WM0824TU Economics of Cybersecurity

Malware Droppers Assignment 3

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

October 15, 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/MZbaZ12fFOSD2QV`

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 malicous 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:
The main 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.

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.

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 bad publicity, which causes damage to the image of the organization.

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:
Again 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, as explained in the previous assignments, reveal the number of different times that particular domain was visited. A high frequency of a specific domain using this metric, reflects a higher success rate of that specific malicious link. This metric can be used to evaluate the performance of antivirus software. This is done by comparing the domain count of month i with month j. Month i is a month which contains several malicious links with high frequency. Month j is a later month in time. This month should contain a lower frequency of the domains compared to month i, because the antivirus should have made measurements to prevent organizations, individiuals or machines from reaching these links. Thus, the security performance of the antivirus software is visible.

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 fine 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. These can be for instance governments.

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

The variance in this 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 URL's posession. This list only reveals when a specific domain is visited. There is no knowledge on the specific Malware Dropper which is downloaded using that 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. This 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.

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 2004, the amount of malicious links is: 605098. The amount of links which are not by organizations are. Likewise the same data for the domains for may 2014 and june 2014 can be found. This results in the following table.

Month	Org Domains	Domains not by Org	Tot domains
April 2014	11C	22C	605098
May 2014	9C	19C	605098
June 2014	9C	19C	605098

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. A top 10 of malicious domains will be compared to the domain frequency of this top 10 in the next month. The top 10 domains for april 2014 can be seen in the following figure.

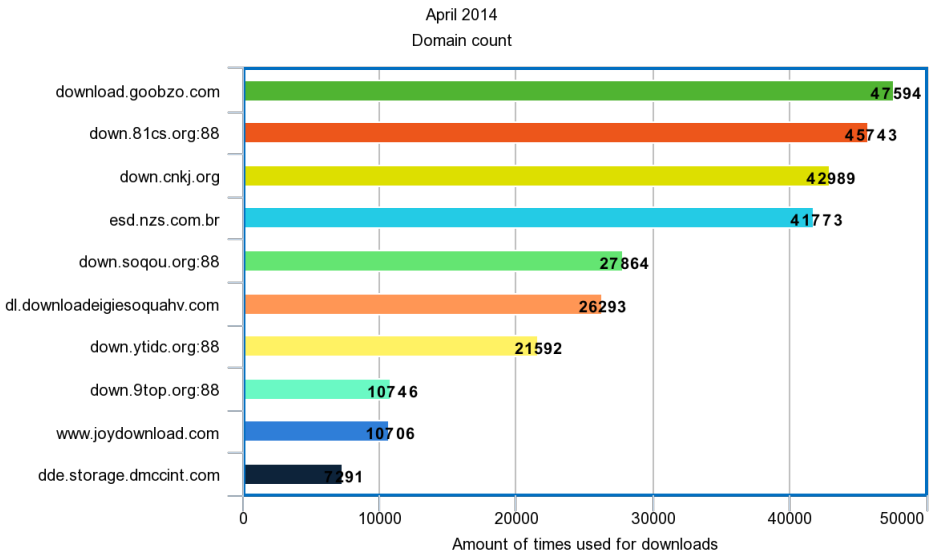

Figure 1: Top 10 domains used in April 2014

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

The odd a domain is from an organization is equal to the ODDS function as seen in the slides.

$$ODDS = \frac{P(SUCCESS)}{P(FAILURE)} \tag{3.1}$$

$P(SUCCESS)$ is calculated by the fraction of the domains being from organizations and $P(FAILURE)$ is the fraction which is not from organizations. We calculate the odds for the named months in the previous section.
April 2014:
May 2014:
June 2014:

4. Conclusion

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] 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.