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

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

October 9, 2017

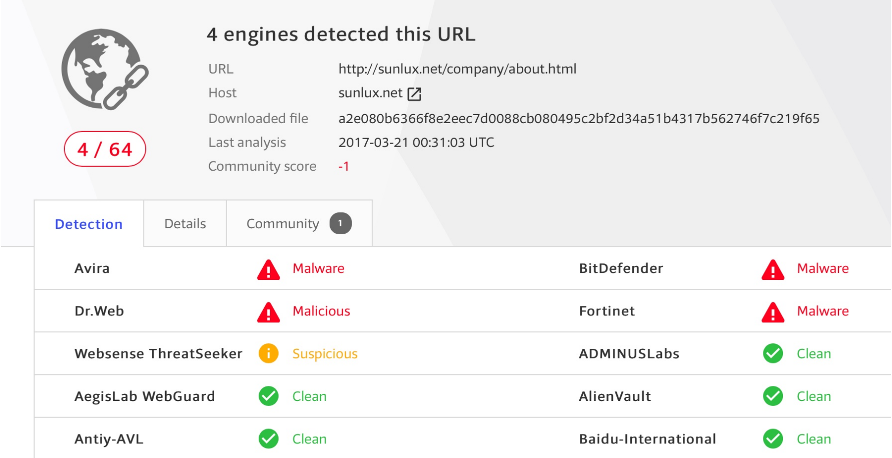
1. Introduction

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 that 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 could be using to reduce the security issues. The report is structured as follows: first in section 2., we discuss what our metric says about AV companies and their 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. In section 5., we discuss what are the costs are and the potential benefits if the actor is investing in the strategies that are mentioned in section 4.. We then pick one strategy from the list and calculate the Return on Security Investment (ROSI) for the actor. The result can be found in section 6.. Finally, section 7. concludes this report.

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. An example score for a URL can be seen in Fig 1.



4 engines detected this URL

URL http://sunlux.net/company/about.html
Host sunlux.net
Downloaded file a2e080b6366f8e2eec7d0088cb080495c2bf2d34a51b4317b562746f7c219f65
Last analysis 2017-03-21 00:31:03 UTC
Community score -1

4 / 64

Detection | Details | Community 1

Avira	Malware	BitDefender	Malware
Dr.Web	Malicious	Fortinet	Malware
Websense ThreatSeeker	Suspicious	ADMINUSLabs	Clean
AegisLab WebGuard	Clean	AlienVault	Clean
Antiy-AVL	Clean	Baidu-International	Clean

Figure 1: Example VirusTotal score for a URL.

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. The influence of other actors is further explained in the next section.

The “VirusTotal Score" metric could therefore provide an AV company information on how well they are performing in comparison to their competitors. Based on this information, the AV company can adapt their strategy.

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. There were one billion websites in 2014 and it has been increasing ever since [4]. The increase in number of websites can be seen in Fig. 2. Therefore it depends on the users, whether an AV company needs to review a website that is not in the malware domain list.

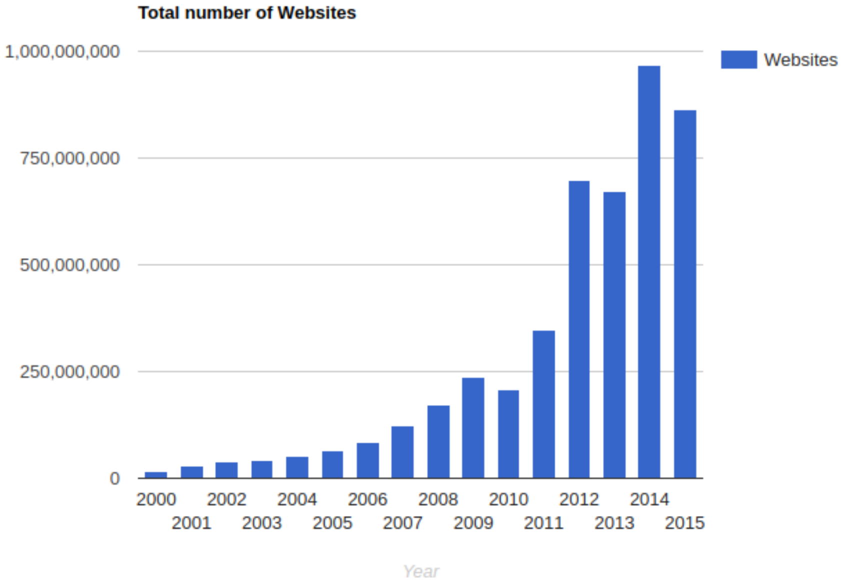


Figure 2: Total number of websites from 2000 to 2015. Graph is from [4]

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 companies 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. But from a study that has been carried out by Eidizadeh et al [2], sharing knowledge could help with gaining competitive advantage. The authors has argued that by just having knowledge does not provide power and value [2].

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 companies 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 websites or content they could share this information to the AV companies or they can give AV companies the content so that they can assess if this is a new form of malware or a different implementation of a known malware. This way AV companies can be better equipped to handle them in the future.

5. Investing in the Strategies

Let us now take a look at the cost and the potential benefits of the strategies that are mentioned int the previous section. We first consider the strategies that are mentioned for AV companies and then we consider the strategies of the other actors.

5.1 AV Companies

Sharing of threat intelligence does not directly cost the AV companies any money. As mentioned in the previous section, an AV company could lose competitive advantage by sharing knowledge to its competitors. With this knowledge, the competitors can improve their product. This can cause an AV company to lose customers, as there is an alternative product that has the same features or more. What would actually directly cost AV companies money, is organizing the conference or writing the reports.

For the conference, the AV company would have to rent a place that is big enough to welcome all their guests and the AV company would have to have enough staff members to help during the conference. It is possible that an AV company already have a place to welcome their guests, then there is no need to rent a place. Even though the AV company does not need to rent a place, they will still need to have enough staff members to help during the conference; the AV company will still have to pay the staff members.

For the reports, the AV company will have to pay employees to write the reports. If the AV company decides that the report should be printed on paper, then the AV company will also have to pay for the cost of printing. The cost of printing depends on how many copies the AV company wants to print out on paper.

For awareness campaigns, the AV company will have to pay employees to create the communication media that will be used for the campaign e.g. flyers, websites etc. To minimize the cost, the AV company can make use of digital media. This reduces the cost of printing out flyers and paying employees to go out on the street to inform the public.

Investing in these two strategies can provide potential benefits:

- By sharing knowledge, AV companies can learn from each other and use the knowledge to improve their products.
- By organizing conference and/or awareness campaigns, the AV company can build up a good reputation. With a good reputation, an AV company can attract more customers.

Alternatively AV companies can take the approach to actively seek new malware or malware infected domains so they can keep their list updated. This could give AV companies competitive advantage over their competitors. We now cover the two potential approaches that an AV can take and we discuss their potential benefits and drawbacks.

Firstly, AV company can go to the black market and try to buy all the available malwares. In theory this might be possible but this would be infeasible. According to [1] it is expected that a malware would be created every 4.2 seconds. This would financially deplete a company if they would buy every possible malware that has been created. Also there would be malwares that are not in use, meaning that this approach could easily result in loss of money.

Another approach would be for AV companies to start a reward campaign, where users can find malwares that the AV companies are aware of. AV companies could give the users a reward for finding such malwares. However, this approach can lead to the following problems:

- It is possible for an adversary to find out which malwares are not known by the AV companies. The adversary then know which malwares they should use to infect the computer of their victims.
- Malware creators would create new malwares just to get the reward.

5.2 Other Actors

For the strategy of normal Internet users, the only cost is time. A normal Internet user would have to spend time to read about malwares and how they can infect a system. The user have to spend time to gather knowledge on how to spot malicious websites. When the user is online, they would also have to spend a bit more time to be more cautious. Investing in this strategy can provide the following benefit to the user: the user lowers the probability that their system will get infected with a malware.

For the strategy of ISPs and hosting providers, they would have to pay for method that they are using to find malicious websites or content. This can done either manually or by using a tool. In the case that it is done manually, they would have to pay employees to find and report malicious websites or content. In the case that a tool that is used, they would have to pay for the tool.

Investing in this strategy can provide the following benefits to ISPs and hosting providers:

- They can build up a good reputation. With a good reputation, they can attract more customers.
- They can partner up with different AV companies. If they have partnered up with an AV company that has a good reputation, they can use the reputation of the AV company to promote themselves.

6. Return On Security Investment (ROSI)

One of the key factor in business is that the 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.

It is quite complex to calculate the ROSI for AV companies for the risk strategies describe in the previous section. We therefore analyze the risk strategies for normal users, in this example an average enterprise company. To make their employees more aware of the potential risks of malware infections, companies give their employees security awareness trainings. According to [7] a malware is downloaded every 81 seconds by an average enterprise organization. On a normal working day that would amount to around 350 downloaded malwares. Fortunately most of them are known and we assume that the company has common security controls in place to block known malware resulting in no loss. If we assume that the deployed security controls would block 99% of the malwares, 3 to 4 malwares would cause some degree of loss each day. A malware infection could cost an organization relatively little money if detected quickly however. In [8] a simple method is proposed to calculate the cost of a malware infection in an enterprise company. Using this method we estimated the cost of a malware infecting 3 machines causing 4 hours of downtime for 3 employees and 4 hours of repairing by a technician at $880. A data breach resulting from such an infection could cost an organization on average $3.6 million[3]. The impact range is thus very broad. We assume the impact distribution follows a power law distribution with the large majority of incidents being detected soon enough to have a relatively (less than $5.000) impact.

[6] claims that an investment in user awareness and training effectively changes behavior and quantifiably reduces security-related risks by 45% to 70%.

7. 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 [9] and other saying $ 1,077 for certain ransomware [5]. This doesn't cover the variance of the cost with certain ransomware pay-out $17K in [5]. Taken this into account you might potentially block the malware that cost nothing but the one's that cause a massive loss.

In this report, we have discussed what our metric says about AV companies an their security performance. We have listed a set of actors and how they can influence the security issue. We have listed for each actor the risk strategies that they could follow to reduce the problem. For each strategy, we have discussed what are the costs and potential benefits if the actor is investing in the strategy. We chose one strategy and calculated the Return on Security Investment (ROSI) for the actor.

References

[1] R. Benzmüller. Malware trends 2017. https://www.gdatasoftware.com/blog/2017/04/29666-malware-trends-2017, 2017. [Online; accessed 06-10-2017].

[2] R. Eidizadeh, R. Salehzadeh, and A. Chitsaz Esfahani. Analysing the role of business intelligence, knowledge sharing and organisational innovation on gaining competitive advantage. *Journal of Workplace Learning*, 29(4):250–267, 2017.

[3] Ponemon Institute. 2017 cost of data breach study. 2017.

[4] InternetLiveStats.com. Total Numnber of Websites. http://www.internetlivestats.com/total-number-of-websites/. [Online; accessed 6-10-2017].

[5] C Menlo Park. Ransomware damage report. https://documents.trendmicro.com/assets/wp/wp-analyzing-breaches-by-industry.pdf, 2017. [Online; accessed 30-09-2017].

[6] Wombat Security and Aberdeen Group. Reduce cyber security risks with employee training. https://www.wombatsecurity.com/about/news/reduce-cyber-security-risks-employee-training, 2015. [Online; accessed 07-10-2017].

[7] Check Point Software Technologies. 2016 security report. http://pages.checkpoint.com/security-report.html, 2016. [Online; accessed 06-10-2017].

[8] Tenable. The cost of incident response. https://www.tenable.com/blog/the-cost-of-incident-response, 2015. [Online; accessed 06-10-2017].

[9] WYWLT. Average costs of various cyber attacks. http://www.wywlt.com/blog/average-costs-of-various-cyber-attacks.aspx, 2016. [Online; accessed 30-09-2017].