WM0824TU Economics of Cyber Security

Assignment Block 2 Deliverables (Draft)

Group 7

Darli Ciang / 4624211

Samuel Natalius / 4608380

Mathew Vermeer / 4216989

Thomas van Biemen / 4206827

Context

For the assignment, our group uses the Ransomware tracker dataset taken from Ransomware Tracker site [1]. 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” [1]. The website provides CSV feed which can be downloaded and used for performing the analysis.

For analyzing the dataset, we use R, a language and environment for statistical computing and graphics [2].

Security Issue

The data speak to ransomware attack issue. In the ransomware attack, the attacker spreads a ransomware, a type of malware that locks the infected PC or blocks user access to a specific files, and then requests a ransom payment to the victims in order to “solve” the problem [3]. 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.

Methodology

In order to capture ideal security metrics, we used a framework proposed by Böhme [4] together with the provided video lectures of Economic of Cyber Security course on EdX platform [5]. 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 of our choice (R language).

Ideal Metrics

Security metrics ideally includes all 4 types of metrics below (from video lecture 2.3):

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 [6].
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 [7].

Metrics Existing in Practice

In general, there are several companies and organizations establish their own security metrics. Some of them are (from video lecture 2.4):

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).

Specific to the ransomware case, Ransomware Tracker site [1] also 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 many metrics that are 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 [8].

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 [9].

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 [1]
Antivirus status	% of systems with current anti-virus software	Focus on controls. Operational metric.	Extracted from [1]
Patching status	% of systems with the latest software patch	Focus on controls. Operational metric.	Extracted from [1]
Awareness level	% of population that is aware of ransomware attacks and how to prevent them	Focus on controls. Operational metric.	Extracted from [1]
The dwell time	Mean time from compromise or infection to incident detection	Organizational-level metric	[10]
Detection to remediation time	Mean time from detection to remediation	Organizational-level metric	[10]
Total unique infections per country	The number of unique infected hosts by country	Country-level metrics	[8]
Total infected organizations per country	The number of infected organizations by country	Country-level metrics	[8]
Rate of infection of new IPs by Country	Number of newly infected IP addresses per day by country	Country-level metrics	[8]

Dataset Metrics

Several metrics can be designed from the dataset obtained from the Ransomware Tracker. These metrics are listed in table 2.

Table 2: Design of Metrics for the Dataset

ID	Metric Name	Definition	Type of Metrics	Other Notes
1	Incident rate per malware	Number of incidents per malware for every specific time frame	Incident	
2	Incident rate per country	Number of incident per country for every specific time frame	Incident	
3	Differences between malware	Evolution of infection numbers among malwares	Incident	
4	registrar	Distribution among domain registration company (registrar)	Incident	
5	TLD	Number of incidents per top-level domain	Incident	
6	Indirect vulnerability	What domain companies are exploited with which malware	Vulnerability	

Dataset Metrics Evaluation

Figure 1 illustrates the countries with the most ransomware infections that are tracked by *Ransomware Tracker*. As can be seen in the figure, the United States of America is the country with the greatest volume of infections, having over 3000 infections, greatly surpassing Germany, which comes in second with around 600 infections, just 20% of the number of infections in the US.

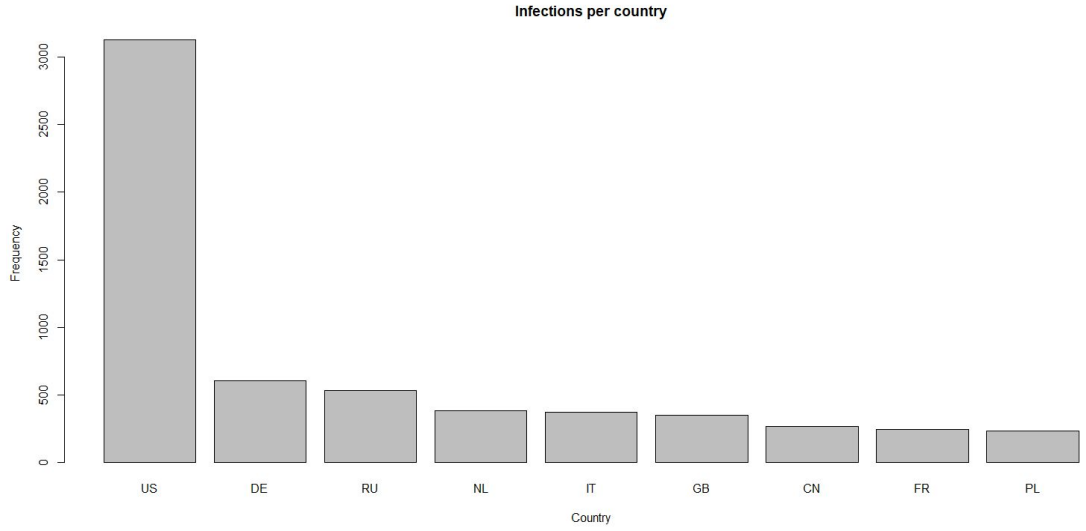

Figure 1: Infections per country

In figure 2 we see that the ransomware malware known as *Locky* is by far the most popular type of ransomware, with over 10,000 occurrences. Its popularity might be due to its ease of use, requiring only that the victim have *Microsoft Word* installed in order for the attack to be possible.

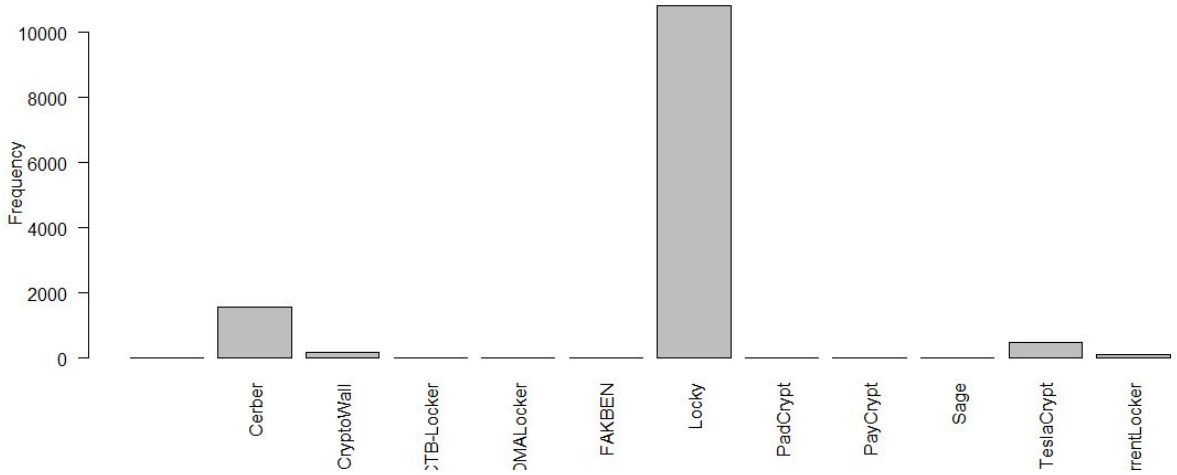

Figure 2: Ransomware type occurrences

References

[1] "Ransomware Tracker." [Online]. Available: https://ransomwaretracker.abuse.ch/. [Accessed: 15-Sep-2017].

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

[3] 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.

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

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

[6] "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.

[7] 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].

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

[9] M. van Dantzig, "Ponmocup - A giant hiding in the shadows," Fox-IT, Nov. 2015.

[10] M. Bromiley, "Incident Response Capabilities in 2016: The 2016 SANS Incident Response Survey," SANS Institute, Jun. 2016.