WM0824TU Economics of Cybersecurity

Malware Droppers Assignment 2

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

October 8, 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. The internet is used in far greater proportions as it used to only a few years ago. This claim is supported by the growth rate of internet usage in some countries. [5]. This growth is not only positive. Cybercrime rates raise as well. [7] Cybercrime can be in the form of malware. Malware is a term used to describe malicious software where each piece of software can have its own negative effect. [12] This types of software need to be installed as well. Therefore Malware droppers come into place. Malware droppers are used to distribute malware into different kind of systems. [10] They are able to download these malware undetectable. This paper describes how to manage risks in case of malware droppers.

First, the problem owner will be defined. Second, security performances will be discussed out of some metrics of past data. Third, all risk strategies will be named. This is followed by all the actors related to malware droppers. After that, these actors will be combined with the different strategies in order to identify risk strategies which can be adopted to tackle the problem. Last, one of the strategies is picked and clarified. This includes a return on security investment.

2. Who is the problem owner of the security issue as measured in your first assignment?

Malware droppers are programs containing code, which when become active, download and install malicious software onto their hosts. In most cases they can be seen as trojans. The main problem here is the fact that people do not interact with these malicious links. In this case anyone or any machine with an internet connection is able to interact with these links. A problem owner is the one who is affected by the issues to be solved or indicates those who benefit from the solution [1]. The problem owner should prevent these users to interact with these links.

In our case we define the problem owner to be a private organization. Within companies, a person or a department should be designated to prevent its employees from clicking the malicious links. This department or person is able to implement firewall rules and therefore can be seen as problem owner for this problem within its company. These problem owners can also be designated within other organizations. This report focuses on problem owners being administrators who should prevent members of their organization from accessing the malicious links.

3. What relevant differences in security performance does your metric reveal?

In this section we take both the domain count, as-well as the url-count into consideration.

Domain count metrics, as explained in the previous assignment, reveal the number of different times that particular domain was visited. Clearly, a high value of this metric reflects the success rate of that particular malicious link. The domain count can be easily used to evaluate the security performance of an organization, however the Url-count is an even more intuitive measurement when it comes to a company's security performance.

Figure 1: Url count 2014

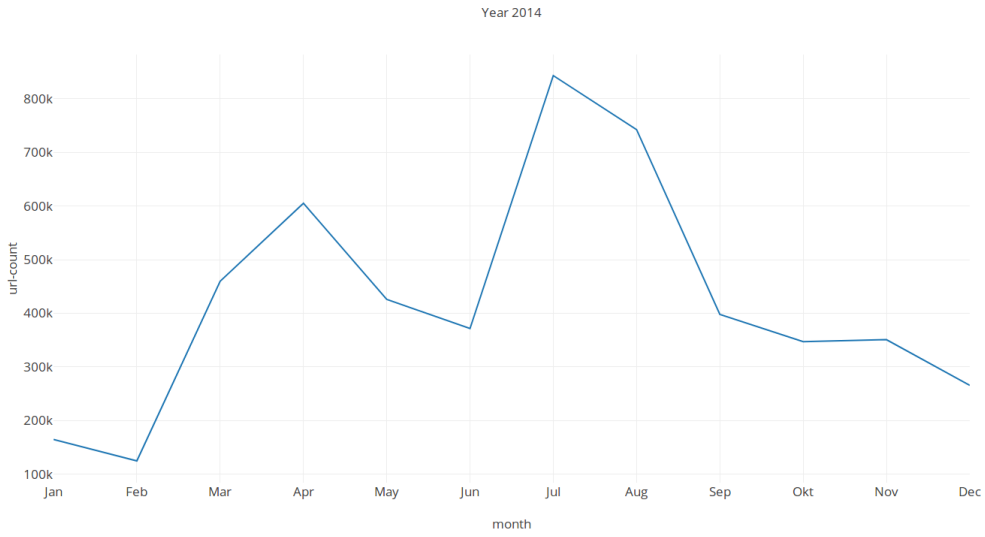
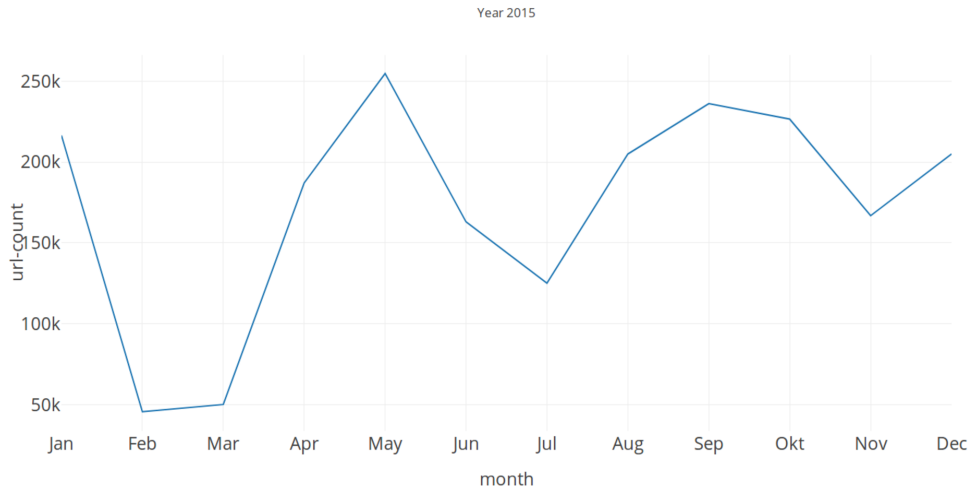


Figure 2: Url count 2015

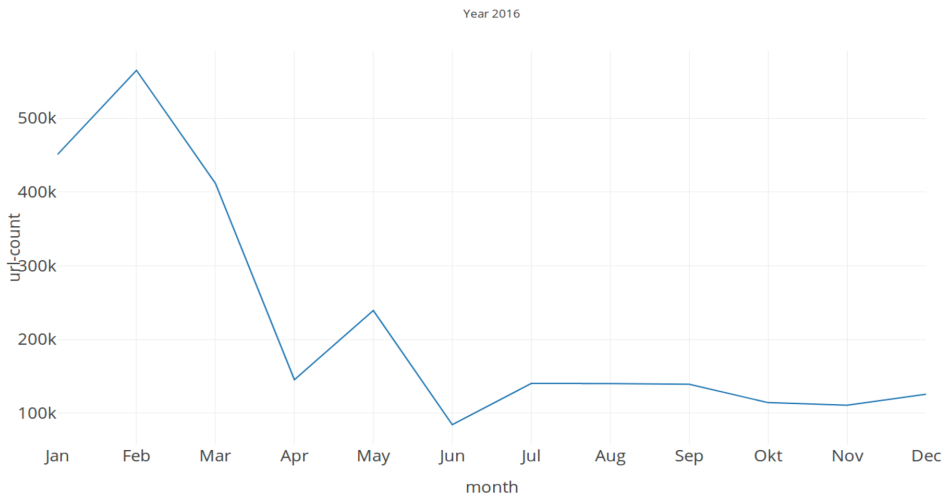


Consider a scenario, where a company has highly invested in an antivirus software to avoid these malicious domains. This metric can be used to validate the quality of this

software. If a certain domain or url is deemed not malicious by the antivirus software, it still can have a high url count which suggests that the antivirus is not doing its work.

In the above figures we can see that there is a very large decrease in the amount of malicious urls when comparing 2015 to that of 2014. When we look at 2016 we see an even larger decrease in malicious url's reported by our dataset.

Figure 3: Url count 2016



Thus, the above metric can be used as an extra validation tool to evaluate the security performance of an organization. Although, this largely depends on the quality of the url list provided in the dataset (and also on the attackers behaviour). As it is assumed to be our ground truth dataset.

3.1 Domain count insights

In the figures below we can see one of the elements of the evolving nature of malware droppers, by taking the url count of a single month april from three different years we see that the top 10 domain- urls are different. This shows that making risk strategies based on specific domains is not the solution. Domains differ, because attackers might have decided to place there droppers elsewhere. An other option is that the software has been confiscated by the authorities.

Figure 4: Domain count April 2014

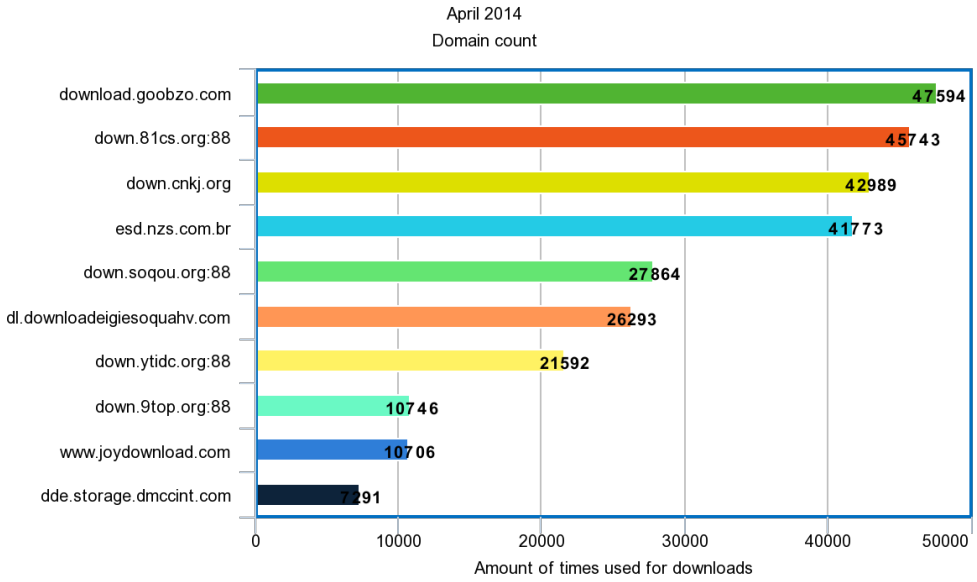


Figure 5: Domain count April 2015

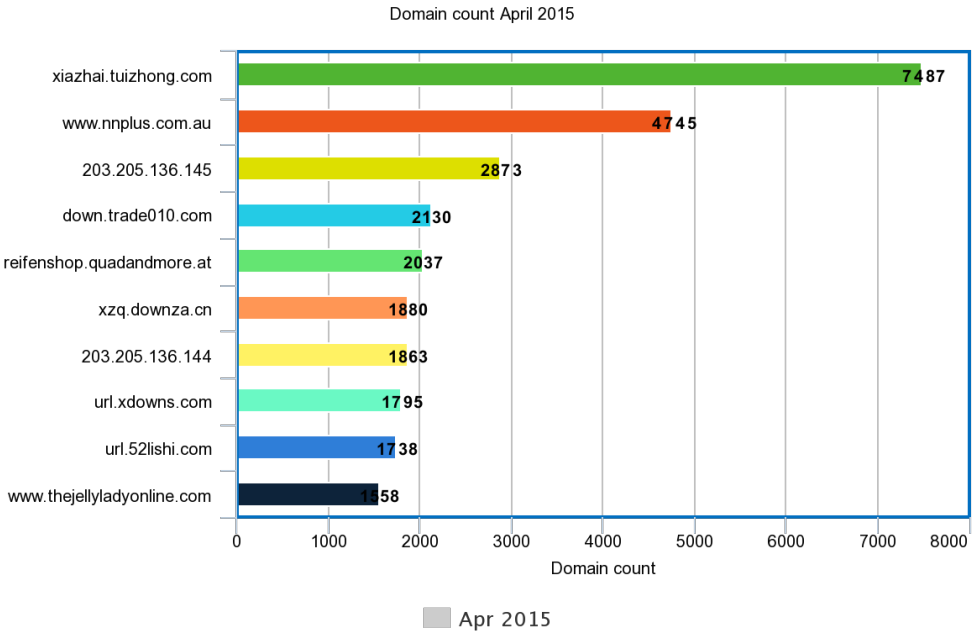
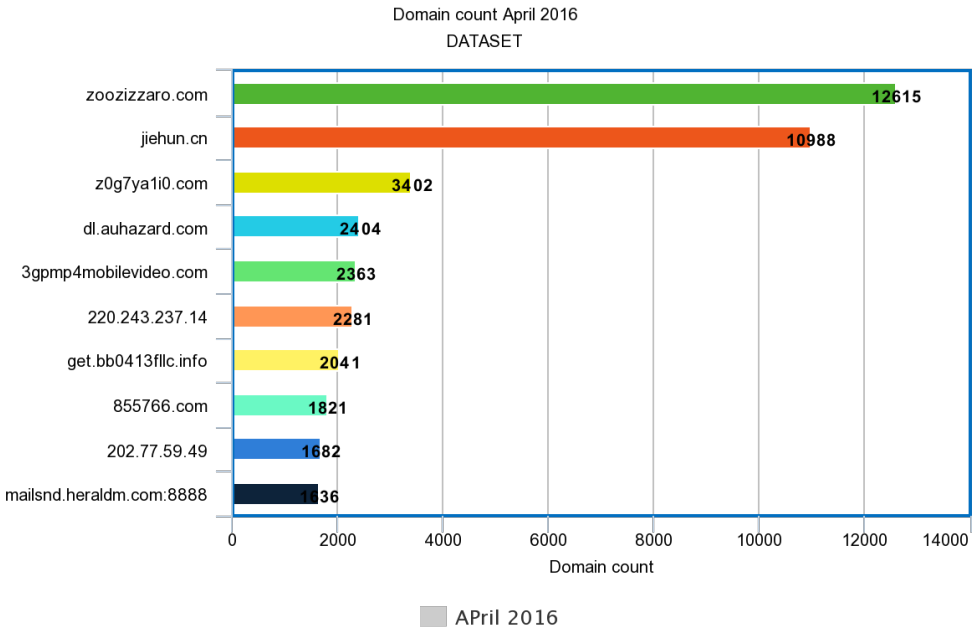


Figure 6: Domain count April 2016



4. What risk strategies can the problem owner follow to reduce the security issue?

Because we are dealing with a malware dropper it is not the user of the computer that is clicking the links but rather, a program (called dropper) that downloads the actual malware onto the computer. Risk management for malware droppers are less focussed on human error, because of this. Although, human error still comes in play. The management of risks can be differentiated into four different categories: mitigation of risks, transferring risks, avoiding risks and accepting risks. Many Malware-droppers can avoid detection due to the fact that the malicious code is hidden within a larger code-base of the program. They are relatively new and evolving in terms of their behaviour.

There are 4 major categories when it comes to strategy choices:

4.1 Risk Mitigation

Mitigation is a form of risk management in which the risk is mitigated. The impact of the risk will be lower once a mitigation is made. Mitigations which can be done in order to reduce the risk for malware droppers are:

1. **Invest in a quality antivirus**
   Good quality antivirus software can help users detect and ban malicious links thanks to its large database and algorithms used to detect malicious links.

2. **Update Frequently**
   It is a good practice to check your system daily for any malicious content. By daily updating your antivirus tool, it keeps the user safe from new and latest malicious links created recently

3. **Surf smart**
   Within a company, not everyone know how to use a computer properly. This can result in users surfing on websites which they should not be on. Thus, an organization can offer some sort of trainings to teach employees the basics of surfing cautious. This also raises their awareness of the risks available online. A paper by Kumaraguru et al.[9] showed that common real world training helped them in identifying phishing. This also implies to users which did not have a technical background. Phishguru, a tool which is used for training against phishing, helps identify phishing websites and prevents users from providing their information. Furthermore, it does not retain users on clicking valid mails. It has been shown that users retain knowledge from Phishguru even after 28 days. [8]

4. **Prevent users from clicking email links or attachments**
   This is the most common and important strategy as it is the easiest way to get in contact with a user. It is always strongly advised avoid clicking links that seems phishy.

5. **Monitor & Block Internet Traffic** Blocking known malicious websites helps against malware infiltrating the network and computers. Monitoring internet traffic inside the organization can help find suspicious behaviour of potential malware infected systems. This monitoring and blocking can be done by using firewalls and/or having specialized personnel doing it

6. **Investing in a firewall**
   It is worth to invest in a system fire-wall that blocks suspicious attempts originating from a program to download software without user's consent. [TODO –> add sources]

4.2 Transferring Risks

Transferring a risks means that a risk is taking care of by using external sources. [13] In this case an insurance can be taken for damage done by malware droppers. However, it can be hard to prove that damage has been done by malware droppers. Most of the actual damage are caused by the malware downloaded by the droppers. Another reason that a makes the risk transfer of droppers difficult is the fact that some droppers remove themselves after it served its purpose. This was the case with ***pushdo*** [2].

4.3 Avoiding Risks

One rigorous way of dealing with risks is avoiding them. As seen in the lecture, this will cost a lot of money. Furthermore, it is a really difficult task to detect a malware dropper.

This makes avoiding one even more difficult. Avoiding malware droppers is therefore (likely) impossible.

4.4 Accepting Risks

One could also accept the fact that malware droppers exist and that they are able to infect their systems. By accepting the risk, an higher proportion of systems will get infected by malware by the use of droppers.

5. What other actors can influence the security issue?

The actors associated to the security issue can be divided into four categories, which are: security providers, security consumers, security industry and attackers.

5.1 Security 'providers'

Security 'providers' can be seen as software developers who have aim to develop software. They make money by selling this software. One example of a security providers is: Microsoft. Microsoft provides the operating system which is used the most. The fact that Windows is the most provided operating system is also mentioned during the lecture. Other security 'providers' can are the companies who developed the other pieces of software needed for the specific security 'consumer'. One specific example of a security provider is the Internet Service Provider (ISP). As the name says, these companies make sure that people can have access to the internet. They sell this as a service and their main goal is to make money out of it. However, an ISP can also be seen as a security industry. Sometimes an ISP sells firewalls. They also are able to block certain IP addresses among users, so that they do not have access to them anymore. This provides a block to certain domains and IP addresses, which makes them a security industry as well.

5.2 Security 'consumers'

Security 'consumers' can be seen as the ones who need security. This include organizations like banks, but also individuals who use computers for their own personal needs. They rely on security in order to operate efficiently. Some security 'consumers' need security in order to not lose reputation. The competition relies on the same power of technology. There is no technological advantage among these companies.

5.3 Security "industry"

The security industry can be seen as the component who provides security to the security 'consumers' and to the security 'providers'. An example of the security industry are: antivirus companies. They sell their software in order to provide security.

5.4 "attackers"

1. **Professional criminals**
   As the term professional indicates, there is usually a monetary benefit behind these attacks. The attacks can be carried out in order to gain some private information that could be used for extortion or there is already a buyer who is willing to pay for that personal information. Other motives might include damaging the resources of the organizations in exchange of money. One famous example of this is WannaCry, where attacker would encrypt the victim's hard drive in exchange of Crypto Currency. [11]

2. **Terrorists**
   The main motivation of this group of actors is to create a social upset or imbalance, instead of monetary gain. As everything is moving online and is being controlled online, the role of this actor will get only more significant. It could also involve stealing secret information from various government organizations to gain useful insights.

3. **Cyber vandals and script kiddies**
   It refers to the amateurs who carries out basic attacks/small sized attacks with the use of widely available scripts and tools. It is mostly done to demonstrate their abilities or as a challenge or prank.

4. **Non-governmental organizations**
   Additionally, non-governmental organizations can create malware droppers in order to achieve their goals. One such non-governmental organization is Anonymous. [6]. The desire of Anonymous was to create a truly democratic system.

5. **Abuse Organizations**
   Some Organizations deliberately create malware droppers. These organizations create the malware droppers. One of the goals of these companies is making. They do this by creating droppers and selling them to third parties.

6. **Governmental Organizations**
   Some governments attack other governments by the use of malware. By doing this, they are able to achieve valuable information. Another goal is that they can harm other governments by installing malware on their systems.

6. Identify the risk strategies that the actors can adopt to tackle the problem

For malware droppers the risk strategies for actors can vary. The problem owners of different companies can have a different view on risk strategies. For example a tire company, which is a security 'consumer', decides to accept the risk. They never had any occurrence of a malware or were infected and did not notice any loss. For them it is not fruitful to

invest in security measurements for malware droppers, because the cost of damage done by malware droppers is likely lower than the security measurements against it.

However, not all the problem owners of all companies have the same strategy. For instance a bigger software company where its employees rely on excessive internet access which exposes them to all kind of malicious links and e-mails. This company rather does not want to accept the risk, because the costs of infections by malware droppers will probably be higher than the costs of mitigating them. They rather want to avoid or mitigate the risks than accept them.

Malware droppers are a rather new form of installing malware on systems. Because their only goal is downloading other pieces of malware, they are hard to detect by antivirus software. [3] Over time they have increased risks, because of their low detection rate and because they are a recent form of malware distribution, as well as their constant evolving nature. In order to reduce the risk, antivirus software should focus on detecting malware droppers as well.

7. Pick one of the risk strategies identified previously and calculate the Return on Security Investment (ROSI) for that particular strategy.

In order to choose a strategy as a security consumer, the budget is taken into account. According to Microsoft one in every 14 downloads from the internet has the probability of containing some form of malware. [4] This combined with the fact that most malware-droppers tend to disguise themselves as (part of) a legitimate non-malicious software, teaches company workers about click-bait and phishing emails. This also may prove to be less effective or insufficient when it comes to malware droppers.

For this reason we choose to incorporate a new anti-virus suite in the companies computer systems. This has the benefit of not only preventing infections but also notifying management of malicious attempts that were mitigated and alerting them on suspicious behavior.

The other benefit of this system is that it automatically reminds any user of the computer system to be cautious when opening there emails teaching them to practice caution even when the person using the system is a customer, guest or any other user that is not on the companies pay-roll.

7.1 Estimate the costs involved in following that strategy

7.1.1 Direct

The anti-virus chosen for this company requires installation and configuration costs (25 euros per computer) next to the default price [1] (45 euros per computer).

[1] https://www.avg.com/en-eu/business-security (not taking the temporary 20% discount into our calculation)

- Expenses for acquisition = $300 \times (25) = 7.500$
- Deployment = $300 \times (45) = 13.500$
- Maintenance = $300 \times (45) = 13.500$ / Year (after the first year)

The total costs c for year 1 in this scenario $c = (13.500 + 7.500) = 21.000$.

7.1.2 Indirect

It is expected for the anti-virus to slow-down certain business process due to routinely updating its database as-well as performing other relevant security updates that may require restarting computer systems or planning a more time consuming upgrade which may require scheduling maintenance day - periods.

7.2 Estimate the benefits of following that strategy (assume a particular loss distribution)

In order to estimate the benefit of this security investment; an estimate of the losses with and without the security investments might be required. However in order to do so one would need to know the amount of breaches that would occur and how many of these breaches would be mitigated if one were to invest in this new anti-virus system. However because this information was not known before hand we use a breach probability function in order to estimate the possibility of a breach. The breach probability may possibly be influenced by some of the previously defined variables such as cost and attacker behavior.

According to [] the average cost of cyber-crime globally per organization in the year 2017 is 11.7 million. However things may be different for this organization.

7.2.1 Attacker behaviour

In the current estimation the exogenous factor of the Attacker's behaviour is modeled as a random variable x.

7.2.2 Expected prevented loss

We now estimate the expected loss with as well as without the security investment. Because of the fact that there is possibility that no malware infection could occur, zero inflated loss distribution is assumed.

YEAR	avg urls/month
2014	424893
2015	173430
2016	222325

Table 1: Average malicious urls per month (based on dataset)

An overview of the average amount of malicious urls per month used by malware droppers can be found in table 1. The average in 2016 is significantly lower than in 2014 however it is the most recent one and also when looking at the graph depicted in figure 3 we see a more stable graph compared to figure 1 and 2 (where there seems to be allot more fluctuation in the amount of urls per month). For this example the year 2016 is used for estimating the expected amount of attacks per month.

Zero-inflated distribution is used with expected amount of incidents 222325 per month.

Here we define the Return On Security Investment formula as follows:

- $(expected-benefit)-(expected-costs)-(monetary-costs) = (expected-prevented-loss)$

Because of the stochastic variables in the ROSI formula we call this the expected prevented loss. A plot of the expected prevented loss can be found in figure [figure] (kan je dit nog even schrijven dat het inleverbaar is)

8. Conclusion

In order to manage risks for malware droppers, a problem owner should define proper risk strategies. The problem owners for this security issue are departments of private organizations. They try to prevent their employees or their systems from installing malware droppers. In order to do so the problem owner tries to invest in better antivirus software. The investment seems worth-wile for the first year because there is a positive expected benefit.

9. Discussion

Despite this security investment seems worth while investing, there is still room for some future work. More analytically tools to compare the investment should be considered. For example one could also use The Gordon-Loeb model in combination with the The breach probability. When using this method we can estimate how far the current investment may be from the calculated optimal Gordon-Loeb - level of security. Also the chosen method has the advantage that it not only deals with malware-droppers by itself but also teaches user's of the computers to practice so called 'skeptical browsing' where users learn to practice caution when browsing;

References

[1] C. Csáki. The mythical decision maker: Models of roles in decision making. In *Encyclopedia of Decision Making and Decision Support Technologies*, pages 653–660. IGI Global, 2008.

[2] A. Decker, D. Sancho, L. Kharouni, M. Goncharov, and R. McArdle. Pushdo/cutwail botnet, 2009.

[3] R. Fedler, J. Schütte, and M. Kulicke. On the effectiveness of malware protection on android. *Fraunhofer AISEC*, 45, 2013.

[4] J. Haber. Smartscreen application reputation in ie9, 2011.

[5] J. Iqbal and B. M. Beigh. Cybercrime in india: Trends and challenges. 2017.

[6] J. Jagodzinski. Anonymous: The occupy movement and the failure of representational democracy. *Journal of Social Theory in Art Education*, 33(1):21–37, 2013.

[7] A. Kigerl. Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review*, 30(4):470–486, 2012.

[8] 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.

[9] 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.

[10] B. J. Kwon, J. Mondal, J. Jang, L. Bilge, and T. Dumitras. The dropper effect: Insights into malware distribution with downloader graph analytics. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 1118–1129. ACM, 2015.

[11] S. Mohurle and M. Patil. A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, 8(5), 2017.

[12] P. K. Singh, P. R. Prashanth, and N. Jyoti. Dynamic cleaning for malware using cloud technology, Mar. 18 2014. US Patent 8,677,493.

[13] D. Spinellis, S. Kokolakis, and S. Gritzalis. Security requirements, risks and recommendations for small enterprise and home-office environments. *Information Management & Computer Security*, 7(3):121–128, 1999.