Economics of Cyber Security:
Botnet Tracker: Actors Involved and Security Strategies
Assignment Block 3

M. Kesteloo - 4291158
R.D. Meeuwissen - 4287150
P. Remeijsen - 4286243
B. Czaszyński - 4571984

October 8, 2018

1

INTRODUCTION

In this report we build upon the security issues and metrics that were defined in the previous assignment. The focus will be mainly on identifying involved actors, applicable risk strategies and evaluating their potential impact and cost. First, we will give information about specific problem which will be the center of this report, namely botnets.

A botnet is a network of computers, which control is taken over by a malicious actor and can be further leveraged by him for malicious and criminal activity. Botnet often serves purpose of executing distributed attacks, sending spam messages in bulk, hiding originator of malicious traffic by acting as a proxy, or spreading malicious programs to other computers. It is capable of acting in an automatic and autonomous way.

The dataset which was used in this report comes from online botnet activity trackers. These trackers monitor behavior of malware, such as the online status, infected domains/IP-addresses, and botnet Command & Control (C & C) servers. The trackers often provide lists of IP-addresses to allow companies to block malicious network traffic coming from a particular botnet, facilitating easy mitigation of the threat.

One of the larger datasets available from investigated trackers concerns ransomware. This particular type of malware holds data for ransom by means of encrypting it and disallowing anyone besides the key generating party (C & C server owner) access to the data. In order to coerce the victims into paying the spreaders of the ransomware, a victim is instructed that upon receiving a ransom payment, the key will be delivered to him/her and data can become accessible again. Like with a lot of types of malware, ransomware often spreads through Trojans. These are computer files that seem legitimate, but actually are capable of executing malicious activity on the victim's machine. Victims download malware either through a malevolent web application, email phishing or some other type of delivery scheme. Once ransomware is on the victim's computer, it activates and consequently encrypts data on that computer. Next, the ransomware notifies the victim that only the attackers have the ability to decrypt the data in order to recover its contents [1, 2]. The result is that the victims are left with the choice to pay, or consider the data to be permanently lost.

Ransomware is a significant problem with a very large number of victims and is certainly at the forefront of cybercrime. This particular tracker differentiates between three types of threats. The first type is C & C servers. These are arguably the most interesting as these are the servers that send commands to other nodes in a botnet. The second type are payment sites and the third are distribution sites. These are distinctions that other trackers often make as well.

In this report, we used a dataset that contains feeds from a ransomware tracker retrieved from `https://ransomwaretracker.abuse.ch/feeds/`. We chose to only focus on this dataset because the ZeuS dataset and Feodo dataset only had approximately 500 entries each while the ransomware dataset contains around 14.000 entries.

Section 2 states what the main security issue is and explains who the problem owner is and which other actors are involved. Section 3 elaborates on the metrics which are used to evaluate security impact. In Sec-

tion 4 a discussion is carried out on what types of strategies could be used by the problem owner and other involved actors to reduce the risk caused by the security issue. Section 5 evaluates the ROSI model for one of the risk strategies. Finally in Section 6 it is concluded how the metrics and risk strategies help to remedy the security issue at hand.

2

Security Issue

As already stated in the introduction, botnets sending out ransomware poses a serious concern to society. In the ideal case botnets should not exist at all. Although this is nearly impossible as there will always be ways to get systems infected by malware, the threat of botnets can be reduced. If a botnet is of a small size, it will not be able to send a lot of malware, so the potential threat it poses will also be smaller. The reduction of botnet impact, and consequently decrease of a potential threat, is the main security issue that is elaborated on in this research. This section discusses who the actors are and who the problem owner is for this security issue.

2.1. Involved Actors Security Issue

To remedy the security issue posed in this paper, we investigate which actors are involved in the problem of botnets distributing ransomware. There are actors who have a critical position in battling botnets and there are actors which are directly or indirectly affected by the issue. In this section all identified possible actors are discussed.

Internet Service Provider

The Internet Service Provider (ISP) is the supplier of internet service to customers, providing an access point to the world-wide network. They have an enormous market share on a national level. All packets of data, and thus also malicious data, which are transferred between the customers are routing through their systems. Many ISPs provide additional functionality like inspection of the traffic, classification of traffic type and disallowing access to certain parts of the Internet. Therefore they are directly involved in this security issue, due to handling and routing the malicious traffic.

Hosting Provider

In case the affected system is not owned by the direct actor but by a hosting provider, then the hosting provider is a direct actor as well. In most situations, people do not host their website on their own network infrastructure, but rather rent such services from a hosting provider. In some cases, the ISP is the same as the hosting provider or the registrar, but a hosting provider is considered to be a different entity in this report. A hosting provider is the literal owner of the IT-infrastructure that can be infected by malicious code.

Consumers

Other directly affected entities are consumers whose (rented) devices are affected through operation of a botnet. This group is basically why botnets can become so effective, as consumers are often not aware that their devices are compromised due to malware infection. By being unnoticed, botnets can grow more easily to bigger sizes. Of course, this actor can also be victim of the ransomware. Hence, parties who aim at providing certain functionality or operate a service on a compromised IT-infrastructure are considered another direct actor to the security issue.

Governmental Institutions

When looking from a national perspective, governmental institutions take a part in this issue as well. They use their regulation and legislation capabilities, as well as law enforcement to influence how entities interact

with the digital world (recent introduction of privacy laws in GDPR[1]. If companies do not follow the law, they can be prosecuted by the government. Through such measures, governments can create new laws to help reduce the threat coming from botnets, and thus of ransomware. In the light of the research, governmental institutions are considered indirect actors, due to their potential impact on operations of direct actors.

EDUCATIONAL INSTITUTIONS

Many educational institutions host their own networks, frequently composed of large set of machines being an attractive target for botnet herders. For example a famous and large international network is Eduroam, currently available in 90 countries and launching pilot implementations in another 26. This is like any other ISP a possible internet supplier that could contain parts of a botnet. Though the networks of educational institutions have much less users than large ISPs, from user's perspective they provide for a similar functionality, hence becoming another indirect actor.

2.2. PROBLEM OWNER

Considering machine infections turning computers into nodes in a botnet network, the problem owner has been identified as the hosting provider. The main task of a hosting provider is to maintain a reliable IT-infrastructure which can be rented to third-parties willing to host any type of functionality online. Responsibilities of hosting providers are hence in ensuring uninterrupted delivery of online machines and timely and correct execution of tasks the infrastructure was designated to perform. Given a breach of security perimeters of a hosting provider has happened and many of its machines becoming infected, guarantee of desired functionality can no longer be granted. Without proper inspection mechanisms and security monitoring, it is this actor's infrastructure which functionality has been hijacked, is carrying out tasks which it is not contractually agreed by its clients and was never designated by the owner to perform. Aiding a cyber-criminal activity is illegal, but it is hard to put the responsibility on the hosting provider because they might not be aware of their customers' desired behavior.

Hosting providers do have direct incentive for stopping botnets. The main source of income comes from reliable online services the clients subscribe to. Additionally, hosting providers can incur direct financial losses, due to botnet operations. Revealing that infrastructure rented by clients is controlled by a malicious third-party can cause many of them to leave in favour of another, more secure hosting provider, guaranteeing reliable operation. Another incentive for addition of more security measures to a hosting provider might be that single infected machine may cause other machines of the same hosting provider to get infected as well due to ease of access and often similar access control measures. This can cause severe incident recovery costs, further loss of customers and irreparable reputation loss. Finally, according to a research by Fryer et al.[3] hosting providers are in one of the more promising positions to deal with botnets, due to direct physical control over the affected infrastructure.

[1] General Data Protection Regulation. Found on: gdpr-info.eu/ can serve as an example of such influence.

3

METRICS

In this section we use one of the metrics that was defined in the previous report to investigate a relevant difference in security performance. We have chosen to focus on the metric describing which registrars are relatively often associated with malicious behavior. The metric shows the percentage of infected domains for each domain registrars in the dataset. It would make sense that a larger registrar has more malicious behavior in their network because the chance of infection is bigger when there are more possible victims. For this reason we have to check percentage of infected domains per registrar instead of just counting the total amount of infected domains per registrar. The result is that hosting providers can see which domain registrars are often involved with malicious behavior. If one registrar turns out to be affiliated with cyber criminals, hosting providers can for example increase monitoring on websites registered by such a registrar or by completely blocking it. From the dataset, we only included the registrars with more than 100 infected domains in the dataset as these have a more reliable size to compare than the smaller sizes.

The website *Registrarowl*[1] was used to get the size of every domain registrar which is used to calculate the percentage. It should be noted that such a public source for the data is not ideal considering the data is always several months old and the collection is not completely accurate. Furthermore, the entries in the dataset are mostly from 2016 and 2017 and we retrieved the data from *Registrarowl* in September 2018. However, due to there not being other convenient sources, we have chosen to settle for this.

The relevant difference in security performance this metric reveals, is that not all registrars are equally involved with malicious sources. Using the dataset and the domain registrar sizes retrieved from *Registrarowl*, we can reveal whether certain domain registrars are often involved with malicious behavior. With this metric, the hosting provider can then decide to take counter measures. Like we have discussed above, they could for example stop hosting websites which have bought the domain name from a certain registrar or increase monitoring. They could also simply accept the fact that certain registrars are more often linked with malicious behavior than others.

In Figure 3.1, the percentage of infected domains is shown based on the data from *Registrarowl* and the ransomware dataset. The x-axis is shown in log-scale as a response the skewness of the resulting values of the graph. It is clear that the domain registrar *Paknic (private) limited*, based in Pakistan, is the domain registrar which is linked to malicious domains most often in terms of percentage: almost 8 percent of the total domains using this particular domain registrar are malicious. It is interesting to note that *Paknic (private) limited* has a very small market share: around 4000 domains are registered by this domain registrar. In comparison, *GoDaddy.com* has the biggest market share with 60 million registered domains, but, the metric used reveals that only 0.002 percent of the domains registered via *GoDaddy.com* are malicious. With these market shares in mind, it might not make a lot of sense for the hosting providers to actually take measures against these particular registrars.

[1] http://www.registrarowl.com/index.php

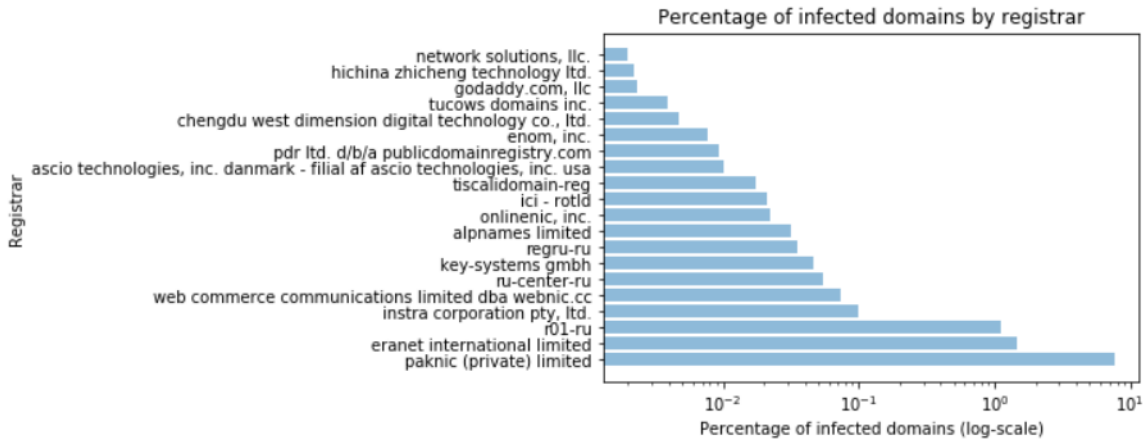

Figure 3.1: Percentage of domains infected per registrar (log-scale).

4

RISK STRATEGIES

In this chapter we will discuss the risks involved in a particular scenario that affect the chosen problem owners: the hosting providers. First, we need to define risk. Risk is the probability of an incident happening times the impact of such incident, for instance a damage or loss on the expected performance of a system or product, considering a chance of such event. This definition suggests that the problem, or security issue, can be described in 4 different ways:

- **Threat**: What is it that can actually happen to the system or actor in general?
- **Impact**: What are the financial or operational consequences of the threat and how bad is it?
- **Frequency**: How often can or does the threat actually happen?
- **Certainty**: How accurate are the estimates for the cost and frequency?

Next, we will explore what this means for the problem owners and other actors.

4.1. GLOBAL STRATEGIES

There are a number of global strategies that enable decision makers to manage the risks that are relevant to their particular scenario.

- **Risk mitigation:** This would mean actually doing something to take away the risk. In the case of a hosting provider this would mean mitigating the risk of being used to host a botnet. One possible strategy could be investing in advancing the monitoring capabilities of the network that they operate. Being able to detect more botnets could result in reduced risk.
- **Risk acceptance:** Sometimes the actors do not have a tool or policy to deal with the threat, or at least not an economical one. For example, hosting providers may simply choose to do nothing because it may not be in their best interest. This usually happens when there is no benefit for the actor when investing in security.
- **Risk Avoidance:** When the actors cannot mitigate or accept they could avoid the risk altogether. This is often done by selling the part of a business that has a high risk. However, hosting domains is usually the major part of a business and for hosting providers it is their only business. Avoiding risk is thus not feasible for hosting providers.
- **Risk transfer:** This entails an agreement with a third party, like an insurance company, to take over the risk. However, cyber insurance is still an immature business and it has to changes continuously because cybercrime also changes very fast. Therefore, this option can be taken into consideration, but the costs will probably rise very quickly.

4.2. RISK STRATEGIES FOR THE PROBLEM OWNER

As stated earlier, the owner of the problem discussed in this paper are the hosting providers. To reduce the risk posed by the problem at hand, the hosting providers can use multiple strategies. Whether they have the right incentives remains a question as we have discussed in Section 2 However, according to Fryer et al.[3], they have a promising position to deal with botnets.

MONITORING

The hosting providers are the ones providing the physical machines and operating systems to customers, often many customers at a time. Customers pay a fee to the hosting provider in order to gain access to a part of that physical machine. This means that hosting providers are in a great position to use software for monitoring the files that are being uploaded to their machines and if they find known malicious code they can for example stop hosting the site until the malicious code is removed. This can be seen as risk mitigation.

FIREWALLS

The goal of hosting providers' customers is to get people to visit their website and this involves network traffic. Firewalls can be used to block network traffic from known malicious hosts. However, the list of those hosts should be kept up-to-date because otherwise the control strength degrades over time. This can also be seen as risk mitigation.

ACCEPTANCE

Finally, hosting providers could also simply accept the risks. They get paid for hosting, not for providing security to the people visiting websites hosted on the hosting providers' machines. However, in the future, governments might create new laws in which they can be held responsible. Furthermore, hosts can also be attacked by botnets: if a hosting provider is hit by a DDoS attack, they are not able to keep the websites of their customers available. Depending on the contract, this could cost them money or will have a negative impact on their reputation.

4.3. RISK STRATEGIES FOR OTHER ACTORS

In addition to the problem owner, there are other actors in this scenario that could take actions to limit the negative impact of the threat. First we will discuss some strategies that all these actors could take. Afterwards, we will discuss what strategy each of the actors mentioned in Section 2 can follow.

BACKUP

One of the things that actors can do is making regular back-ups. Doing this often enough will ensure that there is little data loss when their files get encrypted. Home users do have to keep in mind that when creating a backup on a physical hard-drive, then this should be disconnected because otherwise the files are still susceptible for infection. This can be considered as a risk mitigation.

ANTI-VIRUS

Another option is to use anti-virus software. Even when an actor makes a mistake of clicking on an email link that they should not have, anti-virus software might be able to detect the malware in time before it can do damage. Of course, the percentage of risk mitigated is heavily dependent on the detection rate of the anti-virus software and whether it is up-to-date or not.

UP-TO-DATE SOFTWARE

Similarly, keeping ones software up-to-date ensures that there are as little vulnerabilities as there have to be. In addition to the software vulnerabilities, new updates might also add never known malicious parties to white- or black-lists, which in turn decreases the probability of exposure to malware sources. However, a new update is not always safer than the last version of the software because a new version might bring new vulnerabilities into the picture.

FIREWALLS

Like we discussed above, firewalls can be used to block network traffic coming from malicious hosts. This strategy could be used by other actors as well.

Last Resort

If prevention from getting infected failed, and a botnet is carrying out an attack, there are limited options left. The last option is shutting down all devices connected to the internet. Of course, for most actors this is disastrous. For example, an ISP shutting down means no one has access to the internet anymore.

4.3.1. Home Users

Home users are not only the most numerous, but arguably the most vulnerable targets. This is mainly due to the fact that there are countless individuals who are not up-to-date on the technical side of things and cannot determine for themselves that something is off. The strategies for this actor have already been explained above.

4.3.2. Enterprises

Another type of actor that could be targeted by botnets are enterprises and governments. Enterprises might be the preferred targets of cyber criminals, considering that there is often more money to be made compared to targeting individuals. This also means however that the security often is better as well, making it harder for the criminals to actually exploit any vulnerability and getting the target to pay.

White-listing Applications

One of drawbacks of the enterprise is that there are often many people working on the same network. It is hard to check whether any of those individuals are using applications that they should not be using. One solution could be the white-listing of applications, so that you can have one person responsible for approving the use of a certain application on the network.

Enhanced Mitigation Experience Toolkit

The EMET is a tool which is used to prevent that unpatched vulnerabilities are used in the Windows operating system. It can mitigate the vast majority of the attacks from exploit kits by protecting against software vulnerabilities that are not patched yet or for which no patch exists at the moment. These are known as zero-day exploits.

Email Filtering

Nowadays, there are more and more ways to make emails look as legitimate as possible. Cyber-criminals can use emails to send malware via the attachments in an email or by simply misleading people to click on a link which is in the content of the email. Because of the many ways of misleading, there are so many people that could accidentally open malware, it is a smart idea to filter or block emails that have certain file types attached, such as: .js, .bat, .exe etc. or which contain a link to known malicious domains.

Awareness Training

Another strategy for companies to reduce the risk is making customers and employees aware of the risks of certain actions on their systems. Unfortunately not all intrusions can be prevented by tools. Social engineering attacks can in many cases bypass any security tools that are in place. Social engineering is making use of malware disguised as something familiar to a user such as an attachment to an email. Whenever the user interacts with it, the system in use can get infected. Making users aware of social engineering techniques can help them recognize it which reduces the risk.

4.3.3. Governments

In fighting cybercrime, governments can play a crucial role. Governments could use the risk strategies for enterprises as well, but they have another strategy which we will discuss here.

Creating New Laws

Cybersecurity is an immature field and there are not a lot of laws regulating cyberspace. In the future, when the threats are more clear to the general public, they might have to create new laws in order to regulate cyberspace. These laws might for example enforce ISPs or hosting providers to do what they can in shutting down malware or make individuals responsible for the security of their devices.

4.3.4. ISPs

Like hosting providers, ISPs are in a promising position to take measures against botnets. They have access to all network traffic on their infrastructure. Analyzing this data is of course privacy sensitive.

NOTIFYING INFECTED CUSTOMERS

ISPs are in a position where they can easily see all network traffic, so they are also able to see malicious traffic if it is recognized. When a malicious C & C server is connecting and sending malicious traffic to a customer, the ISP can notify that customer. This has some downsides: the average customer might not be able to actually remove the malicious code from his/her device or they might decide to not do anything with the notification.

5

ROSI

In order to get a better overview of the costs and benefits of possible solutions for the problem, it is worthwhile to make a Return on Security Investment (ROSI) calculation. This is a tool used to compare strategies and clarify whether the investments will be recovered through the avoided losses. To give an example of such a calculation, we will focus on a medium-sized enterprise. Because the provided datasets do not grant us any insight into the ability of companies to detect whether they are in a botnet or not, we have chosen to focus on ransomware. As an example, we will take a medium-sized enterprise with 200 employees using roughly 200 machines, that is attempting to mitigate the ransomware threat by investing in anti-virus software[1]. This is one of the strategies discussed in Section 4.3. We have chosen to make it more specific because calculating ROSI for an actor like "all enterprises" is very hard to do, because of the intricate differences between any two enterprises. One of the most important weapons in the defenders arsenal is anti-virus software. There are the standard cost associated with such a tool:

- **Direct cost:** acquisition, deployment and maintenance.
- **Indirect cost:** productivity loss, opportunity cost, cost of decisions with incomplete information.

By performing the ROSI calculation in the next sections, we will gain insight into the utility of this strategy and provide actionable information to the theoretical decision makers.

5.1. What The Data Tells Us

When looking at the ransomware dataset, we can see that the most prevalent ransomware in the dataset is Locky, see Figure 5.1. Locky is a specific ransomware variant that was released in 2016. It was often delivered by email and claimed to be an invoice for a payment. Then, through social engineering, it would get the victim to download the actual malware that encrypts the data of the victim. It gained notoriety through a massive attack on a hospital[2]. Due to this malware type being the most common in the dataset as well as being an example of malware with well-documented statistics, we have chosen to use this malware as the focus of the risk analysis.

5.2. ROSI Equation

It is difficult for security decision makers to decide on where to invest. A good way of making a decision is by using the return on security investment (ROSI) calculation[4]. It is a method of determining whether a set of proposed security measures can be cost effective. ROSI can be estimated using the following formula:

$$ROSI = \frac{Risk\ Exposure * \%\ Risk\ Mitigated - Solution\ Cost}{Solution\ Cost} \tag{5.1}$$

where *"risk exposure"* represents the costs of getting exposed to the ransomware which also includes costs

[1] Source: https://ransomwaretracker.abuse.ch/mitigation/
[2] Source: https://www.nbcnews.com/tech/security/big-paydays-force-hospitals-prepare-ransomware-attacks-n557176

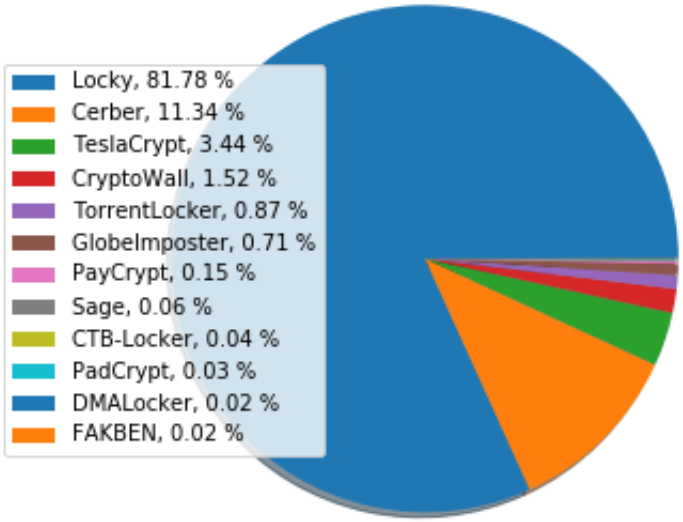

Figure 5.1: Percentage of type of malware

like reputation costs, productivity loss, etc. The *"percentage of risk mitigated"* is how much of the risk is getting mitigated by using the proposed solution or in other words how much money you will save by using the solution. The *"solution costs"* does not only contain the acquisition cost of the solution, but also implementation/maintenance of the solution and possible productivity loss caused by the solution.

Another equation which gives the same result, is the following formula:

$$ROSI = \frac{ALE_0 - ALE_S - C}{C} \tag{5.2}$$

Here ALE stands for Annualized Expected Losses. It is an impact of particular event multiplied by the probability of its occurrence. ALE_0 represents the ALE without the security measures in place and ALE_S represents the ALE with the security measures in place. The variable C represents the costs of the control on an annual basis.

5.2.1. CALCULATING ROSI

In calculating ROSI, the following steps should be taken:

1. Determine the expected impact of an incident.
2. Determine the likelihood of the incident occurring.
3. Use the expected impact and the likelihood to determine the risk exposure.
4. Calculate the costs of investing in the control for the specified time frame.
5. Determine the effectiveness of having the control in place.
6. Calculate ROSI by using either formula 5.1 or 5.2.

DETERMINING THE IMPACT

It is hard to determine the exact impact, so we estimate the impact by looking at different statistics retrieved from cyber security websites. We have determined that the lower bound of the impact is 500 euros because the average ransom asked is around 0.5 - 1 Bitcoin in 2016 which had a value between 1.000-2.500 euros. The upper bound is more difficult to determine. We assume that 10 % of companies affected are asked to pay a ransom higher than 5.000 euros[3]. There is one extreme case reported by Fox News: a South-Korean enterprise

[3]Source: https://www.comparitech.com/antivirus/ransomware-statistics/

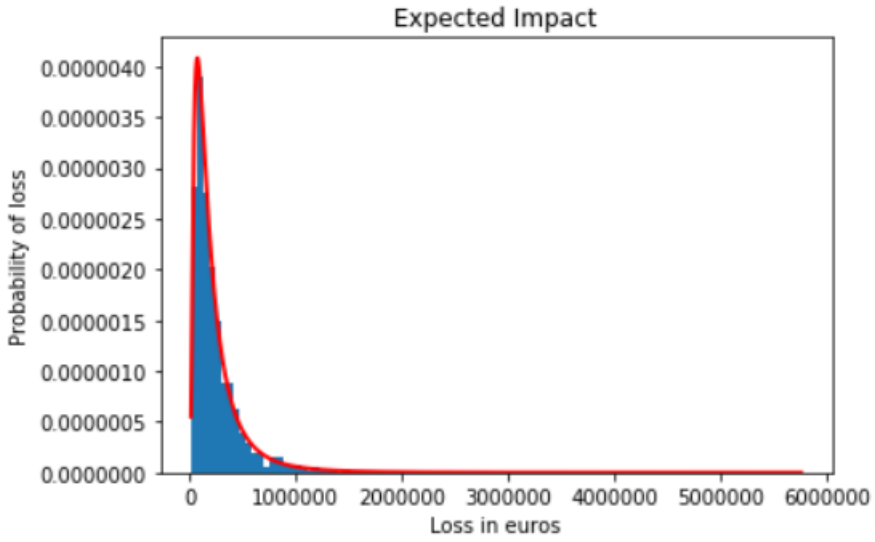

Figure 5.2: The expected impact of an attack on the enterprise

was hit by ransomware and after negotiating with the criminals, they paid 1 million dollars in Bitcoin to get their files decrypted[4]. This however, does not happen very often. Furthermore, a survey under CEOs showed that most CEOs are willing to pay between 20.000 and 50.000 euros to regain access to their data[5]. Based on all the above, we assume that we have a 90% confidence that the ransom is between 1.000 and 50.000 euros. Furthermore, there is productivity loss when the 200 employees are not able to work. This cost is assumed to be around 10.000 euros per hour which is around 50 euros per employee per hour (based on average project cost per hour). According to Intermedia [6], 96% are down for at least one day, 32% at least five days and 17% at least 10 days. Based on this, we assume the costs due to loss of productivity will be between 60.000 and 800.000 euros with a **90% confidence**. This means we have a **lower bound** of approximately **60.000 euros** and an **upper bound of 850.000 euros**. With all this information, we can create the expected impact distribution that will approximately look like Figure 5.2.

Determining the Likelihood

The likelihood of an attack will, according to some sources, decrease in the coming years because cyber criminals will move on from quantity to quality. This means they will target vulnerable but high quality victims more often[7]. However, there are also cybersecurity experts which predict that there will be a huge rise in the number of attacks. One way or the other, this company might be a high value target for cyber-criminals, but to really get this knowledge, we should create an attacker model. This is out of the scope of this report, so we will base the likelihood on the numbers of previous years. The reported percentages of attacked enterprises vary a bit, but they are around 25%.

Risk Exposure

The exposure to risk is defined as the product of the magnitude of the loss and the frequency of those losses. These are the quantities that we have determined in the previous sections. By using the upper and lower bounds of the impact we calculate that the lower bound of the risk exposure is 15.000 euros and the upper bound is around 200.000. The risk exposure distribution will approximately look like Figure 5.3.

Costs Of Investment

A cost of the investment comes down to purchasing a software license for each machine belonging to the network. The cost of such a licence for anti-virus products that will be the subject of this analysis comes down

[4]Source: https://www.foxnews.com/tech/ransomware-attack-costs-south-korean-company-1m-largest-payment-ever
[5]Source: https://assets1.dxc.technology/security/downloads/DXC-Secuity-Ransomware_To_Pay_or_Not_to_Pay_White_Paper.pdf
[6]Source: https://www.intermedia.net/report/ransomware
[7]Source: https://securityintelligence.com/are-ransomware-attacks-rising-or-falling/

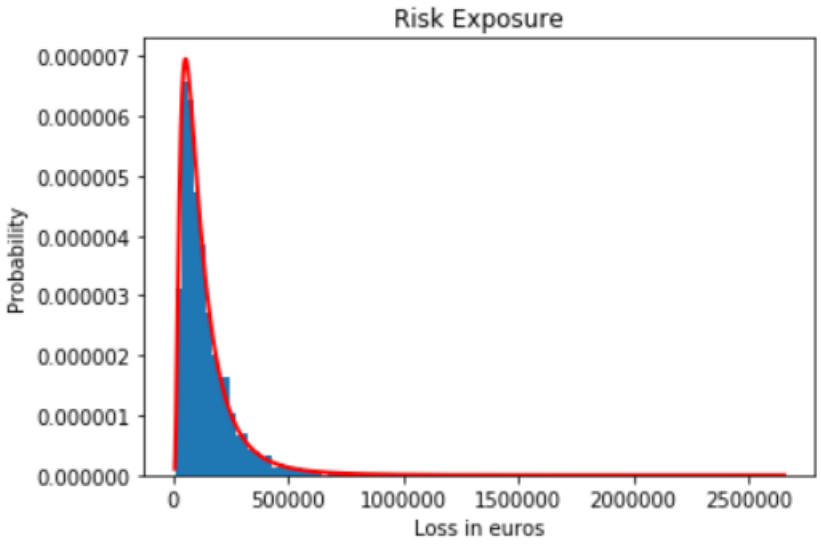

Figure 5.3: The risk exposure: a product of likelihood and impact.

to around 30 euros per year per machine [8]. Considering there are 200 machines in our scenarios, this will add up to 6.000 euros each year. Besides the primary costs of the licence, there are also complementary costs such as the cost of productivity loss due to the anti-virus software slowing down the machines. Additionally, the anti-virus software will generate false-positive alarms, flagging legitimate software and files as malicious content. This forces the employees to waste time using other solutions to send attachments, share files and deal with consequences of false alarms. Finally, both installing and updating the software will also cost time and money. We will consolidate these extra costs into a single cost for productivity loss of about 20.000 euros per year. This includes work time of a network administrator that has to extensively test the new update. This work time is approximated to be 90 hours[9]. The **total cost** that we will use in the following calculations is thus **26.000 per year**.

CONTROL EFFECTIVENESS

The effectiveness is always dependent on the software being up-to-date and the providers of the software keeping up with the latest developments in the malware detection research. The extend to which these companies are able to achieve this, together with the quality of the software determine how much of the threats can be repelled. Due to the nature of anti-virus software, it is hard to reach specific conclusions. The best the industry can do is regular benchmarking tests of the top contenders in the market, such as the Business Security Test 2018 by AV-Comparitives[10]. The top contenders seem to achieve protection rates between 95% and 100%, with varying rates of false positives. We have to keep in mind however that the database of malware that is used to run these tests are the ones that are already known. For example, research by Zhou et al. tested some software for security on Android [5]. The results showed that, in the worst case, only 20% of the malware could be detected. Therefore, we will show a negative scenario where the risk is only mitigated by just 20% and one positive scenario where 95% of the risk is mitigated.

ROSI

Now that we have calculated all the factors of the ROSI calculation, we can use the formula to determine what kind of return we are looking at when considering the anti-virus strategy. For both the scenario in which 20% of the risk is mitigated and the scenario in which 95% is mitigated, we have the following numbers for which we will derive the ROSI:

- The lower bound of the risk exposure is 15.000 euros
- The average risk exposure is 100.000 euros

[8] Source: https://www.techradar.com/news/best-antivirus
[9] Source:https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/lower-IT-costs-through-better-anti-virus-99-en.pdf
[10] Source: https://www.av-comparatives.org/tests/business-security-test-2018-march-june/

- The upper bound of the risk exposure is 200.000 euros

This means that for the negative scenario, formula 5.1 will be equal to:

$$ROSI = \frac{Risk\ Exposure * 0.2 - 26.000}{26.000} \tag{5.3}$$

And for the positive scenario:

$$ROSI = \frac{Risk\ Exposure * 0.95 - 26.000}{26.000} \tag{5.4}$$

This means that for the negative scenario, we get:

- A lower bound on the ROSI of -0.88
- An average ROSI of -0.23
- An upper bound of the ROSI of 0.54

For the positive scenario, we get:

- A lower bound on the ROSI of -0.45
- An average ROSI of 2.65
- An upper bound of the ROSI of 6.31

As we can see, the range is quite big. This illustrates the difficulty of calculating the ROSI and the difficulty for decision makers to invest as efficiently as possible. The key insight that is illustrated with this example is that the gathering of accurate information regarding the factors of the ROSI calculation is the most important. If an actor does not have sufficient insight into the costs and benefits of a certain strategy, then the evaluation yielded holds limited value.

6

Conclusion

In this report we have investigated who the actors are in a ransomware incident scenario and have given an analysis of the security issue. We learned that besides the problem owners, there are a number of parties who all have their own interests and their own strategies to mitigate their risks. In the metrics sections, we showed that by using certain metrics one can identify a difference in security performance. Next, we learned that the issues can be described along multiple lines, such as threats, frequency, impact and certainty. Similarly, there are global strategies that can be used to deal with risk, such as mitigation, acceptance, avoidance and transfer. We also discussed a number of strategies for the actors involved. Lastly, we took the example of the anti-virus strategy for an enterprise to calculate the ROSI. We learned that whether an investment is worth it depends greatly on the loss distribution.

BIBLIOGRAPHY

[1] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, *Cutting the gordian knot: A look under the hood of ransomware attacks,* in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (Springer, 2015) pp. 3–24.

[2] X. Luo and Q. Liao, *Awareness education as the key to ransomware prevention,* Information Systems Security **16**, 195 (2007).

[3] H. Fryer, S. Stalla-Bourdillon, and T. Chown, *Malicious web pages: What if hosting providers could actually do something...*, Computer Law & Security Review **31**, 490 (2015).

[4] W. Sonnenreich, J. Albanese, B. Stout, *et al.*, *Return on security investment (rosi)-a practical quantitative model,* Journal of Research and practice in Information Technology **38**, 45 (2006).

[5] X. Jiang and Y. Zhou, *Dissecting android malware: Characterization and evolution,* in *2012 IEEE Symposium on Security and Privacy* (IEEE, 2012) pp. 95–109.