WM0824TU Economics of Cyber Security

Assignment Block 2 Deliverables

Group 7

Darli Ciang / 4624211

Samuel Natalius / 4608380

Mathew Vermeer / 4216989

Thomas van Biemen / 4206827

September 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 [1]. Just a few months ago we saw how a ransomware *WannaCry* spread quickly to thousands of computers worldwide and caused a huge loss for companies worldwide who became the victims [2]. Many attempts are being performed in order to inhibit the spread of the ransomware or to prevent it to successfully attack any victim. Unfortunately, until recently ransomware attacks are still happening on a daily basis and still have a high rate of success, and it still becomes a destructive yet profitable cyber attack [3]. It is important to look at this problem comprehensively in order to get a complete understanding of the ransomware ecosystem. This assignment tries to give a new perspective of the ransomware issue based on a dataset provided in the context of the Economics of Cyber Security assignment and in the end, proposes several security metrics extracted from the dataset that can hopefully complement other existing security metrics out there.

Methodology

For the assignment, our group uses the *Ransomware Tracker* dataset taken from *Ransomware Tracker* site [4]. The dataset gives information about "the status of domain names, IP addresses and URLs that are associated with Ransomware, such as Botnet C&C servers, distribution sites and payment sites" [4]. The tracker has been collecting such data since 2015-03-02 01:18:48 and the data are still being updated up to this date. The website provides CSV feed which can be downloaded and used for performing the analysis. The CSV file until recently contains over 13000 malware occurrences [5]. The analysis is performed through the flow as illustrated in figure 1:

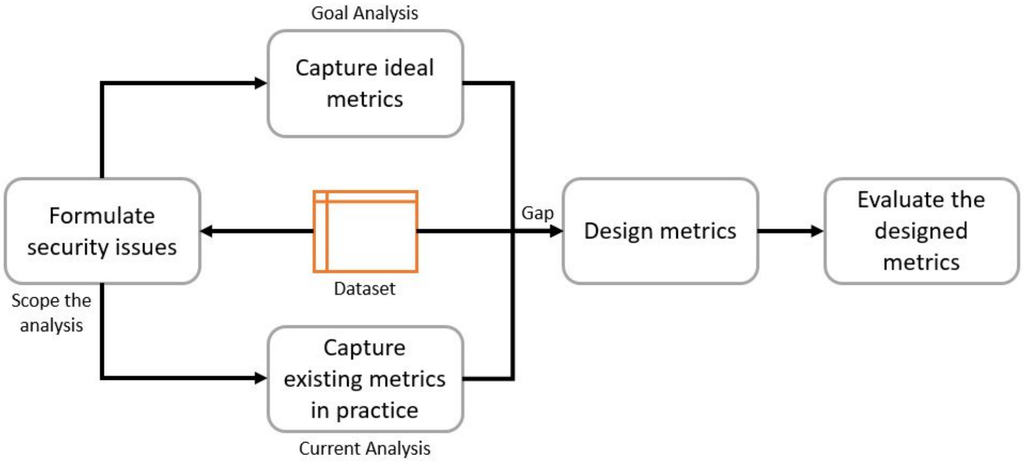

Figure 1: Flow of the analysis

We performed a thorough analysis on the dataset in order to formulate a security issue that can be addressed from it. In order to capture ideal security metrics, we used a framework proposed by Böhme [6] together with the provided video lectures of Economic of Cyber Security course on EdX platform [7]. Furthermore, research through external resources e.g. journal papers, company whitepapers, and archived forums/presentations were conducted to capture the metrics existed in practice. All of these provided some ideas for designing metrics out of the dataset in our case. The designed metrics were then evaluated using the analysis tools, which is R, a language and environment for statistical computing and graphics [8].

Security Metrics, Explained

Security metrics are metrics used to define inputs, outputs and parameters of a security investment model [6]. Based on a security breach probability function defined and proposed by Gordon and Loeb [9], there are three categories of security metrics that can be determined: the cost of security, the security level, and the benefits of security. These categories are interrelated to each other, since the security level often aligns with the cost of security and stochastically determines the benefits of security. That means the security levels serve as intermediate factors which, in practice, are often better observable than directly mapping the cost of security to the benefits of security, as they are typically more abstract. This report will explain further metrics for the security levels in the next section.

Metrics for Measuring Security Level

Security metrics to measure the security level ideally includes all 4 types of metrics below [7]:

1. **Controls:** The measure put to mitigate risks. It can be physical, organizational, procedural and technical. An example for ransomware attack case is the number of backups performed per a specific period of time.
2. **Vulnerabilities:** Weaknesses in the controls. These metrics can be from outcome of an audit, vulnerability scanners or penetration testing/red teaming. An example for ransomware attack is the number of detected bugs in the environment system potential to be exploited.
3. **Incidents:** Events where security is compromised in some form. The metrics can be from detections and alarm from automated event monitoring systems. An example for ransomware attack case is the number of incidents detected [10].
4. **(Prevented) Losses:** Losses that occur/can be prevented when incidents happen/prevented. An example for ransomware attack case is the number of users/businesses paid the ransom, the amount of money paid for the ransom and the number of users lost their data due to ransomware [11].

In current practice, there are several companies and organizations establish their own security level metrics. Some of them are provided as below [7]:

1. Cloud Security Alliance (CSA)

   CSA identified 133 security metrics. However, all of them are control-based metrics

2. Security Service Level Agreement (SLA)

   Mostly deals with controls, with very few metrics for vulnerabilities and incidents

3. Software Security Maturity Model

   Mostly deals with controls, with some metrics for vulnerabilities (e.g. penetration testing) although it does not seem to measure the rate or severity of vulnerabilities (instead, treating actions towards vulnerabilities as controls).

4. Cyber Security Assessment Netherlands

   The assessment is predominantly a qualitative evaluation of the existing controls in light of emerging vulnerabilities (and incidents, which are treated as potential vulnerabilities to others).

Moreover, cybersecurity firms such as Fox-IT and Symantec use other metrics when investigating and analyzing new threats. For instance, in the case of the Ponmocup botnet, Fox-IT uses early patterns of infection spread in order to narrow down the possible origin of botnet [12]. Similarly, Symantec used the number of infected hosts and infected organizations per country, as well as the geographic distribution of all unique infections to find the organizations and countries most at risk of Stuxnet infection [13].

Although these metrics are useful for the specific use cases of these cybersecurity firms, they are not particularly useful for analyzing the economic aspects of general cybersecurity issues. Countries with a well-developed internet infrastructure will be more exposed to threats than countries with a less-developed internet infrastructure. Well-developed countries will therefore generally have higher counts of infections, meaning that country-level metrics will simply be a measure of a country's size and state of its internet infrastructure.

Security Issue

In this report, the security issues are assessed from the perspective of domain registrars. In the case of ransomware, a domain registrar holds a crucial position due to its ability to mitigate the spreading rate of ransomware by taking down the malicious domain hosted in its registrar [14]. Other than that, the credibility of domain registrar is compromised when it failed to response towards the exploitation of its services as ransomware hosts. Therefore, the security issue in this report is stated as **"the exploitation of legitimate domain registrar service for ransomware hosting**".

In order to swiftly respond to the misuse of its domain registry, the domain registrars need an ability to precisely distinguish the exploited domain from the legitimate one. Ransomware uses several types of server consist of Command & Control Server, Payment Sites, and Distribution Sites. However, these servers can be unknowingly infected legitimate sites that are being used as the ransomware hosts [15]. If the domain registrar took down every malicious host without any consideration, there will be disruption of service for the legitimate site owners.

Furthermore, failure to mitigate the spreading of ransomware hosts will hurt the domain registrar reputation resulting in the addition of domain registrar in the blocklists. However, there are domain registrars especially created as "bulletproof domain registrar", which are usually used as the host for C&C servers. In this case, the domain registrars are very lenient on the utilization of its service by the customer and rarely comply with the takedown request on the domain it hosts [16]. Therefore, from the perspective of those bulletproof domain registrars, the exploitation of their services are not an issue.

Ideal Metrics

In the context of the above security issue, the ability to accurately detect the exploited hosts is needed as the domain registrars will therefore be able to precisely distinguish the exploited domain from the legitimate one. In a larger scale, it is also useful to identify which domain registrars whose services are mostly exploited as ransomware hosts. As explained earlier, domain registrars need to put measures in place to prevent the exploitation otherwise their reputation is at stake. By getting such information, warnings can be given to the exploited domain registrars so that they could pay extra attention in responding to the issue.

However, this only works when it is assumed that all domain registrars are "normal" registrars. Certain actions should also be taken to crack down bulletproof domain registrars as well. It will be insightful if one can identify which domain registrars out there are actually bulletproof domain registrars and where they are located. Such insights can be obtained by IT authorities in order to close and punish bulletproof domain registrars operating in a country, like in the case of Russian-based PROXIEZ-NET [17], or if this apparently becomes a regional or global issue, other nations can give pressure to countries that fail in responding to it or even supporting it.

Metrics Existing in Practice

Specific to the ransomware case, Ransomware Tracker site [4] provides a guideline aimed for home users and enterprises to avoid becoming a victim of ransomware. From the guideline we can extract several practical control metrics, as listed in table 1. However, these metrics focus mostly on controls and are very operational.

There are also many metrics used in practice by different organizations and cybersecurity firms, and to different ends. Several types of metrics are used by such firms in order to identify and understand the origin, target, and magnitude of cyber threats. Take Symantec, for instance, in the case of Stuxnet. They used several country-level metrics such as number of infected organizations and total unique infections per country to identify Iran as its primary target [13].

Fox-IT used similar metrics in its investigation and analysis of the Ponmocup botnet. By looking at the early infections per country, it was discovered that the botnet would avoid infecting machines belonging to the post-Soviet States of Ukraine, Russia, and Belarus, therefore indicating Russia as a possible origin of the botnet [12].

See table 1 for an overview of different metrics used in practice in the field of cybersecurity.

Table 1: Metrics currently existing in practice

Metrics	Definition	Other Notes	Sources
Backup rate	No. of backups performed per specific time	Focus on controls. Operational metric.	Extracted from [4]
Antivirus status	% of systems with current anti-virus software	Focus on controls. Operational metric.	Extracted from [4]
Patching status	% of systems with the latest software patch	Focus on controls. Operational metric.	Extracted from [4]
Awareness level	% of population that is aware of ransomware attacks and how to prevent them	Focus on controls. Operational metric.	Extracted from [4]
The dwell time	Mean time from compromise or infection to incident detection	Organizational-level metric	[18]
Detection to remediation time	Mean time from detection to remediation	Organizational-level metric	[18]
Total unique infections per country	The number of unique infected hosts by country	Country-level metrics	[13]
Total infected organizations per country	The number of infected organizations by country	Country-level metrics	[13]
Rate of infection of new IPs by Country	Number of newly infected IP addresses per day by country	Country-level metrics	[13]

Dataset Metrics

The CSV file that is made available from the ransomware tracker website [5] provides information on over 13000 ransomware associated domains. Of these domains, the tracker specifies when the domain was first seen as associated, the treat (function of the domain), what kind of malware it is associated with, its host, domain registrar, IP address, URL, country where the domain is located, ASN and the status of the domain (online or offline).

Aside from basic information on the number of IP-addresses that host malware threats, the number of hosts that are associated with specific malware, or the location of these threats, the dataset can also be used to design security metrics to respond to the central threat that is discussed in this paper: **"the exploitation of legitimate domain registrar service for ransomware hosting"**. The dataset can, for example be used to indicate the "Total unique infections per country" and "Rate of infections of new IP's by country" metrics as discussed in the previous section.

The dataset in question can, however, also be used to help to measure other metrics to better indicate not only the rate of exploitation of registrar domains for ransomware but also the efficiency of threat removal by those registrars and countries. Both metrics, that can be found in table 2, can help to identify threats, efficiency and tactics for fighting the exploitation of domains for ransomware hosting by/for registrars. The proposed metrics will be evaluated in the next section of this report, followed by an verdict on their value in the conclusion.

Table 2: Design of Metrics for the Dataset

Metric Name	Definition	Type of Metrics	Explanation
Threat removal effectiveness	Percentage of threats per registrar that is removed	Vulnerability / Incidents	This shows how efficient the registrar is in removing threats that are hosted on domains registered by the domain registrars.
Country removal efficiency	Percentage of online threats per country	Vulnerability / Incidents	This gives an indication of the effectiveness of malware removal in different countries.
Evolution of ransomware	Change in the occurrence of malware per month	Incident	This will give us an indication as to the evolution of the usage of the different types of ransomware.
Fraction of malware still online	Fraction of online threats and total threats associated to a specific malware	Vulnerability / Incidents	This gives an information about how a proper response has been or has not been performed to a particular malware in a global scale.
Dominant type of ransomware per domain registrars	Per domain registrar, the number of ransomware threats that appear the most	Vulnerability / Incidents	This will give us an insight about domain registrars preferred by a certain type of ransomware, thereby indicating their vulnerability to specific kinds of malware.

Dataset Metrics Evaluation

Domain registrars have the power to take down domains that are used for hosting malware. Removing such domains certainly hinder the impact of malware spreaders' actions. Domain registrars generally do not want to be known and used as safe havens for hosting malware, as this will likely have a negative effect on an organization's business. It is therefore in the interest of the legitimate parties involved to address the threat as soon as possible.

Some domain registrars are naturally more alert and proactive than others. One could expect the domain registrars based in countries with a well-developed internet infrastructure to be able to root out malicious domains more effectively than others. This does not seem to be the case, though. Figure 2 illustrates a domain registrar's threat-removal effectiveness as the ratio between the detected occurrences of hosted ransomware that have successfully been taken offline and the total number of ransomware detections on domains belonging to that particular domain registrar. As can be seen in figure 2, British *Plusnet Plc* and Dutch *Tele2 Zakelijk*, although based in countries with decent internet infrastructure, do not have the effectiveness that one would expect of such countries, both having an effectiveness of 25%.

On the other hand, the previous results are biased and tend to rank domain registrars disproportionately for the registrar with lower number of detections. For instance, *Plusnet Plc* and *Tele2 Zakelijk*, both have four total detections, out of which only one has been taken offline, resulting in the 25% effectiveness. In order to counteract this bias, the data was thresholded to include only those registrars that have appeared in at least 10 separate ransomware detections. Using this threshold, it is seen in figure 3 that the results change drastically. Now, we see much more diversity in the countries in which the registrars are based, which perhaps gives a more realistic quantification of effectiveness. This figure includes American *GoDaddy*, Chinese *BizCN*, Czech *GRANZY* and *REG-STABLE*, and Romanian *RoTLD*. In this case, there does not seem to be a clear correlation between state of internet infrastructure and threat-removal effectiveness.

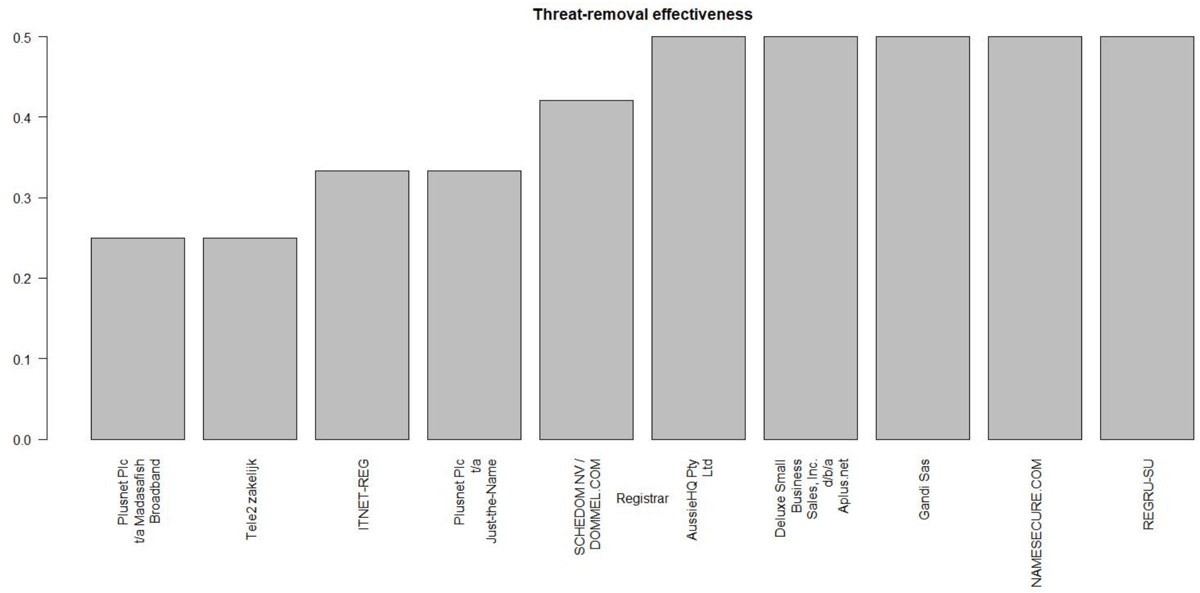

Figure 2: Top 10 registrars with worst threat-removal effectiveness

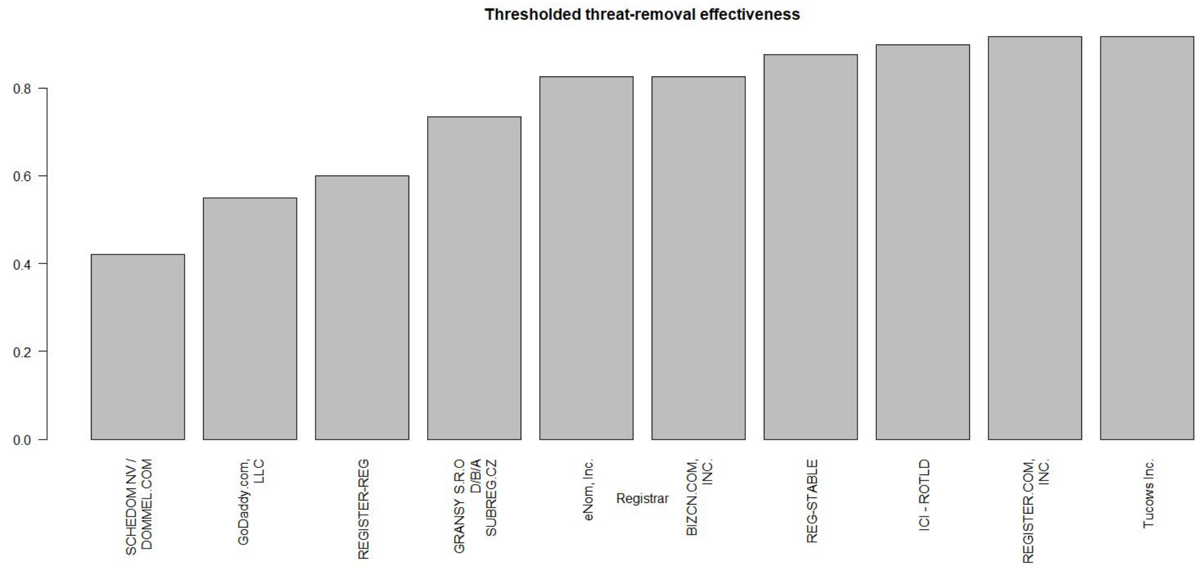

Figure 3: Thresholded top 10 registrars with worst threat-removal effectiveness

Figure 4 and 5 below illustrate the top 10 countries around the world with the highest fraction of threats that remain online after being detected by the *Ransomware Tracker*. Interestingly, Belgium appears as the country with the highest fraction of these online threats, coming in above Great Britain with around 0.29, even with less than a fifth of Britain's population. Similar to the process performed in figure 3, the results were thresholded to include only the countries where more than 10 ransomware threats have been detected. In both cases Belgium appears as the country with the highest fraction, closely followed by Great Britain.

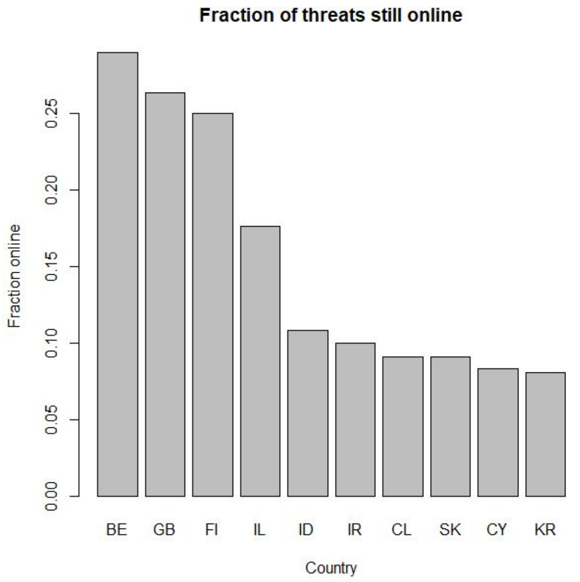

Figure 4: Top 10 countries with the highest fraction of online threats

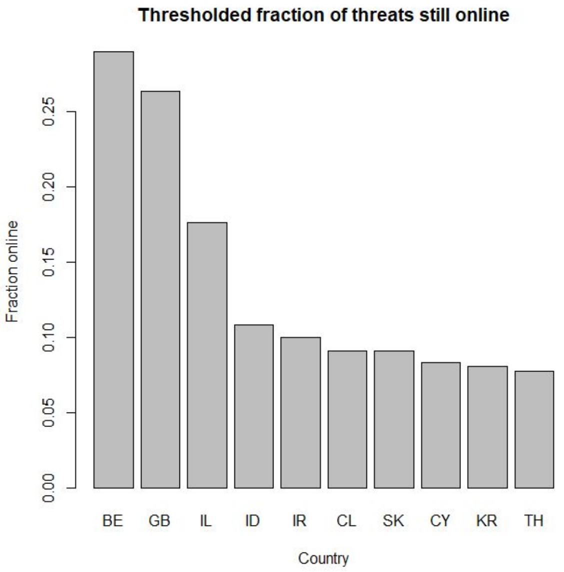

Figure 5: Thresholded top 10 countries with the highest fraction of online threats

It is beneficial for an organization to know the status and current usage patterns of the different ransomware tools. Many of the different tools use different delivery methods, different files, and different exploits. Some tools are used more than others, while others have not been used in a long time. By focusing prevention efforts at the most-used variants of ransomware, an organization can improve its protection significantly. Figure 6 illustrates the ransomware detections per month since mid-2015, grouped by ransomware family. The clear favorite is the *Locky* ransomware, peaking at around 3000 unique infection detections in November of 2016. *Cerber* and *TeslaCrypt* also experienced several peaks in usage.

Technology evolves rapidly. Some technologies die out quicker than others, while others maintain their 'market domination' for an indefinite amount of time. Figure 7 is essentially the same as figure 6, but capture the trend in year 2017. While it seems that *Cerber* achieve reasonable popularity compared to most of the other ransomware tools in figure 6, in figure 7 it is seen that *Cerber* is losing out to *Locky*, which overall has been the most utilized tool. It has even experienced another surge in usage betweem August and September of 2017.

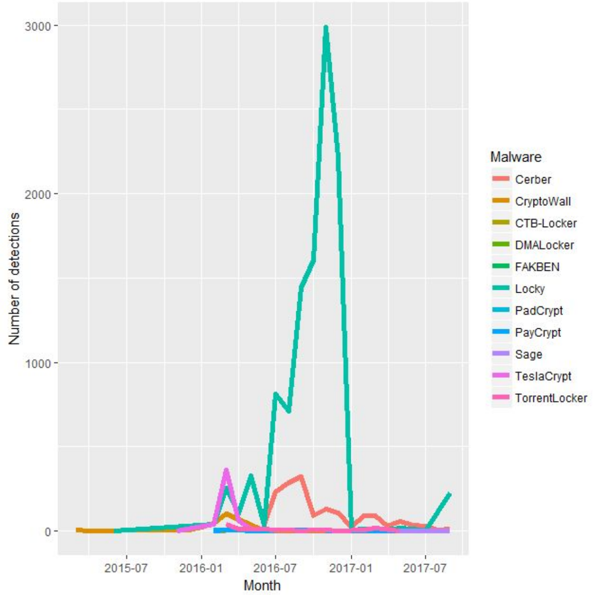

Figure 6: Ransomware detection occurrences per month

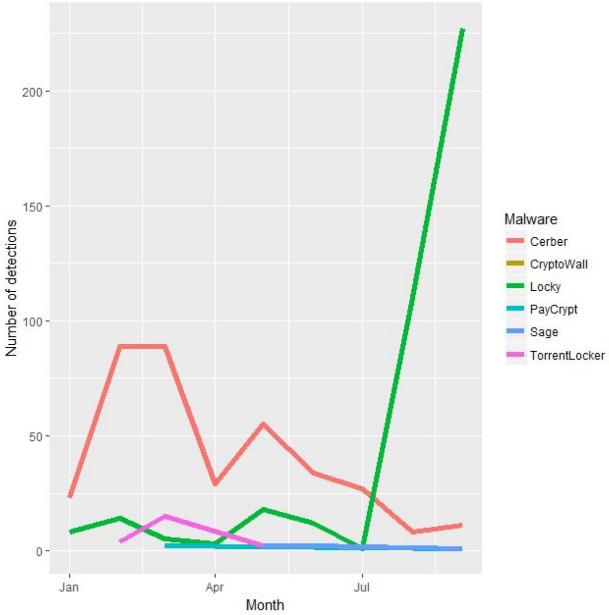

Figure 7: Ransomware detection occurrences per month in 2017

Figure 8 illustrates the fraction of ransomware threats that are still online, grouped by the specific type of ransomware. As can be seen, *CryptoWall* is the ransomware that is most prominent. *Locky*, on the other hand, has been significantly combated. This is even more impressive if the magnitude of *Locky*'s usage from figures 6 and 7 is taken into account, compared to the miniscule occurrence of the *CryptoWall* ransomware. It seems organizations are more preoccupied with the detection and removal of *Locky* ransomware due to its enormous popularity. This would come at a price, though, since it is found that *CryptoWall* ransomware has over 40% of its total threats still online.

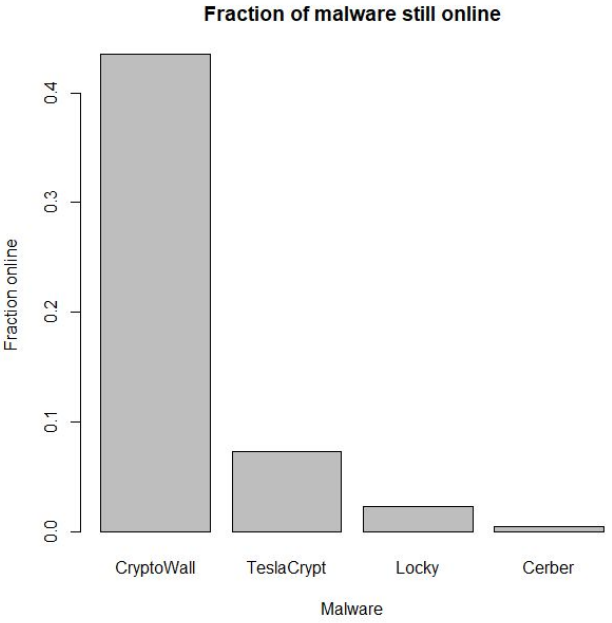

Figure 8: Fraction of malware threats that remain online

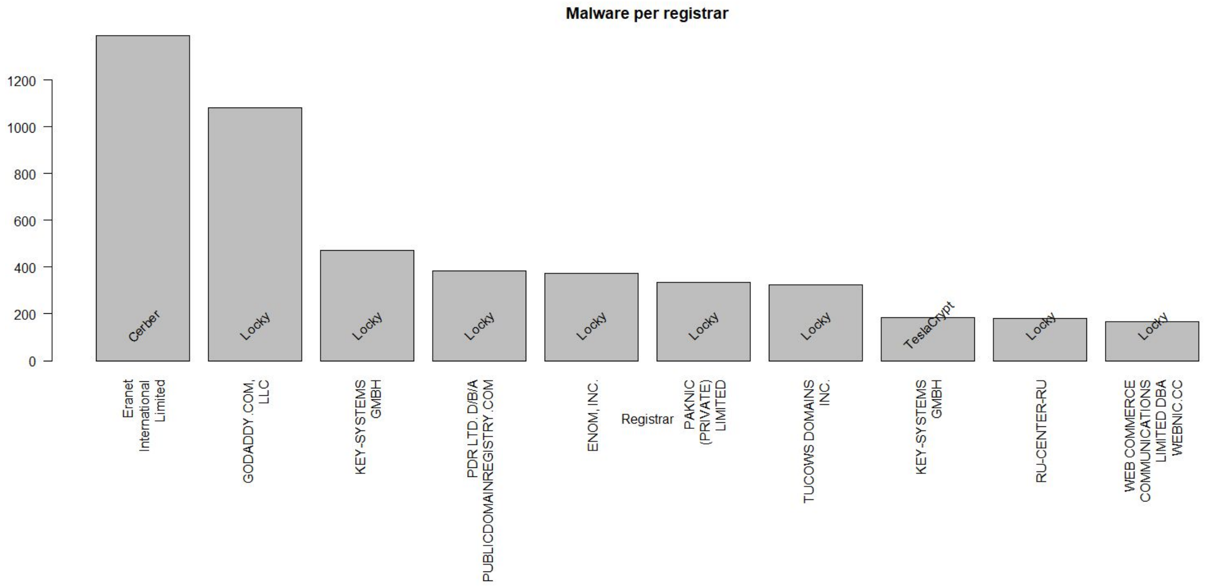

Figure 9: Domain registrars prefered for a particular ransomware

Figure 9 illustrates the tendencies of cyber criminals using ransomware to register their domains at certain specific domain registrars. Taking into account the identified preferences, this knowledge can be used for easier identification of ransomware servers, as well as faster response time. *Locky* is the ransomware that appears the most in this figure, which is not necessarily a surprise, since *Locky* has a significantly higher usage than the rest of the ransomware types, as figure 6 shows. It is interesting to see, however, that the Hong Kong-based *Eranet International Limited* registrar is the prefered registrar for registering domains for the *Cerber* ransomware, with it being single handedly responsible for around 1,400 *Cerber* domains. Perhaps it says something about the origin of *Cerber* itself or about the owner of the ransomware.

Conclusion

In this report, we have seen that in a particular cybersecurity case, performing a thorough analysis is very important in order to identify the real security issues that occur in the case. Every actor may have a different perception of the case, thus taking an actor's point of view is the key to see the issues that the actor experiences. Based on the nature of the dataset, focusing on the security issue come from domain registrars' perspective is the most feasible for this assignment.

It is also crucial to realize that there is a challenge in deriving proper security metrics to address a security issue, since many metrics commonly exist in practice are mostly not aligned with the ideal metrics that should be captured in order to address the issue. Defining accurate ideal metrics is thus an important step to do after having a proper definition of the security issue. Realistic metrics should be designed in accordance with the ideal metrics. Taking a step further from common metrics like counting attack occurrences or incidents is also needed since sticking to such metrics will not give any valuable insight. Therefore, this report proposed several metrics that are feasible to be analyzed with the provided dataset and align with the ideal metrics so that hopefully the insights that emerge from the analysis are valuable to provide a new perspective on the security issue defined earlier.

Finally, the security issues not only depend on the technical capabilities or infrastructures of so called domain registrars. The effectiveness of threat removal also depends on the policy framework of the country where the domain registrars reside. We recommend further study on the intertwined effect between technology and policy on the security issues addressed in this report.

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_2

References

[1] K. Miyakawa, T. Sato, K. Aga, and Y. Sugiyama, “Improvement of Financial Service Safety by Promoting Cyber Security Measures,” *NEC Tech. J.*, vol. 11, no. 2, pp. 42–45, Jun. 2017.

[2] “What you need to know about the WannaCry Ransomware,” *Symantec Security Response*. [Online]. Available: http://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware. [Accessed: 22-Sep-2017].

[3] I. Rijnetu, “A Closer Look at the Ransomware Attacks: Why They Still Work,” *Heimdal Security Blog*, 08-Aug-2017. [Online]. Available: https://heimdalsecurity.com/blog/why-ransomware-attacks-still-work/. [Accessed: 22-Sep-2017].

[4] “Ransomware Tracker.” [Online]. Available: https://ransomwaretracker.abuse.ch/. [Accessed: 15-Sep-2017].

[5] “Ransomware tracker CSV feed.” [Online]. Available: https://ransomwaretracker.abuse.ch/feeds/csv/.

[6] R. Böhme, “Security Metrics and Security Investment Models,” in *Lecture Notes in Computer Science*, 2010, pp. 10–24.

[7] “Course | WM0824 | Edge.” [Online]. Available: https://edge.edx.org/courses/course-v1:DelftX+WM0824+Fall_2015/course/. [Accessed: 18-Sep-2017].

[8] “R: What is R?” [Online]. Available: https://www.r-project.org/about.html. [Accessed: 17-Sep-2017].

[9] L. A. Gordon and M. P. Loeb, “The economics of information security investment,” *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 438–457, 2002.

[10] “Security Metrics What Can We Measure?,” presented at the Open Web Application Security Project (OWASP), Nova Chapter meeting presentation on security metrics, viewed (Vol. 2), Jul-2011.

[11] A. Zaharia, “What is Ransomware and 15 Easy Steps To Keep Your System Protected [Updated],” *Heimdal Security Blog*, 15-May-2017. [Online]. Available: https://heimdalsecurity.com/blog/what-is-ransomware-protection/. [Accessed: 17-Sep-2017].

[12] M. van Dantzig, “Ponmocup - A giant hiding in the shadows,” Fox-IT, Nov. 2015.

[13] N. Falliere, L. O. Murchu, and E. Chien, “W32.Stuxnet Dossier,” Symantec Security Response, Feb. 2011.

[14] 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.

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

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

[17] “‘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].

[18] M. Bromiley, “Incident Response Capabilities in 2016: The 2016 SANS Incident Response Survey,” SANS Institute, Jun. 2016.