WM0824TU Economics of Cyber Security

Assignment Block 3 Deliverables (Draft)

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 could 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.

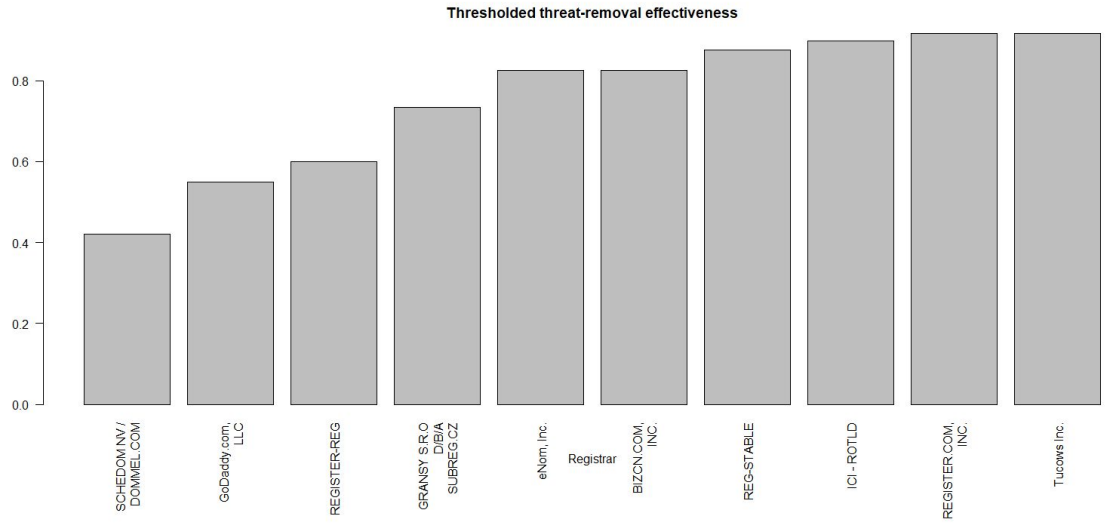


Figure 1: Thresholded (minimum of 10 cases) top 10 registrars with worst threat-removal effectiveness

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.

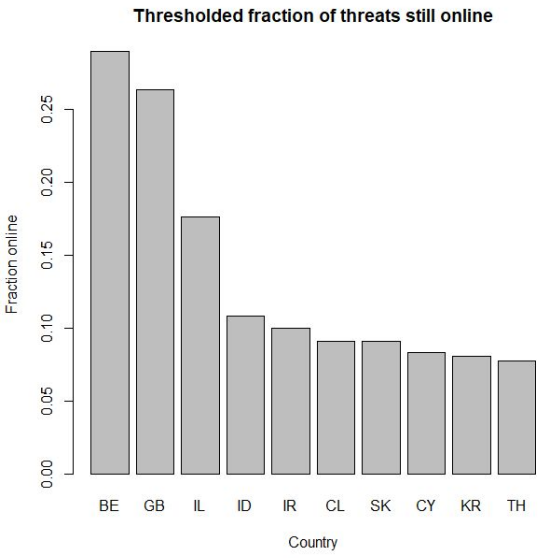
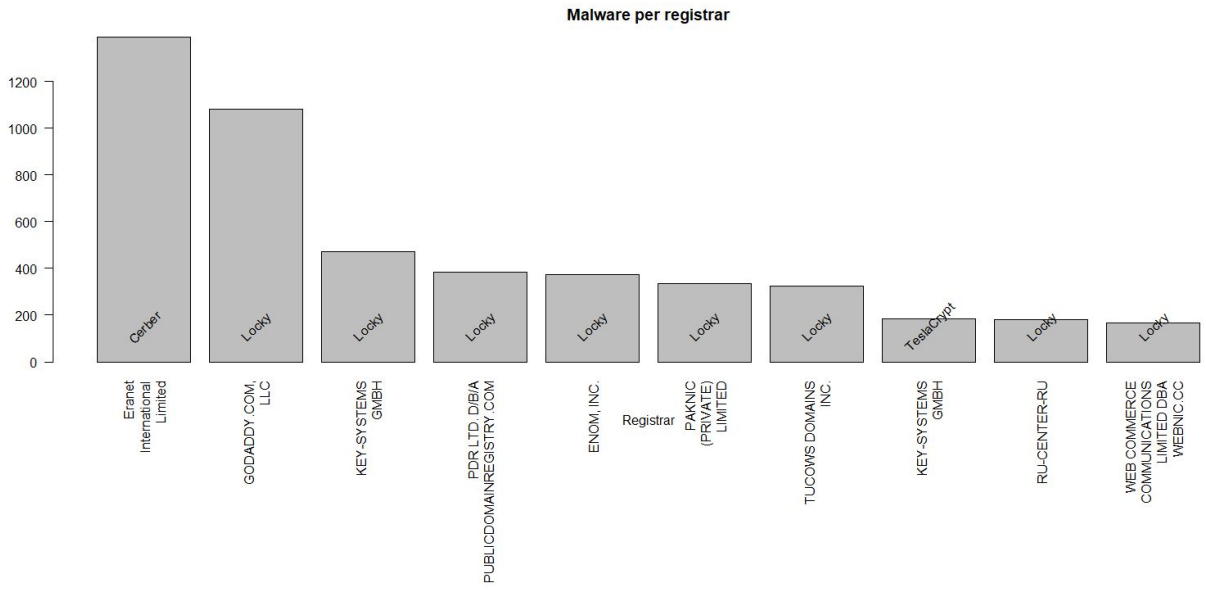


Figure 2 : Thresholded top 10 countries with the highest fraction of online threats

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.

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.

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, can influence the security issue. These actors are explained below.

- Attackers

Actors who make use of ransomware to attack people and organizations and benefit (in terms of ransoms) from them. They play such important roles in influencing the security issue since they are responsible for the infection of systems with the ransomware..

- (Legitimate) domain users

(Legitimate) domain users can be 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 victims of the attack when the attackers compromise 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 their 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.

- Regulatory body

Regulatory body is responsible in establishing a secure cyber environment for its people. Regulatory body has a 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)

Antivirus industry can partnered with domain users in establishing more protections for their servers.

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 users

It is important to be aware that not every domain user 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). The expectation is the tools can prevent or make it harder for ransomware to successfully infect systems they protect. Additionally, the users can invest in some sort of security awareness training. This training could help these users remain on alert and not let their guard down when receiving emails with suspicious attachments.

- Hosting providers

Hosting providers may **provide protection services against ransomware** for the 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 proved to be malicious.

- 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 raid team.**

- The security industry

The security industry can contribute by **investing more resources in research** about ransomware.

Evaluation of risk strategies

This section will start with explaining the concept & theory used in the evaluation. Next, the evaluation methodology will be described and in the end the analysis and calculation will be done in accordance with the methodology.

Concept & Theory

Return of Security Investment (RoSI) is usually calculated in order to evaluate a risk strategy. RoSI measures the relation between benefit and cost of a security investment and is often used to find out the strategy that provides the most value [5]. RoSI can be calculated as below.

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

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.

Methodology

In this paper we will evaluate the risk strategy from a hosting provider's perspective, which is partnering with security service companies in order to provide ransomware protection service to its users. 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 loss distribution without security investment will be estimated by assessing dataset and finding information from external resources. The loss distribution with security investment is a hypothetical measure and will be estimated by a reasonable prediction backed up by external data and information. When data about the loss distributions and the cost are gathered, RoSI of the risk strategy can be calculated.

The Evaluation

The evaluation will be provided in the final version

Conclusion

The conclusion will be provided in the final version

Additional Note

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

The link will be provided in the final version

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.