WM0824TU Economics of Cyber Security

Assignment Block 4 Deliverables (Draft)

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 proved to be malicious and furthermore take down the domain registrars which show no compliance to security standards. 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

Externalities in the Security Issue

These actors, however, are not the only influence on the exploitation of legitimate domain registrar service for ransomware hosting and the subsequent hit in registrar credibility. A whole range of externalities are also at play, such as:.

- The performance of botnets, which affects how efficiently the ransomware is spreaded. The number of Locky ransomware infections for example, fell down rapidly when the underlying botnet crashed.
- Discovery and usage of zero-day exploits. No amount of preparation can completely defend an organization from an undiscovered or unreported vulnerability. More of these might lead to an increase in ransomware spreading.
- The update of operating systems and software may possibly patch new security holes which can no longer be exploited by attackers to spread and activate ransomware, giving negative externalities to businesses or individuals using the OS.
- Awareness training provided by a company to employees may increase the awareness about the risk of ransomware and the way to address it to other people or the general society as well .

Factors explaining the variance in metrics

This part is not finished yet. However, these steps will be followed to complete this part:

- Choose the metric that wants to be analyzed. We select Country removal effectiveness (ratio of online vs offline hosts per countries) metric.
- Identify potential factors affecting that metrics
- Find potential external datasets that helps us to find the potential factors or to support our previously identified factors (e.g. from World Bank open data).
- Combine our own dataset & external datasets. By now we should have a big dataset consists of our metric values as Y and values from other factors as the X-es
- Perform statistical method (e.g. regressions to find the coefficient and p-values of the X-es, or ANOVA) to extract the correlation.
- Explain the result in terms of the pattern identified, the statistical confidence and the possible explanation of the cause.

Conclusion

Conclusion will be added in the end.

Additional Note

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

Link to GitHub

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/