Economics of Cyber Security (WM0824TU)
Malware Domain List
Assignment Block 3

Clinton Cao, Jehan Da Camara, Sharif Jacobino and Sunwei Wang
Group - 9

October 2, 2017

1. Introduction

In the previous report we took a look at the security issues that antivirus (AV) companies could be facing. AV companies are therefore our main actor and the owner of the problem that was discussed in the previous report. We have discussed the ideal metrics that AV companies would like to have to measure the security issue and we have found several metrics that are used in practice by AV companies. Based on the ideal metrics and the metrics are already being used by AV companies, we have designed and evaluated two metrics: Location based and VirusTotal Score.

In this report the focus is on the security strategies which AV companies are using to reduce the security issues. The report is structured as follows: first in section 2., we discuss the relevant differences that our metric can reveal in security performance. In section 3., we analyze the actors that could influence the security issue. Then in section 4., we list for different actors, the risk strategies that they can follow to reduce the problem. We then pick one strategy from the list and calculate the Return on Security Investment (ROSI). The result can be found in section 5..

2. VirusTotal Score & Security Performance

For the VirusTotal Score metric, we used the website of VirusTotal to calculate scores for malicious domains for which we can define an appropriate threshold for malware classification. The score is calculated using the evaluation result of multiple AV software. But one might ask: what does this metric say about AV companies and their security performance?

If the malicious domain is already known by the AV company, this metric can be used as an extra validity check; if all (or most) of the other AV companies have categorized the domain as a malicious domain, then there is a high probability the AV company has put the domain in the right category. This can provide information to the AV company that its performance is up to par with other AV companies.

On the other hand, if a malicious domain is not known by the AV company, then using this metric could provide information to the AV company that there is high probability that its security performance is lower than other AV companies. But not knowing that a domain is a malicious domain might be due to the influence of other actors (this is explained in the next section).

3. Actors Influencing the Security Issue

The security issues, which were described in the previous report, are heavily dependent on user interaction with the web. It would be infeasible to review every single website on the Internet; The Internet is large and there are constantly new sites being created. Therefore it depends on the users, whether an AV company needs to review a website that is not in the malware domain list.

This can vary immensely for different types of users or locations. Lets say that in a certain country where access to the Internet is limited to what the government allows, the public can only see what their government wants them to see. This means that the government could have already blocked some malicious domains. But on the other hand, users might still be able to use a VPN to access these malware infested sites.

It also depends on whether someone is browsing the Internet at home or at work. Lets say that at a big corporation, the traffic of the employees is being monitored. Employees will tend to refrain from visiting non-work related content on their devices if it can get them into trouble.

Another set of actors directly influencing the security issue is the group of cyber criminals putting malware online. They have the capability of setting up countless malicious websites. Those skilled enough could even hack legitimate websites and plant malware on it. Considering they also have access to some of the metrics AV companies use they can easily outmanoeuvre and outpace those trying to defend themselves or defend others.

4. Risk strategy

4.1 Risk Strategies for AV companies

In the previous report we have defined the following security issues for AV companies:

1. Keeping a list of domains that are considered to be malicious.
2. Checking whether domains that are not on the list are malicious or not.

Using these security issues as a focal point we define strategies, that can be followed by AV companies to handle these issues. One possible strategy is the sharing of threat intelligence. Different AV can share the (different) new malwares that they have encountered so other AV companies can be aware of these new malwares. This can be done by, for example, organizing conferences for AV companies or by publishing reports that are available to the public. The drawback of this strategy is that an AV company is also sharing knowledge to its competitors. This can cause the AV company to lose its competitive advantage in the business.

Another possible strategy would be to try to influence the user's actions with awareness campaigns or feature(s) which could influence users. For example in an awareness campaigns, AV comapnies can give users tips and tricks on how to spot whether a website is malicious or not. This could cause users to be more cautious when visiting random websites. But with this strategy, users might ask why it isn't automatically checked by the AV software. As an argument, AV companies can say that new malwares can be created (or evolve) over time and not all of them can be found directly. Making sure that users are aware of this problem, they could be more cautious online.

4.2 Risk Strategies of other Actors

Not only AV companies can make use risk strategies to defend against malware. Normal internet users can, for instance, refrain from using certain sites which are known to be malicious or download from unknown sources.

Other actors that can also implement risk strategies, that could help AV companies, are ISPs and hosting providers. If these actors find malicious sites or content they could share this information to AVs or can give them the content so they can assess if this is a new form of malware or a different implementation of a known malware so they can be better equipped to handle them in the future.

5. Return On Security Investment (ROSI)

One of the key factor in business is that benefits of an investment should surpass the initial cost, otherwise the investment is not worth it. This statement also holds for security and we will use the Return On Security Investment (ROSI) model to calculate if the investment is worth it. The equation is as follows:

$$ROSI = \frac{(\text{Risk Exposure} \times \%\text{Risk Mitigated}) - \text{Solution Cost}}{\text{Solution Cost}} \tag{5.1}$$

Calculation of the cost will be done for the final version.

6. Conclusion

Security is a very important and fast growing field in Computer Science. But it is very difficult to estimate cost for malicious content given the novelty of the field, and or lack of data. For example, cost can vary immensely from a malware cost. One example is that one site saying malware cost average is around $1,090 to resolve (http://www.wywlt.com/blog/average-costs-of-various-cyber-attacks.aspx) and other saying $ 1,077 for certain ransomware (https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/). This doesn't cover the variance of the cost with certain ransomware pay-out $17K in (cybersecurity ventures). Taken this into account you might potentially block the malware that cost nothing but the one's that cause a massive loss.

So an awareness campaign can potentially help but to calculate how much money it save can vary immensely.

Conclusion will be finished in the final version.

References