WM0824TU Economics of Cybersecurity
Malware Droppers Assignment 3

Kanav Anand 4712870
Dinesh Bisesser 1512250
Philip Blankendal 1547682
Richard Vink 4233867

October 22, 2018

Contents

1. Introduction

Internet and cyberspace are things that have spread themselves into a lot of the main and most relevant areas in today's economy. It is as important as other utilities like water and electricity. With more and more companies being digitalized, adversaries are increasing and becoming more active. Thus cyber security is becoming more important in order to protect not only data but also services, communication and users.[6] Implementing cyber security is hard, for there are allot of factors that need to be accounted for. One of these factors is economy. The economics of cyber security deal with economic concepts, measurement approaches and data analytics in order to make better security decisions.

For this assignment we will look into a dataset of malware droppers: **A Trojan that installs some malware on a target machine**.[1] The dataset[2] contains timestamps and urls, so the time and place of where the malware droppers were downloaded from are known.

We have analyzed the dataset and came up with security metrics that can be used to measure malware droppers data. In order to do that we looked at what security issues the data speaks to. After that we discussed the ideal metrics for security decision makers and found out which metrics exist in practice. Finally we defined the metrics we can design from the dataset and evaluated them. We thus came up with the following three metrics: Downloader Count, Time Difference and Domain Count.

After that we defined the problem owner and came up with other actors that are involved with this problem. Risk strategies were defined for all of these actors and the ROSI was calculated for one of these risk strategies.

Now that we have knowledge about the security issues and metrics, actors involved and risk strategies, we will look into why different actors have different risk strategies and how different these strategies are.

In the first section we define the problem owner and two other actors. For each of these three actors we then define one concrete countermeasure, analyze costs and benefits among the different actors that the deployment of the countermeasure would entail, analyze if actors have an incentive to take the countermeasure and reflect on the role of externalities around this security issue.

Last we identify the type of actor, whose security performance is visible in the selected metric. Different factors are explained for causing the variance in the metric, data is collected for these factors and a statistical analysis is performed to explore the impact of these factors on the metric.

2. The 3 actors (including the problem owner) involved in the security issue

In order to see why there are different reasons behind different actors, we first need to come up with three actors to analyze.

[1] https://en.wikipedia.org/wiki/Dropper_(malware)

[2] https://surfdrive.surf.nl/files/index.php/s/MZbaZl2fF0SD2QV

The problem owner has been defined as private organizations and its employees, for malware droppers can cause a lot of damage to them.

Another actor we will consider are the hosting providers. These malware droppers are hosted on several domains of several hosting providers, so they can be (partially) considered responsible for hosting these malware droppers.

Finally the government will be the last actor to compare to. While they can also be harmed by these malware droppers, they have the power to create laws and actually change things on a national level. Stopping these malware droppers nationwide.

2.1 One concrete countermeasure for each of the 3 actors that they could take to mitigate the security issue.

Private Organizations:
Training employees to not click on malicious links with malware droppers can help reduce the amount of malware installed within a private organization. By continuously training users in the real world for phishing trained them to identify phishing scams, no matter if the user has a technical background or not.[4] Phishguru (tool used for training against phishing) helps train users to avoid giving information to phishing websites,does not retain users on clicking valid mails and users retain knowledge from Phishguru even after 28 days.[3]

Hosting Providers:
Using an antivirus on their hosts to detect malicious activities or compromised websites could help create a safer internet environment.[1] This way less malware droppers will be hosted and thus less users and organizations get effected by them.

Government:
Create laws(with fines) to ensure security within organization. This way organization have to act against these malware droppers, which gives a better feeling of security within these organizations and consumers.[2] They could also help enforce blocking of certain domains,either by hosting providers or ISPs, if it's known to be malicious.

2.2 Analysis of the distribution of costs and benefits (without quantifying) among the different actors that the deployment of the countermeasure would entail.

Private Organizations:
Depending on the amount of employees of the private organization, the cost will rise if there are more employees. Training should also be done frequently and it will cost the organization not only money for the training and tools itself, but also employee time which they are not spending on their actual job. This indirectly will cost the organization money as well.

The benefit however is more awareness among employees about malicious websites and email, making malware less likely to be installed within the organization's network.

This then ensures less likely of assets being attacked or information being leaked.

Thus the benefits outweigh the costs, for the potential damage would be higher then the investment in training.

Hosting Providers:
The costs of a good antivirus is not very high, whereas the benefits of detecting and mitigating malicious hosts is very high for consumers and organizations become more trustworthy if a hosting provider has few malicious hosts. This in turn might get the hosting provider more customers, thus more profit.

So the benefits outweigh the costs extremely for installing a good antivirus for hosting providers.

Government:
Creating laws is hard and a tedious process. It costs a lot of money and time to actually come up and implement good laws to ensure security within organizations.

The benefits are also low for the government itself, for these laws will help organizations and civilians the most. It will however produce good publicity for the government.

So the benefits do not outweigh the costs in case of creating new laws.

2.3 Analysis of whether the actors have an incentive to take the countermeasure.

Private Organizations:
Training their employees will help ensuring less malware getting in private orgranizatons' network. The incentive here is thus that it helps ensuring that confidential information stays confidential and that assets within the organization are safe. This is important for any private organization and so their incentive to take countermeasure is very high.

Hosting Providers:
A major incentive for the hosting provider is having hosts without malicious content on them, so that they are not part of the problem and can be hold (partly) accountable. Another reason for taking counter measures for hosting providers is to ensure good publicity. This way organizations and consumers will trust them more and thus will use their services. It might also be illegal to (help) host malware. These incentives can be important, depending on the country and types of clients the hosting providers is looking to attract.

It could also be the case that hosting providers might have incentive to not take any actions. If for instance the majority of their customers are people who are setting up these malicious hosts. In this case they would lose them as customers and might attract less similar customers.

Government:
If certain malware can cause privacy issues, by leaking information, the government might see that as incentive to create laws for organizations to have better security. Petitions

and a referendum may also urge them to act on that, and start creating new laws or edit current laws.

Governments however can also use malware to find backdoors or exploits in software to use. This way they can spy on people (for good or bad), which could be an incentive not to take any countermeasures.

2.4 Reflection on the role of externalities around this security issue.

Private Organizations:
There are many negative externalities for private organizations when it comes to malware droppers. One such negative externality is that compromised computers within the organization's network might be used for bad activities by being part of a botnet. For example a DDoS attack. Another externality might be increase of energy bill and/or (early) failure of hardware due to, for instance, mining malware for cryptocurrency.

A positive externalitiy would come from the counter measure. Employees might use their training in other aspects of their live, to become more aware of security. Both online, as well as offline.

Hosting Providers:
Bad publicity might be a negative externality for hosting providers. However if countermeasures are implemented well, they can use that as good publicity in order to attract more customers.

Another negative externality could be that fines and lawsuits might be considered by governments or organizations, when they find out that the hosting provider is hosting malicious content.

Government:
The government will have a hard time convincing companies to settle in their country if they do not act against the security issue. Civilians might also loose their faith in the government.

3. The type of actor whose security performance is visible in the selected metric(s) (e.g. ISPs, software vendors, countries).

Domain count metrics help people see the domains which contained malware. Domain count metrics can help security officers find the most dangerous URLs. These URLs can be seen as the URLs which contained a lot of malware droppers. A high frequency of a specific domain using this metric, reflects a higher infection rate on that specific domain.

This metric can be used to evaluate the performance of antivirus software. This is done by comparing the domain counts of each month. Antivirus software should destroy these malware on these specific domains. If the antivirus software did its job, the malware should not be on the domain in a later point of time. If its still there, the domain is probably owned by a malicious organization who strives to infect as many machines as possible. Figure 1 shows the top 10 of domains which contained malware the most over the timespan 2014-2016.

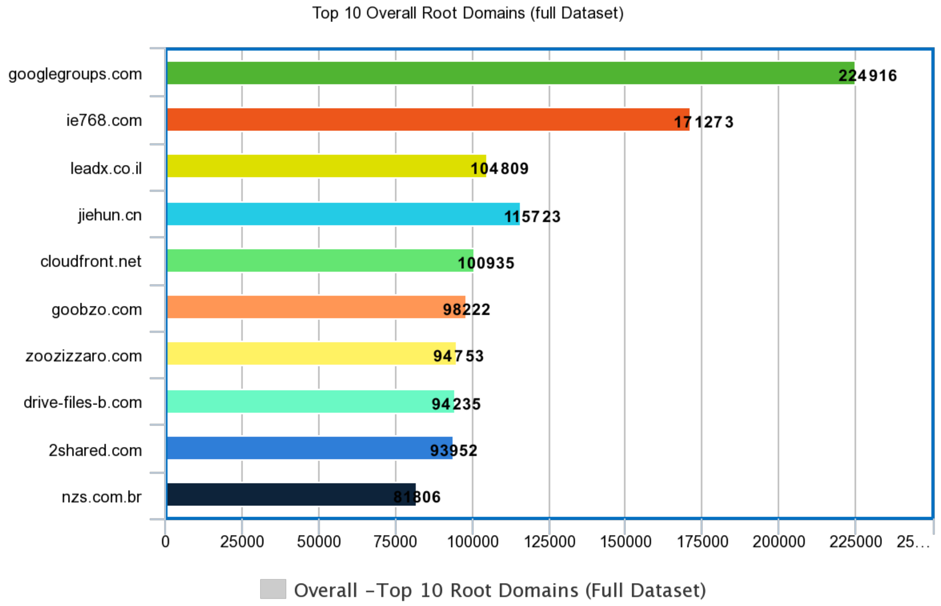

Figure 1: Top 10 domain count

In appendix A you can find the top 10 domains of 2014, 2015 and 2016 individually.

Another performance measurement which can be detected out of the metrics is the difference between domains from an organization and domains like : `http://down.81cs.org:88/`. Domains which consist of IP addresses and domains on a specific port number are domains which most likely are not owned by organizations. It is easier to find organizations who have malware on their domain then finding the culprits of owning the other malware droppers. Actors involved here are the actors in charge of regulating the rules. Governments can be one example of those actors.

3.1 Different factors explaining (causing) the variance in the metric.

The variance in the domain count metric can have different causes. These causes are listed below.

1. An adversary might have decided to place its dropper on a different domain. Measuring the effects of this change of domain is difficult. For this research, we only have a list of infected URL's. This list only reveals when a specific domain was compromised. There is no knowledge on the specific Malware Dropper on the URL. Thus, antivirus software are not able to detect this change of domain.

2. Another factor which could cause the variance in this metric is the fact that antivirus

software are having a hard time detecting malware droppers. That is, most of the time they have a low detection rate[5].

3. Another variance in the metric is that the domains of organizations can be hard to detect. For instance a dropper located on an URL containing a port number, can also be a legitimate link within the organization. For this research, we count all these types to be not in the set of organizations' domains.

4. The amount of malicious malware can differ per month. As seen in the data, the amount of malware in August is higher than the amount of malware in other months. This can be seen later in the paper. Reasons for this variance can be new trends in malware droppers, higher detection rates by antivirus software or adversaries being deliberately active.

3.2 Collected data for one or several of these factors

For the purpose of collecting data we check URLs by organizations compared to URLs not by organizations. Differences are: IP addresses used instead of domain names consisting of letters and the use of port numbers. Port numbers are typically not used by organizations construct their public URLs. For April 2014, the amount of malicious links is: 605098. Likewise the same data for the domains for may 2014 and June 2014 can be found.

Second, a distribution is made based on the amount of malicious domains. This distribution shows the probability that a malicious link is from a specific month. This distribution can be seen below in Figure 2.

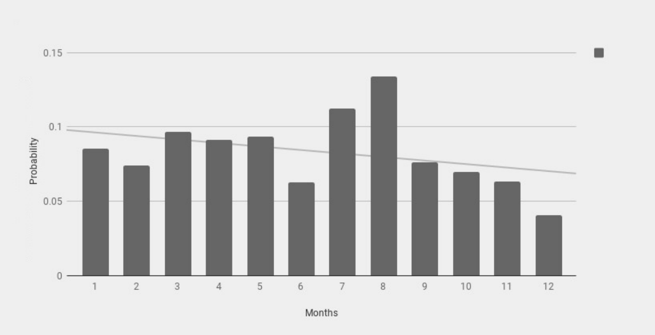

Figure 2: Probability malicious links per month

Furthermore, a comparison between the domain counts of several months are used. This data will be collected to compare if the antivirus software is doing its work like it should. The amount of malicious domains for one month will be compared with the amount of malicious domains of other months to find differences for each month. This data can be used to make a linear regression out of the acquired data.

3.3 A statistical analysis to explore the impact of these factors on the metric.

To create a linear regression out of all the months containing malware, one first has to find the medium. This can be calculated by the average of all the months which is: 265388,1176. Now one can compare this number with the amount of malware for each month, as can be seen in Figure 3.

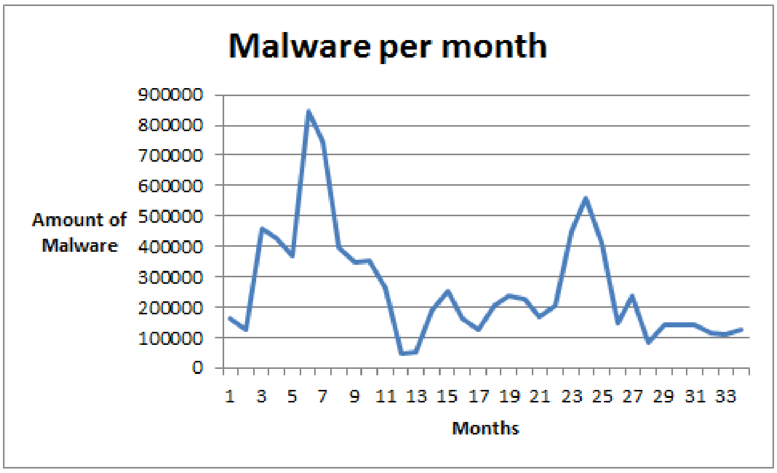

Figure 3: Malware per month

To compare the differences per months in which the malware could be found, linear regression can be used. 2014 and 2016 contain a lot of spikes, whilst 2015 contained a more linear distribution of the spikes. Therefore, we create a linear regression of the months of 2015 combined with the malware it contained. This can be seen in the figure below:

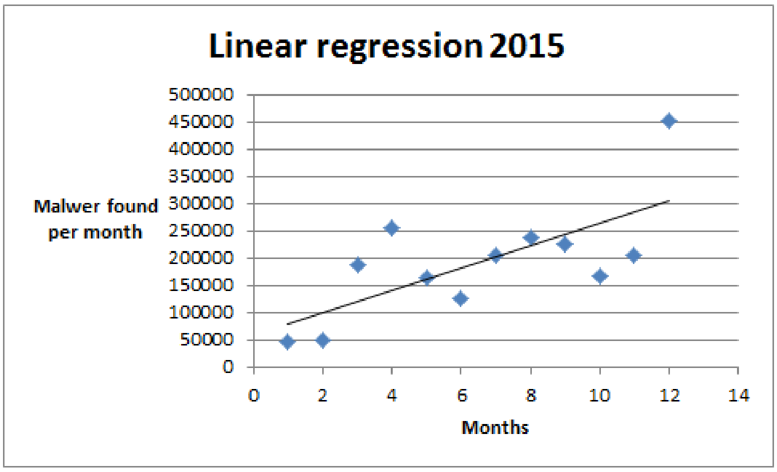

Figure 4: Linear regression 2015

As you can see in Figure 4 the malware for this year is spread around the 20.000 per month. There is only one big outlier in December. A possible reason for this outlier is because people are getting their Christmas gifts in this month. Creators of malware might infect more URLs because of this.

Another important feature this regression has, is the fact that more malware droppers can be found at a later point in time. There can be a lot of reasons why this would occur. For starters, antivirus software could have a harder time detecting the newer droppers. Another reason is that adversaries created a larger volume of droppers. A larger amount of droppers could potentially return in a higher rate of infected URLs. Last, this rise can also be explained by the fact that the internet is getting larger as well.[3] A larger amount of websites, automatically means a larger amount of infected websites as well.

4. Conclusion

So we see that the three different actors have different countermeasures, costs & benefits, incentives and externalities. Private organizations, as the problem owner, and hosting providers have the biggest incentives and benefits to take countermeasures against the problem of malware droppers. The government on the other hand has less incentive to countermeasure, with less benefits compared to the costs. All three have negative externalities around this security issue, with both private organizations and hosting providers having one positive externality.

With our security metric being domain count, the type of actor whose security performance is visible in that metric are the organizations of those domains. Four different causes have been explained for the variance in the metric and data was collected for these factors. A linear regression was made for months containing malware. This showed us that the metric is strongly influences by the month, due to different general activities (like holidays) for different months.

Another important feature of the data was the rise of malware droppers over time. This can be explained by: antivirus software having a hard time detecting the newer malware droppers, adversaries creating a larger amount of droppers or because of the rise of the internet. This means that malware droppers still can cause trouble in the future.

References

[1] D. Canali, D. Balzarotti, and A. Francillon. The role of web hosting providers in detecting compromised websites. In *Proceedings of the 22nd international conference on World Wide Web*, pages 177–188. ACM, 2013.

[2] K. J. Knapp, T. E. Marshall, R. K. Rainer Jr, and D. W. Morrow. The top information security issues facing organizations: What can government do to help. *Network security*, 1:327, 2006.

[3] https://news.netcraft.com/archives/2018/01/19/january-2018-web-server-survey.html

[3] P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M. A. Blair, and T. Pham. School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, page 3. ACM, 2009.

[4] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong. Lessons from a real world evaluation of anti-phishing training. In *eCrime Researchers Summit, 2008*, pages 1–12. IEEE, 2008.

[5] D. Quarta, F. Salvioni, A. Continella, and S. Zanero. Toward systematically exploring antivirus engines. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 393–403. Springer, 2018.

[6] R. Von Solms and J. Van Niekerk. From information security to cyber security. *computers & security*, 38:97–102, 2013.

A Top 10 domains per year

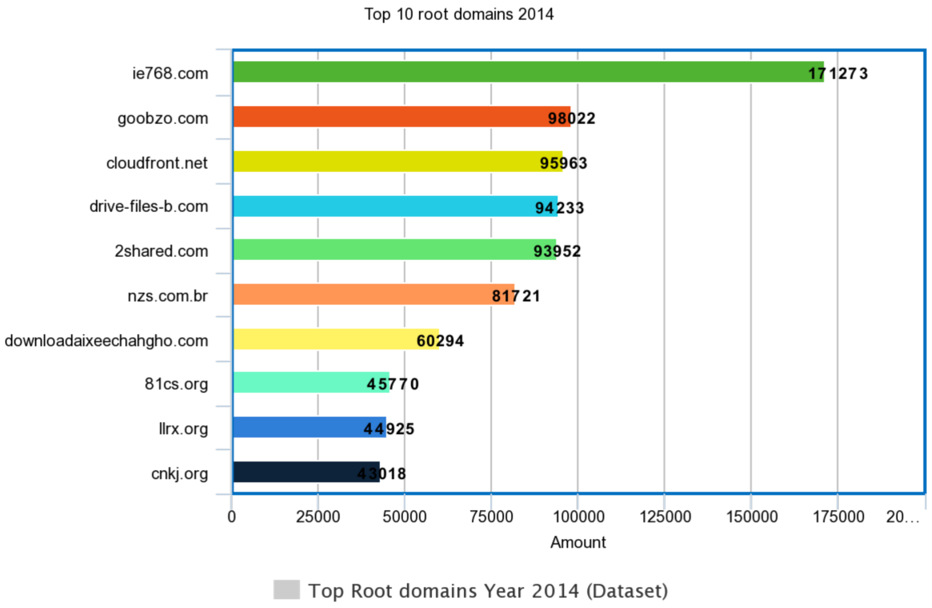

Figure 5: Top 10 domain count of 2014

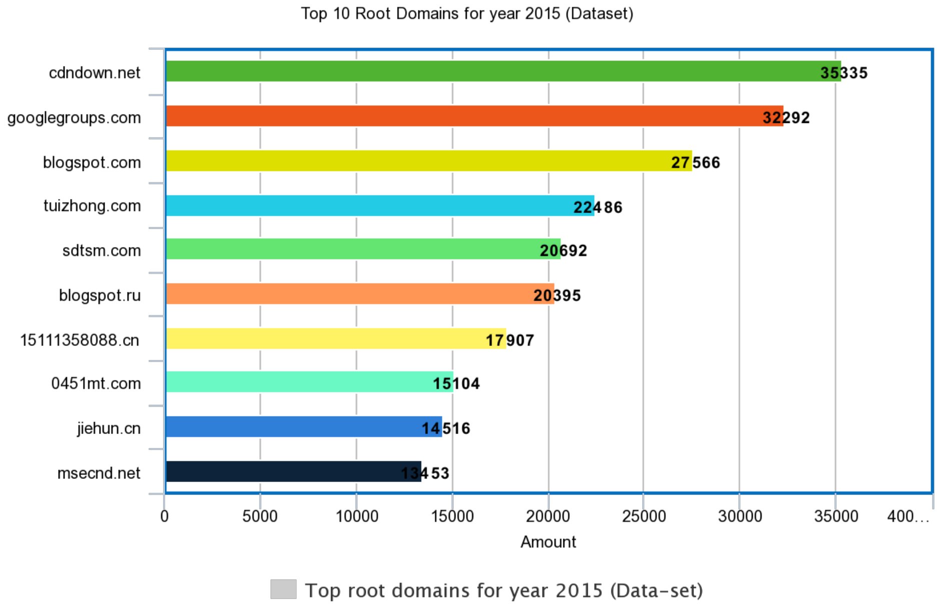

Figure 6: Top 10 domain count of 2015

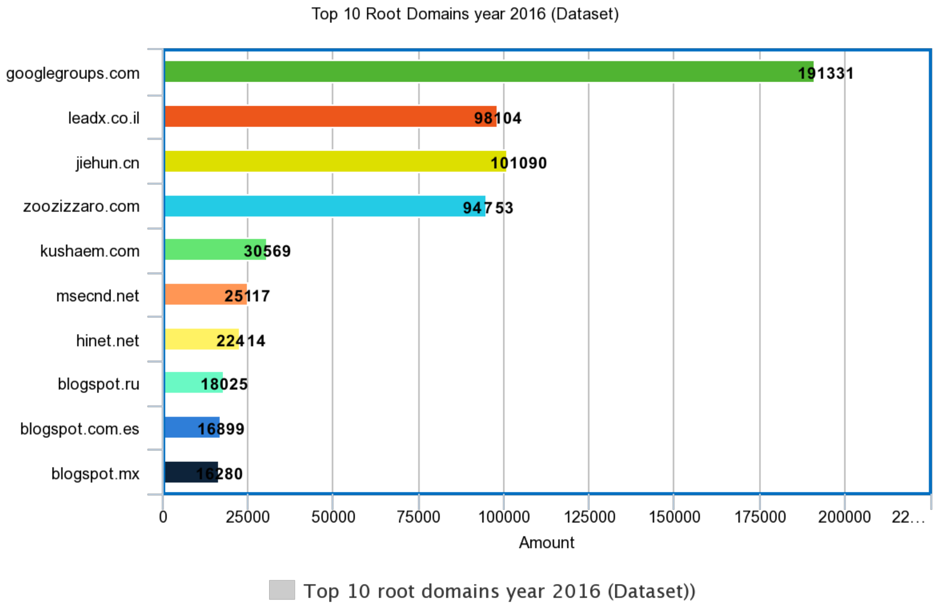

Figure 7: Top 10 domain count of 2016