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

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

October 16, 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 1., we look at what we think is a suitable countermeasure of each actor for the security issues. In section 2., we list the benefits and cost that these actors for deploying the countermeasure. In section 3., we discuss whether the actors have the incentive to take the countermeasures. Lastly for the first part, in section 4. will cover the externalities for these countermeasures.

The second part of the 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 5., 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 6., we perform statical analysis to explore the impact of these factors on the Virus Total metric.

Part I
Countermeasures Towards Security Issues

1. Countermeasures

As stated in the introduction we have taken the following actors : AV companies, an average internet user, and ISPs. In this section we will discuss for each individual actor one countermeasure that they can apply to mitigate the security issues.

1.1 Internet User

Last year in the Netherlands, there were almost 16 million Internet users. This is about 93.7% of total the population of the Netherlands[2]. 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 educate themselves on how to avoid malicious software and use tools to check whether their system is infected or not. Users can educate themselves 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. Users can download and use, for example, AV software to check whether their systems is infected with a malware.

1.2 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 awareness campaigns where they inform their users (and even the public) on the different types of malwares and the risks of these malwares. Additionally, AV companies can provide information on when you could tell that a website could be malicious or not.

1.3 Internet Service Provider

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 [3] that by analyzing the time patterns of malware events they can allocate resources to mitigate attacks in a more efficient manner. Alternatively in [4], 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.

2. Benefits & Costs

In section 1. we stated, for each actors, the countermeasure that they can take against malware. Now we will cover the benefits and costs of the countermeasures for each actor.

2.1 Internet User

As stated in section 1., the countermeasure for an Internet user would be to educate themselves and use tools to help mitigate the problem. The financial aspect for the countermeasure can vary depending on which tool is bought or how the education process is covered. 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 could be that there are fewer malware attacks, because informed users can make a better decisions. But this countermeasure does not provide a solution the following problem: Adversaries can still use social-engineering to infect their victims. For example, 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.

2.2 Anti-Virus

The countermeasure for AV companies is to organize different awareness campaigns for their users or for the general public. This can be done in person or via online videos. The benefit of this countermeasure is that more users 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 users or 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 the campaigns and run.

2.3 Internet Service Provider

The countermeasure for an ISP is to monitor the traffic of their network and block that traffic that are related to malicious activities. 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 check the entire traffic that is generated by the users of the network.

3. Incentives

In the section we will cover the incentives that our actor : ISP, internet user, and AV, would have to implement the countermeasures stated in section 1.. Each actor incentive would can be very different and for that reason we will cover each actor individually.

3.1 Internet User

One important incentive could be that a user wants to learn more about malware is privacy. With malware being able to access the camera of a user without their consent means that someone would be able to be alone within his or her home. Also passwords can become compromised with all the information on the sites. So there is a personal incentive to protect oneself.

3.2 Anti-Virus Companies

For an AV company, reputation is very important. If 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 want get money from their customers. 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.

3.3 Internet Service Provider

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.

4. Externalities

Main points that need to be mentioned in this section (this is therefore a plan on what we are going to write in this section):

4.1 Internet User

- positive: users can further teach other Internet users, creating a bigger community of users that are well informed about malwares.
- negative: one user that learns a lot about malwares, can use this information to create their own malwares.
- negative: charge other users for teaching them about malwares

4.2 AV Companies

- positive: engage other AV companies to also collaborate in the awareness campaign
- positive: create a community of users that are well informed on malwares and this can they can also further teach other Internet users, expanding the community.
- need to research on negative externalities of this countermeasure.

4.3 Internet Service Provider

- positive: engage other ISPs to collaborate with each others to solve the problem.
- negative: Clients/user of the network might not like it that ISPs are monitoring all the traffic.

Part II
Security Performance

In this part of the report we will be looking at external factors that could be causing the variance in Virus Total scores for malicious domains. The Virus Total metric gives an indication of the security performance of AV companies, specifically their performance in blacklisting malicious domains. We will be looking at factors that explain the difference in measurements between domains and the changing of these measurements over time.

5. Causal Factors

There are many reasons that cause the variance in the result of the VirusTotal metric that we came up with in the first assignment. First off, a website can contain malicious content today but it can be removed the next day. So the amount of malicious content can vary with time for a website. Another causal of the variance is the amount of damage that malware can cause and the resources that is needed to mitigate the malware. According to the VirusTotal site the browser that you are using can also cause a variance for the result. Certain browser can also influence the results of Virus Total score due to the fact that some engines will provide additional information, stating explicitly whether a given URL belongs to a particular botnet, which brand is targeted by a given phishing site, and so on [1]. Furthermore malware signatures are updated frequently by VirusTotal as they are distributed by antivirus companies, this ensures that they are using a set of signatures that are up to date [1].

6. Statistical Analysis

For the statical analysis we plan to carry out the same metric used on the entire Malware Domain List and compare the first result with the next one. The reason that we didn't do it for the draft is that VirusTotal API limits us to certain amount for a given time. In the final version we planned to show the overall difference. And check for each site if there result vary.

References

[1] https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works. [Online; accessed 15-10-2017].

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

[3] 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.

[4] 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.