Economics of Cyber Security (WM0824TU)
Malware Domain List
Assignment Block 4

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

October 23, 2017

Introduction

In the first assignment we covered from the perspective of antivirus (AV) companies, the security issues that they are dealing with:

1. Keeping a list of domains that are considered to be malicious
2. Being able to detect whether an arbitrary domain (that is not in the list) is malicious or not.

Moreover, we have taken a look at the metrics which are used in practice and we have designed a metric that AV companies could use to measure the security issues in the first assignment. In the second assignment, we have identified several actors and discussed how they can influence the security issues. We have also dived into the strategies that each actor can follow to tackle the problem. Each strategy can influence the variability of the security performance of the actors.

In this assignment we will need to select three actors involved with the security issues that is stated in the first assignment. The three actors which are involved in the security issues are the AV companies, an average Internet user, and Internet service providers (ISPs). Additionally we need to find the factors which explain the variance in the metrics and we need to perform statistical analysis on these factors. Based on the results of the statistical analysis, we can then derive the impact of these factors on the metric. In order to perform the statistical analysis, data needs to be collected for one or several of these factors.

The report is divided into two parts. The first part covers the countermeasures, which we believe, would be suitable to handle the security issues stated above. The second part discusses the security performance for the metric we designed in the first assignment. The outline for part one is as follows: first in section **??**, we look at what we think is a suitable countermeasure of each actor for the security issues. In section **??**, we list the benefits and cost that these actors for deploying the countermeasure. In section **??**, we discuss whether the actors have the incentive to take the countermeasures. Lastly for the first part, in section **??** will cover the externalities for these countermeasures.

The second part covers the security performance based on the metric we came up in assignment one. Our metric is based on the Virus Total approach. This approach will be elaborated later on in this report. Part II follows this outline: in section 4., we will take a look at the causal factors that explain the variance in the performance for Virus Total metric and take the data of one or several of these factors. Lastly in section 5., we perform statical analysis to explore the impact of these factors on the Virus Total metric.

Part I
Countermeasures Towards the Security Issues

As already stated in the introduction, ours focus is on the following actors: AV companies, an average internet users, and ISPs. In this part we will discuss for each individual actor one countermeasure they can apply to mitigate the security issues stated in the introduction. We also cover the cost and benefits for deploying these countermeasures. Additionally checking on what it will cost or how it will benefit the actor does not necessarily mean that the actor will deploy the countermeasure. After we analyzed the costs and benefits for the actors, we discuss what are the incentives for the actors to implement their countermeasure. Lastly, for the security issues and the countermeasures we discuss the externalities, both positive and negative, related to the cost and benefit of the countermeasure.

1. Internet Users

Last year in the Netherlands, there were almost 16 million Internet users. This is about 93.7% of total the population of the Netherlands [1]. These are users with different levels of expertise on how to use the subject. For average Internet users, an action that they can take is to be learn more about the different types of malwares that exists and use tools that protect them when they are online. Internet Users can learn about different types of malwares by, for example, reading different sources (blogs, papers, articles etc.) that provides information about malwares and how to tell whether a site might be suspicious or not. Internet users can download and use, for example, AV software to check whether their systems is infected with a malware.

The financial aspect for this countermeasure can vary depending on which tool is bought and/or whether the Internet user would pay to learn more about malwares (e.g. paying for lessons that is taught by an expert). Another cost of the countermeasure for the user would be time; users would have to spend time to read the different sources and gather knowledge from what they have read. The major benefit of this countermeasure is that Internet users are more aware of malwares and they know that they should be more cautious when they are online. They also know which tools they should use to protect themselves.

But this countermeasure does not guarantee that a user is completely safe from malwares. For example, adversaries can still use social-engineering to infect their victims. It is hard for a user to find out whether a file that their friend has sent them, is indeed legitimate and not a file that contains a malware. Adversaries can impersonate themselves as a friend of the user and the user could configure the AV software to white-list the file.

One important incentive for an Internet user to deploy this countermeasure could be that

a user wants protects is privacy against malware. With malwares being able to access the camera of a user without their consent means that someone could constantly watching them in their homes. Also there are malwares that can gather passwords of Internet users. Adversaries can use the passwords to access sites that could contain sensitive information of an Internet user. So from the perspective of an Internet user, there is a personal incentive to protect oneself. Besides the aspect of privacy, if an adversary gets your password of a financial institution (e.g. Bank) that you use, the result could be detrimental to your financial stability.

By looking at the costs and benefits of the countermeasure, we can see that it could have positive and negative effects for others. A positive effect could be that Internet users can help each other by recommending sources to read of tools to use. This can create a community of Internet users that are more aware of malwares and that are more cautious when they are online. This community can keep growing by sharing their knowledge with other Internet users that does not know much about malwares. One negative effect could be that Internet users think that this countermeasure costs them too much of their time and therefore decides not to start or to stop learning about malwares. This will not cause any changes to the problem.

2. Anti-Virus Companies

The job for an AV company is to provide an AV software that is able to detect and remove malwares. For this part, we thought of a countermeasure that an AV company can deploy outside of its regular function: AV companies could organize different could be better informed about malwares and know how they should protect themselves against malwares.

An AV Company can inform the general public in person or via online videos. The benefit of this countermeasure is that more the general public could be informed about malwares and they could be more cautious when they are online, causing them to be protect themselves better. Additionally, an AV company can use this countermeasure to promote their themselves and their product. This can raise the reputation of the AV company. But with this countermeasure, the general public can only learn as much as they can from the information that is provided by the AV company. This will cost an AV company a lot of time, as they constantly need be doing research and keeping the information up to date. Besides spending time on research, an AV company also needs time to organize and run the campaigns. This could also cost an AV company money, as they would need to pay staff members to do the research.

For an AV company, reputation is very important. If an AV company has a bad reputation, then no one will be using their product and thus also means that won't be able survive in the market. With awareness campaigns, an AV company could raise their reputation, as it shows that they are not just a company that only wants people to spend money on their products. Higher reputation can lead to more customers and which it can also lead to more

profit. So for AV companies, the countermeasure is highly profitable if it deployed correctly.

This countermeasure can have both positive and negative effects for others. A positive effect is that by organizing awareness campaigns, more people are better informed about malwares. These people can further inform more people and a community is then created. This community is the same as the one that is described in the analysis of the countermeasure of an Internet user. Another positive effect is that this countermeasure can engage other AV Companies to collaborate in the awareness campaigns. This can also boost the reputation of the other AV companies. There is a possibility that AV companies think this awareness campaigns could cost, in long term, too much money and time, AV companies can then decide to not deploy the countermeasure and this gets rid of the opportunity for the general public to learn more about the malwares and how to protect themselves.

3. Internet Service Providers

In the case of an ISP, a countermeasure they could introduce to combat malware would be to monitor the traffic of their whole network and either block the traffic or notify the host of the activity. Pan et al has shown in [2] that by analyzing the time patterns of malware events they can allocate resources to mitigate attacks in a more efficient manner. Alternatively in [3], they use reputation engine to successfully detect a specific malware called Advanced Persistent Threat. From these examples we want to show that there are various ways which an ISP can monitor the traffic to detect various types of malware.

The benefit of monitoring traffic would be able to remove all the traffic for malicious content. This would free up more bandwidth for benign traffic. So for its user, it could lead to faster traffic. But there is a saying in computer science: There is no free lunch in computer science. The only way to remove these malicious traffic would be to monitor all traffic and this can become very costly. Also this system needs to be created by ISP meaning this is additional work for an ISP. Another point of debate would be whether it is even possible to monitor all the traffic that is generated by the users of the network.

In the case of ISP, the incentive for deploying the countermeasure would be that it delivers a higher quality of service for their clients. A higher quality of service can lead the clients being more loyal to use this specific ISP, given the fact that it is more safe. Additionally another incentive for an ISP that the countermeasure can free up bandwidth for the average user, increasing the performance of the ISP. This could attract more customers as a higher Internet performance could sway users to switch. New user could also have a higher preference for an ISP with a better performance.

There are both positive and negative effects for this countermeasure. A positive effects that it boosts the reputation of an ISP and this can engage other ISPs to collaborate with each other to deploy this countermeasure. The collaboration can also boosts the reputation of other ISPs. Another positive effects is that the ISP can provides the users of its network

a bit more security against malwares. This may help if a user is unaware about malwares. Additionally by deploying the countermeasure, ISPs can provide a better performance to its users and can also attract more users. As mentioned before, it could become very costly for the ISP to monitor all traffic on its network. The ISP can decide that it is not worth it to deploy this countermeasure. This removes the extra security that the users can get from the ISP and therefore they can be vulnerable for malwares. They would have to be cautious and have the right tools to protect them against malwares. Another negative effect is that the ISP can decide to not collaborate with other ISPs and share the knowledge on how to detect malwares. This way the ISP can have a competitive advantage over its compeititor and this can the its competitors to lose profit.

Part II
Security Performance

In this part of the report we look at external factors that could be causing the variance in Virus Total scores for malicious domains. The VirusTotal metric gives an indication of the security performance of AV companies, specifically their performance in blacklisting malicious domains and removing cleared domains from their blacklist. We will be looking at factors that explain the difference in measurements between domains and the change of these measurements over time. Figure 1 shows the slight changes in VirusTotal scores over time.

4. Causal Factors

There are many reasons why VirusTotal scores change over time. First of all, a website can contain malware one day but the malware can be removed by the next day. The underlying factor in this case is whether the domain is intentionally malicious or if it is compromised. In case that the domain is compromised, the administrators of the domain need to be capable of detecting or being notified of a malware on their domain.

Secondly, the ability to identify a malicious domain varies per AV company. Organization focused on detecting malicious malware (such as malwares.com) might detect infected pages faster with other organizations catching up later on.

Another hypothesis is that the popularity of a domain might have an effect on if or when malicious content is detected on the websites. Malware on more popular website that see more traffic would be noticed, possibly faster compared to less popular websites. We gathered some data to test this hypothesis in the next section.

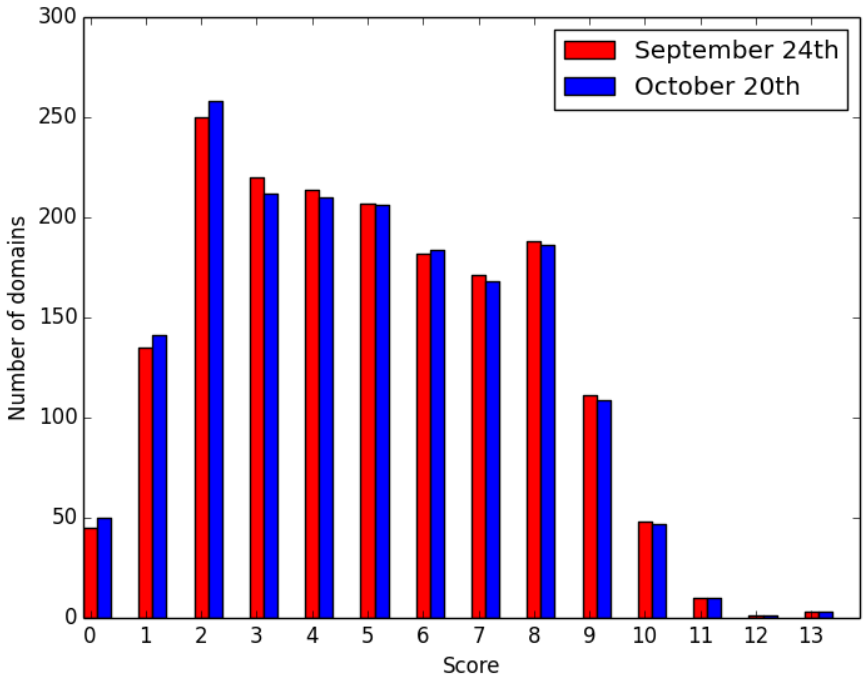

Figure 1: Virus Total score changes

5. Statistical Analysis

To gather data on the popularity of websites we first tried querying a traffic analyzer website (www.siteworthtraffic.com). However this website did not have result on a majority on the domains in our malware domain list. We therefore turned to the result count on Bing.com for queried domains for an indication on their popularity.

Figure 2 shows that most malicious domains have just a couple of thousands results on Bing.com and a VirusTotal score between 2 and 8. From this there does not seem to be a correlation between popularity and VirusTotal score. This however could be because the Bing.com result count is not an adequate indication of a domain's popularity.

We can evaluate the statistical significance of this data using Pearson's χ^2. The null hypothesis in this case is that the number of results on Bing.com and the VirusTotal score are independent. Conversely the alternative hypothesis is that they are dependent.

$$\chi^2 = \sum_i \sum_j \frac{(O_{ij} - E_{ij})^2}{E_{ij}}$$

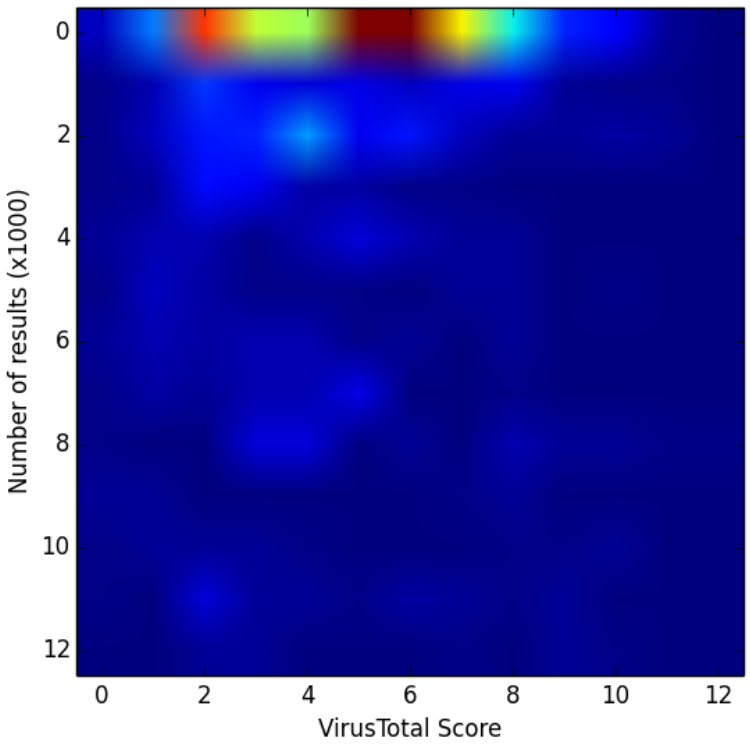

Figure 2: Result count vs Virus Total score heatmap

	0	1	2	3	4	5	6	7	8	9	10	11	12
0	5	22	76	52	48	89	89	58	32	14	10	2	0
1	1	4	16	9	7	8	5	8	9	2	1	1	0
2	1	5	13	14	25	9	13	5	2	2	3	2	0
3	1	2	12	9	3	3	1	1	0	0	0	0	0
4	2	4	4	1	4	7	4	2	2	0	0	0	0
5	1	5	3	1	1	1	0	2	2	0	1	0	0
6	2	4	3	4	4	1	2	0	2	0	0	0	0
7	1	3	2	4	4	8	0	0	1	0	0	0	0
8	1	0	0	7	7	0	2	0	4	2	2	1	1
9	2	2	0	0	0	0	0	1	2	0	0	0	0
10	1	2	2	2	1	0	0	0	1	1	2	0	0
11	1	0	7	2	2	1	3	2	1	2	0	0	0
12	0	0	2	2	0	0	0	1	0	2	1	0	0

Figure 3: Result count vs Virus Total score grid

The χ^2 value for the grid in figure 3 is 308.915822536. The number of degrees of freedom is $(\#colums - 1)(\#rows - 1) = (13 - 1)(13 - 1) = 144$. The χ^2 critical value with 144 degrees of freedom and a cumulative probability of 0.05 is 173.004 ($P(\chi^2 > 173.004) = 0.05$). In this case $308.915822536 > 173.004$ and thus we do not reject the null hypothesis. The number of results on Bing.com and the VirusTotal score are independent.

References

[1] Internet live stats. Netherlands internet users. `http://www.internetlivestats.com/internet-users/netherlands/`, 2017. [Online; accessed 14-10-2017].

[2] L. Pan, A. Tomlinson, and A. A. Koloydenko. Time pattern analysis of malware by circular statistics. In *2017 ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS)*, pages 119–130, May 2017.

[3] G. Zhao, K. Xu, L. Xu, and B. Wu. Detecting apt malware infections based on malicious dns and traffic analysis. *IEEE Access*, 3:1132–1142, 2015.