although a registrar is not always the party that shuts down threats, this metric does indicate a great difference among registrars and their credibility in ransomware-removal.

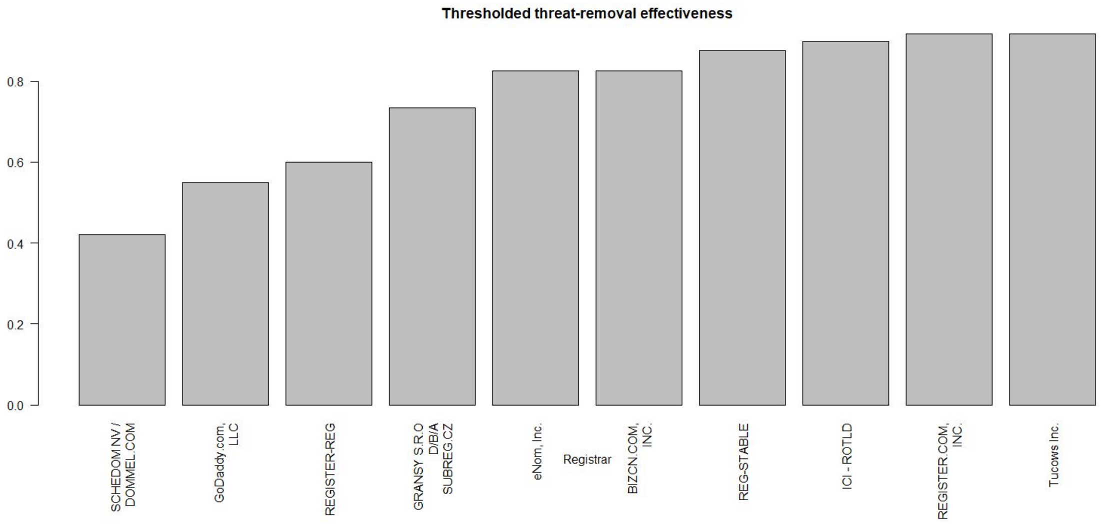


Figure 1: Thresholded (minimum of 10 cases) top 10 registrars with worst threat-removal effectiveness

2. The fraction of hosted threats that is still online per country does not directly measure this registrar threat removal credibility metric, but it does provide registrars with information on hosting locations that appear to be tougher on malware threats.

3. Another useful metric for registrars, or for users to rank the registrar's security performance, is captured in figure 3. The prefered ransomware per domain registrar shows for example that while the Locky ransomware is the most appeared malware for most registrars, Eranet International Limited is the prefered registrar for registering Cerber ransomware. This does not immediately mean that Eranet is deliberately amplifying the Cerber threat however, as it can also point to other differences among registrars such as the location of their business.

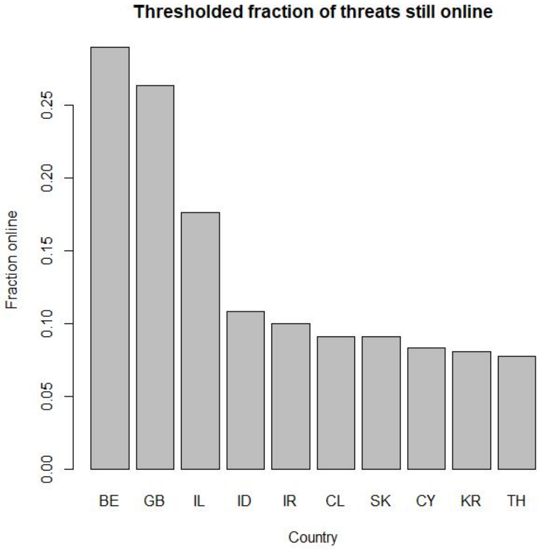
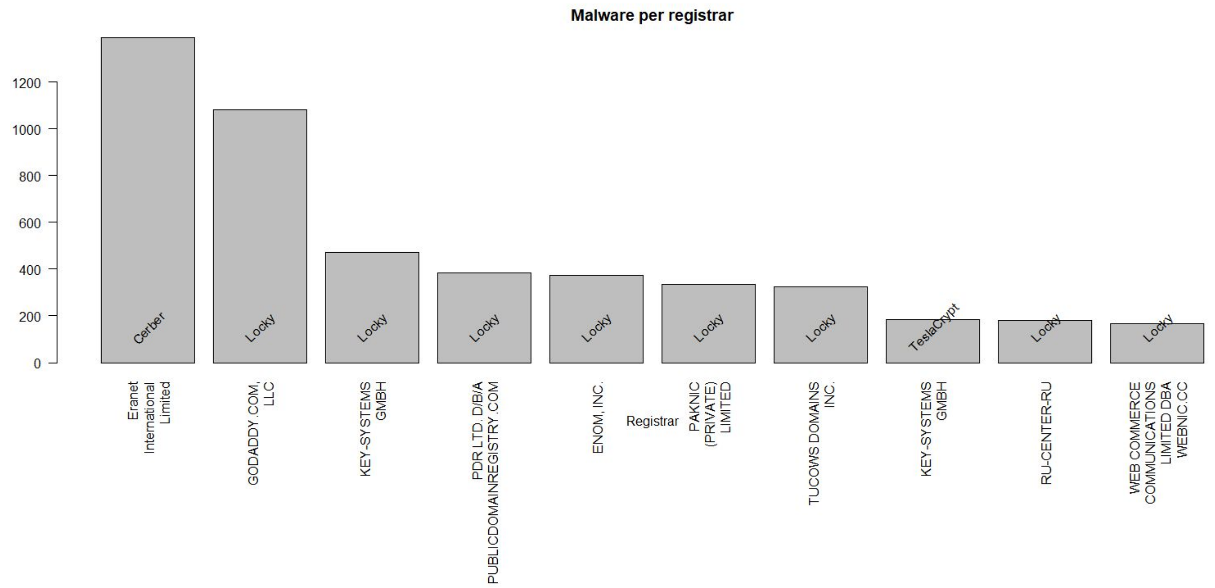


Figure 2 : Thresholded top 10 countries with the highest fraction of online threats

Aside from the specific limitations that each of these metrics have, it is also important to note the absence of normalization. Ideally, the metrics would be controlled for the size of each registrar. This size is not publicly known for each registrar though, making normalization impossible. But even with these limitations, the security metrics that are proposed in our previous report do help us to investigate the exploitation of legitimate domain registrar service for ransomware hosting and which registrars have the higher credibility in malware threat removal.



. *Figure 3: Domain registrars prefered for a particular ransomware*

Risk strategies the problem owner can follow

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. These are the following:

- Automatically check the presence of its domain registrar in the ransomware tracker and notify the legitimate website owner when their website is being used as ransomware hosts.
- Develop clear Terms and Conditions (T&C) and Standard Operating Procedure (SOP) that allows them to promptly take down the proven malicious hosts.
- Openly share information on the % of threats that are still online, possibly in collaboration with other domain registrars.

Taking these measures does not mean that ransomware threats are completely removed from the internet, however. The servers that are actually hosting the threat remain online. It is only after the hosting provider takes the server offline that the threat is finally removed. Nevertheless, since it are the domain names that are used by cybercriminals and their ransomware entities to contact their servers, suspending the registration of a domain name prevents any communication to the corresponding server that uses its domain name, thereby improving the registrar threat removal credibility for the public.

Other Actors

The problem owner is not the only actor who influences the security issue. There are several actors playing in the Ransomware case who, either directly or indirectly, influence the security issue. Five important actors and their background in this issue are described below:

- Attackers

Actors who make use of ransomware to attack people and organizations and benefit (in terms of ransoms) from them. These play such important roles in influencing the security issue since they are responsible for the infection of systems with the ransomware and it is these infections that can taint the threat removal credibility of domain registrars.

- (Legitimate) domain owners

(Legitimate) domain owners are individuals or organizations that make use of a domain registrar's service to do their business. They are consumers of information technology products or services and in terms of information security they are dependent on the available environment. They become one of the victims of an attack when an attacker compromises their servers. Depending on their awareness, they can put some measures in order to protect themselves from getting attacked or manage the risk of the attack, which could influence the security issue.

- Hosting providers

Hosting providers rent out server space for their users. When a legitimate user's server is attacked, this server space is where the ransomware is actually located. This means that these hosting providers have the ability to completely remove the compromised server from the internet by simply wiping or disabling it. Big hosting providers often have security measures in place to detect, protect from or counteract attacks.

- Businesses/end users

While acquiring malicious servers is one of an attacker's objectives, ultimately, the real goal of ransomware users is to successfully infect the systems of businesses, or end users in general, with their ransomware. They have the ability to decrease the success chance by using products such as antivirus. Additionally, as is the case with legitimate domain owners, increasing their awareness of the existence of ransomware and methods of spreading directly leads to a significant decrease in successful ransomware attacks.

- Regulatory body

A Regulatory body is responsible in establishing a secure cyber environment for its people. Regulatory bodies have the power and right to force domain registrars under their legal coverage to shut down services and hosts that proved to be malicious and furthermore take down the domain registrars which show no compliance to security standards. They can also take a non-technical approach to achieve their objective, for example, by creating social awareness about the ransomware.

- The security industry (e.g. Antivirus industry)

The security industry encompasses all enterprises that create products or services to defend against cyber attacks or otherwise increase cyber security. These products or services can be used for other actors to mitigate their cyber risk, such as antivirus software to protect servers from attacks or tools to detect infected domains.

Risk Strategies of Other Actors

This section will elaborate potential risk strategies done by the previously mentioned other actors except ones by attackers, since attackers have a completely opposite motivation with respect to the security issue.

- Legitimate domain owners

It is important to be aware that not every domain owner is a legitimate one. Hence, there will be different objectives and also strategies between non-legitimate and legitimate domain users. This part will focus more on the legitimate one. A strategy that legitimate domain users can do to help tackling the security issue is to **install proven antivirus or other security defense tools** for their server(s). These tools are expected to prevent or make it harder for ransomware to successfully infect systems they protect. Other tools can be used to detect infected domains that are owned by legitimate users. Additionally, the users can invest in some sort of security awareness training. This training could help legitimate users remain alert and not let their guard down when receiving emails with suspicious attachments.

- Hosting providers

Because most hosting providers rent out their own server space to domain users, hosting providers may directly take theoretically directly tackle the problem by clearing their servers of infections. Providers can also **provide protection services against ransomware** for the legitimate users of their services. It can be done, for example, by partnering with antivirus company to provide overall ransomware protection to all hosts under them. They can also **develop clear Terms and Conditions (T&C) and Standard Operating Procedure (SOP)** that allows them to promptly take down & clean up hosts that are proven to be malicious.

- Businesses/end users

The first thing to do for businesses and end users is **invest in some sort of security awareness training**. This will be done to counteract the methods that are used by attackers to spread their ransomware, thus decreasing the probability of a successful infection. Furthermore, businesses and end users can **invest in a high-quality antivirus** product that is able to detect and remove ransomware software before they cause any damage.

- Regulatory body

Regulatory body can address the issue in indirect way. One that they can do is to **create awareness campaign** to every cyber actor about how to avoid being a victim of ransomware attacks. In a more active way, regulatory body can **establish ransomware detection & response team.** Regulatory bodies can also make the use of mitigation strategies, software and or services mandatory or cheaper for other players through regulation.

- The security industry

The security industry can contribute by **investing more resources in research** about ransomware or by designing specific software or tools to mitigate risks or losses. This could potentially increase the quality of antivirus products, for instance, if they are able to identify ransomware better and prevent it from executing.

Evaluation of risk strategies

This section will start with explaining the concept & theory used in the evaluation of a risk strategy for a regulatory body type actor. Next, the evaluation methodology will be described and in the end the analysis and calculation will be done in accordance with the methodology.

Scope

This paper will evaluate the risk strategy from the perspective of businesses in the United States of America.. The risk strategy to be evaluated is: **investing in phishing awareness training to decrease the probability of Cerber infection**. A specific scope taken for this evaluation is Cerber distribution servers hosted in the US.

In order to make the evaluation possible, there are some limitations and assumptions which are described below.

- The type of Cerber hosts that is taken into consideration are distribution servers.
- Only Cerber hosts that have IP addresses in the US are included.

Methodology

The return of Security Investment (RoSI) will be used to evaluate the chosen risk strategy. RoSI measures the relation between benefit and cost of a security investment and is often used to find the strategy that provides the highest relative value [5]. RoSI can be calculated as follows:

$$RoSI = \frac{benefit - cost}{cost} = \frac{ALE_0 - ALE_1 - c}{c}$$

With ALE_0 the loss distribution without security investment, ALE_1 the loss distribution with security investment and c the cost of security investment. The calculation of $ALE_0 - ALE_1$ indicates the shift of probability mass between 2 loss distributions that implies the benefits arise from prevented loss due to security investment.

It is important to note in advance that it is impossible to come up with the accurate result of the calculation since the evaluation deals with future occurrences that is difficult to predict. However, the evaluation can still be useful to give a rough insight about the value an investment can provide.

Evaluation will be done by firstly calculating the cost of investment. Secondly, the annual loss estimation without security investment (ALE_0) will be estimated by assessing dataset and finding information from external resources. Thirdly, the annual loss estimation with security investment (ALE_S) will be estimated. ALE_S is a hypothetical measure and will be estimated by a reasonable prediction backed up by external data and information. Finally, after data about the loss estimation and the cost are gathered, RoSI of the risk strategy can be calculated.

Results

Investment costs

Phishing is the primary method of Cerber distribution. This means that the appropriate security training investment is phishing awareness training. The UK-based company *IT Governance Ltd* offers such awareness training for £8, or $10.47 [6].

According to the United States Census Bureau, in the year 2015 there were 124,085,947 employees, and 7,663,938 establishments in the country. This means that the average business in the USA employs 16 people [7]. This would bring the average total security investment to $176 per business, assuming every employee is susceptible to phishing attacks.

Taking into account the fact that Cerber is a newcomer to the ransomware scene, the sheer amount of different ransomware types already out there, and its popularity compared to the different ransomware types, we estimate Cerber to be responsible for 1% of ransomware currently in circulation. This might even be too generous, as Kaspersky did not rank it in its top-10 list of most widespread ransomware [8]. For the sake of simplicity, though, this figure will remain at 1%.

Since Cerber is not the only type of ransomware that is distributed via phishing email, this security investment also addresses all the other types of ransomware that use this method. This means that the probability of different ransomware attacks (e.g. Locky, CyberLocker) to be successful decreases as well. We therefore set the cost of investment per business to 1% of $176, namely $1.76, corresponding to the estimated 1% market share that belongs to Cerber. The total cost of investment for mitigating the Cerber ransomware threat is then $13.5 million.

ALE_0

To obtain ALE_0 we estimated first the frequency of incidents and the unitary impact of the incident. Firstly, the frequency of occurrence is calculated per month, since the size of the dataset is not large enough for calculating the annual frequency.

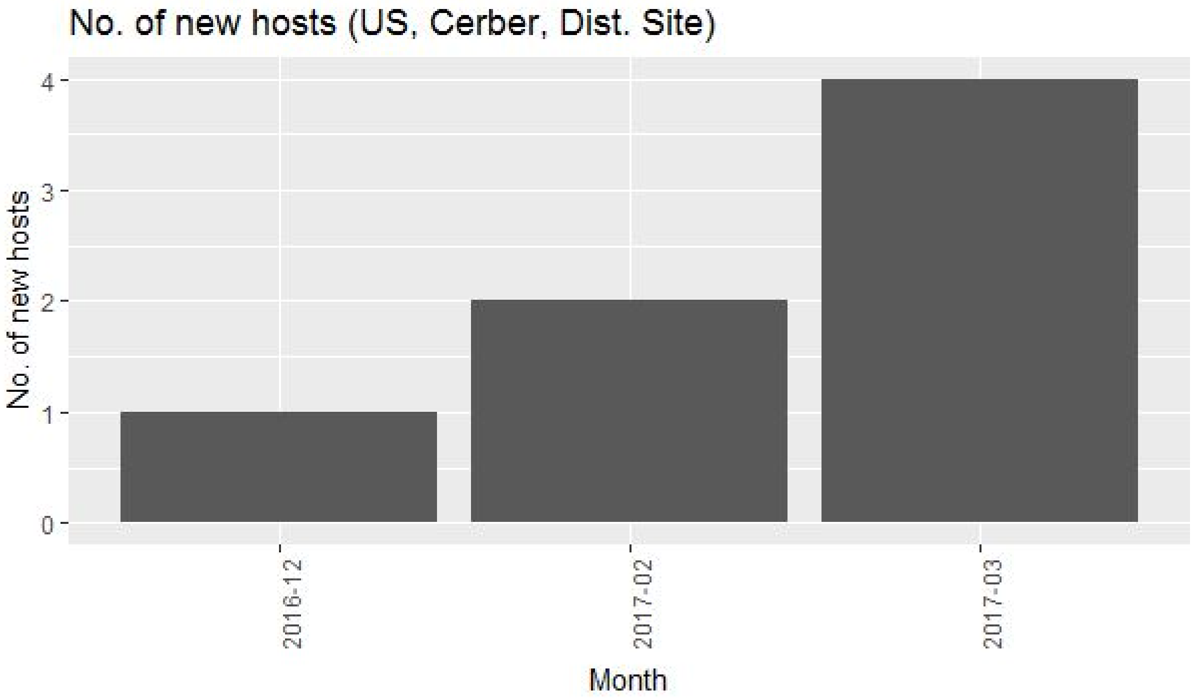


Figure 4: Number of new Cerber Distribution Site hosts residing under US IP Address

From the dataset, as shown in figure 4, we we determine that there are between 1 and 4 new infected hosts tracked per month. However, these hosts do not remain active forever. Assuming that the hosts will be taken down in the near future, then the balance between the emergence of new hosts and the closure of the old active hosts will imply that the number of active hosts per month is the same as the number of new infected hosts tracked per month, which is 1-4 hosts per month. We can therefore assume that the total amount of infected hosts will remain in the range of 1 to 4 hosts throughout the year.

According to a july 2016 report by CheckPoint [9], the Cerber ransomware profit is approximately $195,000 with 14% of the ransom payments come from the United States (US) based victims (see figure 5), meaning a $327,600 profit in the US in 2016. This profit is perceived as the loss to the general public from the government's point of view. In addition to the the payment made, the impact of the Cerber ransomware also includes the productivity loss caused by the encryption of a business's valuable files and data. We estimate this value in the following way: we divide Cerber's total profit in the US in 2016 by the average demanded ransom in 2016, which is $1,000, yielding 328 companies affected by Cerber. Businesses face at least two days of downtime due to ransomware, and every hour of lost productivity is estimated at $8,581[10], bringing the total cost for lost productivity to $135,099,264.

Adding the cost of lost productivity to the ransom profits, the total loss becomes $135,426,864. We will round this number to $135 million. The actual unitary impact per Cerber distribution server then ranges between $33.75 million and $135 million.

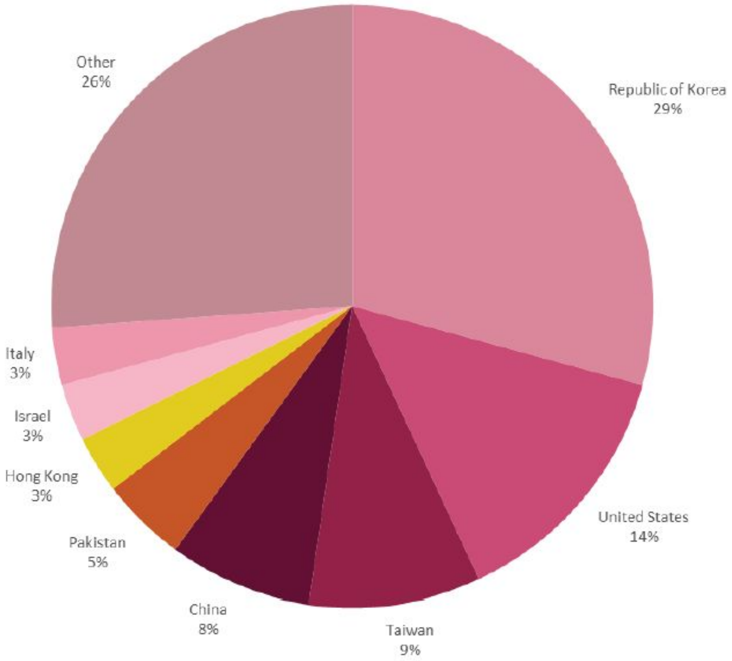


Figure 5: Ransom Payments by Country [9]

Based on the above data, ALE_0 can be estimated as:

$$ALE_0 = No.\ of\ active\ hosts\ per\ month \times Impact\ of\ each\ host$$

$$ALE_0 = \$33.75 \text{ million to } \$135 \text{ million per year}$$

Prediction of ALE_S

Awareness training is said to reduce workers clicking on phishing attacks (which can be the start of ransomware attacks) from 15.9% to 1.2% [11], which decreases the chance of successful infection by 92.5%. Although it will not change the number of active hosts, it will greatly reduce the frequency of successful attacks.

We assume that the phishing awareness training is applied nationally. The probability of a successful attack is reduced, and therefore the impact of a host decreases accordingly. We calculate ALE_S to be the following:

$$ALE_S = \$2.5 \text{ million to } \$10 \text{ million per year}$$

Calculating RoSI

Since we have already calculated both ALE_0 and ALE_S, and the cost of the security investment is known as well, RoSI calculation is rather straightforward. Since the amount of Cerber distribution servers ranges from one to four servers, two RoSI figures will be calculated: one for the case of a single server, and another for the case of four different distribution servers. The RoSIs are calculated for the period of a year.

Below is the calculation for the case of a single Cerber distribution server:

$$RoSI_1 = \frac{ALE_0 - ALE_S - cost}{cost} = \frac{\$135 \text{ million} - \$10 \text{ million} - \$13.5 \text{ million}}{\$13.5 \text{ million}}$$

$$RoSI_1 = 826\%$$

And below is the calculation for four different Cerber distribution servers:

$$RoSI_2 = \frac{ALE_0 - ALE_S - cost}{cost} = \frac{\$33.75 \text{ million} - \$2.5 \text{ million} - \$13.5 \text{ million}}{\$13.5 \text{ million}}$$

$$RoSI_2 = 131\%$$

Conclusion

In this report, we first approach the problem of “**the exploitation of legitimate domain registrar service for ransomware hosting**” from the perspective of domain name registrars. These exploited domains can have an impact on the registrar's business through the credibility of the registrar to prevent and mitigate ransomware hosting. Because this problem was also researched in our previous report, we used the first section to look back at our previous work and review metrics that expose relevant differences in security performances of registrars, although serious limitations on the calculation of specific metrics and impossibility of normalization of these security metrics.

The report then continues by reviewing risk strategies that can be used to mitigate the central security issues, as well as other involved actors and the strategies that are available to them. One of these strategies, namely **investing in phishing awareness training to decrease the probability of Cerber infection** from the US businesses' perspective. Using ROSI calculations, we conclude that this security investment does add to the return on security, although the return can be different depending on the cost spent for the strategy and the estimation of benefits that can be acquired.

The benefit in cyber security field is a matter of probability which is driven by several uncontrollable factors, for example the chance of getting the attacks, the chance of the attacks to be successful and the magnitude of loss which the attacks give as well as the decrease of successful attacks because of awareness training. Hence, it is important to emphasizes that the results of this report should not be used as quantitative certainty, but rather as qualitative suggestion and background to a big problem that should be addressed by a regulatory body.

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_3

References

[1] B. Stone-Gross *et al.*, “Your Botnet is My Botnet: Analysis of a Botnet Takeover,” in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, Chicago, Illinois, USA, 2009, pp. 635–647.

[2] M. Vasek and T. Moore, “Do Malware Reports Expedite Cleanup? An Experimental Study,” in *CSET*, 2012.

[3] D. Bradbury, “Testing the defences of bulletproof hosting companies,” *Network Security*, vol. 2014,

no. 6, pp. 8–12, Jun. 2014.

[4] "'Bulletproof' ISP for crimeware gangs knocked offline." [Online]. Available: https://www.theregister.co.uk/2010/05/14/zeus_friendly_proxiez_mia/. [Accessed: 22-Sep-2017].

[5] "Return On Security Investment (ROSI) A Practical Quantitative Model," in *Proceedings of the 3rd International Workshop on Security in Information Systems*, 2005.

[6] "Phishing Staff Awareness Course," *IT Governance Ltd*. [Online]. Available: https://www.itgovernance.co.uk/shop/product/phishing-staff-awareness-course. [Accessed: 08-Oct-2017].

[7] UnitedStatesCensusBureau, "2015 SUSB Annual Data Tables by Establishment Industry," 2017. [Online]. Available: https://www2.census.gov/programs-surveys/susb/tables/2015/us_state_totals_2015.xlsx. [Accessed: 08-Oct-2017].

[8] Maria Garnaeva, Fedor Sinitsyn, Yury Namestnikov, Denis Makrushin, Alexander Liskin, "KASPERSKY SECURITY BULLETIN: OVERALL STATISTICS FOR 2016," Dec-2016. [Online]. Available: https://kasperskycontenthub.com/securelist/files/2016/12/Kaspersky_Security_Bulletin_2016_Statistics_ENG.pdf. [Accessed: 08-Oct-2017].

[9] CheckPoint, "CerberRing: An In-Depth Expose on Cerber Ransomware-as-a-Service," Check Point, AUGUST 15, 2016.

[10] A. Chandler, "How Ransomware Became a Billion-Dollar Nightmare for Businesses," *The Atlantic*. [Online]. Available: https://www.theatlantic.com/business/archive/2016/09/ransomware-us/498602/. [Accessed: 08-Oct-2017].

[11] W. Staff, "4 Ways to Protect Against the Very Real Threat of Ransomware," *WIRED*, 13-May-2016. [Online]. Available: https://www.wired.com/2016/05/4-ways-protect-ransomware-youre-target/. [Accessed: 08-Oct-2017].