Assignment 2: Security Investments
WM0824TU Economics of Cybersecurity (2019)

Brennen Bouwmeester, Hsin Cheng, Kevin Su, and Jochem Vlug

Group 5 (DDoS), Delft University of Technology

Abstract. This paper researches the different reactions by different actors on the risk of Distributed Denial of Service (DDoS) attacks. By looking at the possible ways to deal with risk, it can be explained why the problem exists and therefore what can be changed to solve the problem, or at least improve the situation. The Return on Security Investment (ROSI) will be used to calculate the risk mitigation strategy by Hosting providers.

Keywords: Distributed Denial-of-Service (DDoS) · Booter · Security Investments · Return on Security Investment (ROSI)

1 Introduction

Distributed Denial-of-Service (DDoS) attacks are considered the top operational threat in the cyber landscape (Holl, 2015; Cheung, 2017). These types of attacks overload the capacity of the target service or its surrounding infrastructure through a flood of illegitimate traffic, aiming to disrupt normal traffic and make the system unavailable for users. Disruptions resulted from DDoS attacks have caused millions in revenue losses, reputation damage, and customer attrition to many industries (Cardoso de Santanna, 2017; Chromik, Cardoso de Santanna, Sperotto, & Pras, 2015; Cheung, 2017).
Even though DDoS attacks have been around for a long time, the emerge of *Booters*, or *DDoS-as-a-service* or *DDoS-for-hire* – along with the use of amplification technique – has deteriorated the DDoS attack problem not only in the attack frequencies but also in attack power (Cardoso de Santanna, 2017; Noroozian et al., 2016). Nowadays, people are able to buy DDoS attack services with very affordable prices at the Booter websites, which are easily reachable through popular searching engine such as Google and Bing (Cardoso de Santanna, 2017). The commodification of DDoS attack has removed the technical barrier to perform attacks; together with the introduction of amplification techniques, the occurrence of reported DDoS attacks has been escalating rapidly (Chromik et al., 2015; Cardoso de Santanna, 2017).

In this assignment, security strategies for DDoS attacks are discussed. We first set the scope of DDoS security issues for this report with having hosting providers as the problem owner. Alongside with an analysis on the actors involved in the defined security issue, the security performances of hosting providers are examined with the metrics using empirical data from the AmpPot dataset (Krämer et al., 2015). Based on the analysis, risk strategies are identified and the corresponding Return on Security Investments (ROSI) are calculated. Finally, we discuss the results and conclude with the findings.

2 Background and Problem Demarcation

DDoS attacks have been escalating in both attack strength and occurrences with the introduction of amplification techniques and the trend towards commodification of DDoS attacks, or so-called *Booters* (Cardoso de Santanna, 2017; Noroozian et al., 2016). In this section, we first introduce the mechanism of DDoS amplification attacks and the Booter ecosystem, based on which hosting providers are chosen as the problem owner in this assignment as they play a vital role in the provisioning of various Internet-based services (Tajalizadehkhoob, Korczyński, Noroozian, Gañán, & van Eeten, 2016). To gain insights for the development of security strategies, different hosting providers are examined by analyzing the characteristics of attacks against whom using empirical data from the AmpPot dataset (Krämer et al., 2015).

2.1 Amplified DDoS Attacks and Booters

Fig. 1 illustrates the mechanism of DDoS amplification attacks: the attacker uses a botnet to send initial small traffic of packets with spoofed IP addresses. By exploiting vulnerabilities in servers, the traffic is amplified to larger payloads of response, which are sent to the spoofed address pointing to the real IP address of the targeted service (or the victim). The target receives the response and its surrounding network infrastructure becomes overwhelmed with the flood of traffic, resulting in an unavailability of service. As trending towards commodification of cybercrime, these amplified DDoS attacks are now available online with very affordable prices from the Booters. Many researches have looked into the target selection factors (Noroozian et al., 2016; Cheung, 2017) and suggest that the targeted autonomous systems (AS) can be categorised into three major groups by the type of networks where they reside (Noroozian et al., 2016):

- *Internet service providers (ISPs)* provide services for accessing, using, or participating in the Internet. Examples of ISPs include AT&T and KPN.
- *Hosting providers* operate servers and provide web hosting services for their customers. In many cases, they are also registrars who sell and register domain names. Examples of hosting providers are GoDaddy and OVH.
- *Others* – any other ASes that are not ISPs or hosting providers. These can be governmental, educational or other enterprise networks.

In this assignment, we focus on **hosting providers** as they play a vital role in the provisioning of various Internet-based services and are associated with all kinds of security threats (Tajalizadehkhoob et al., 2016; Noroozian et al., 2016; Asghari, van Eeten, & Bauer, 2016).

2.2 The Actor Arena

Hosting providers play a key role in fighting cybercrime in the DDoS attack problem as well as the Booter ecosystem, as illustrated in Fig. 2 (Asghari et al., 2016; Cardoso de Santanna et al., 2017): An individual or an organisation (later *victim*) uses the servers and services provided by the hosting providers to set up their own website, against which the *mastermind* of attack is aiming to attack. To hire a DDoS attack, the mastermind will first access the Booter website, create an account, select a "service" and finally make the payment. The payment is done via a third-party payment system, primarily PayPal (Cardoso de Santanna et al., 2017; Karami, Park, & McCoy, 2015). The *Booters* then perform DDoS attacks

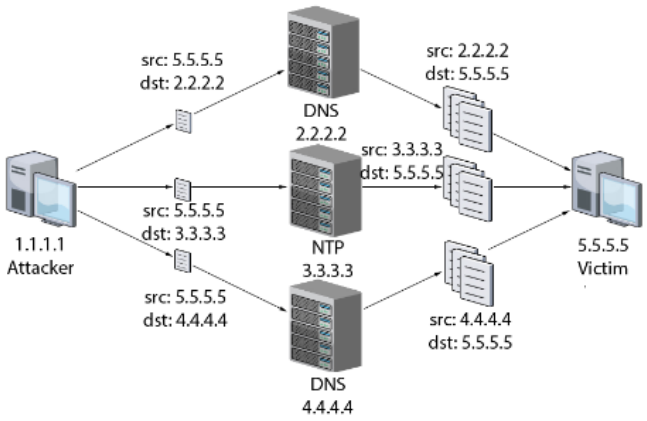

Fig. 1: Illustration of amplification DDoS attacks (Bohte, 2019): the attacker sends small requests with spoofed IP address to different UDP-based services, resulting in large responses directed against the victim

according to the mastermind's "attack plan" (or the sets of attacks that can be performed within a given period of time) using their back-end infrastructure (including their infected machines, or botnets) to send amplified traffic against the targeted website or the victim (Cardoso de Santanna et al., 2017). Interestingly, a market for *DDoS Protection Service (DPS)* has emerged due to the escalated amount of DDoS attacks led by the Booters economy. With DPS, the victims can outsource the cleansing of their traffic by using traffic diversion (Jonker, Sperotto, van Rijswijk, Sadre, & Pras, 2016).

We categorised the key players or actors involved in the security issue by their roles in the notion of cyber risk management:

- *Security providers* – In this study, hosting providers are the ones who are in principle in the best position to shape the information security environment.
- *Security consumers* – These are individuals and organizations who use the web hosting services provided by the hosting providers. They are at the frontline of DDoS attacks and are dependent on the available information security environment.
- *The security industry* – They are the ones who have built a core competence in selling security to customers in need. In this particular case, they are the DPS providers.
- *Attackers* – or the Booter websites.

We then examine different security providers defined in this assignment to understand their performance in the arena.

2.3 Security Performances of Hosting Providers

In order to gain insights for the development of security strategies, we examine the security performance of different hosting providers by analyzing the attack incidents against them. The analysis was done using empirical data from the AmpPot dataset (Krämer et al., 2015), which contains records of amplification DDoS attacks and their victims collected through "AmpPot" deployed within the period of two

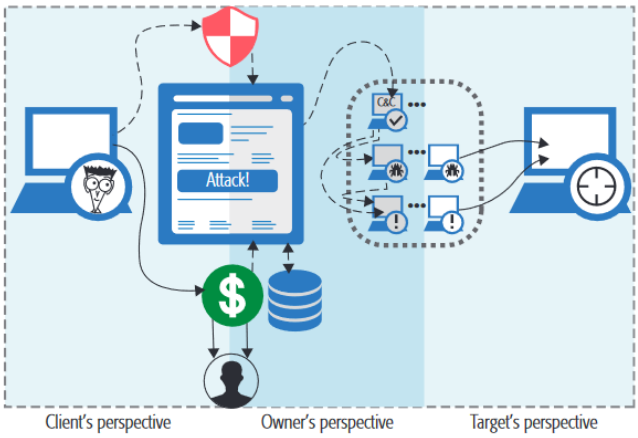

Fig. 2: The Booter ecosystem (Cardoso de Santanna et al., 2017)

years (2014-2015). AmpPot are honeypots which mimic services having amplification attack vectors and respond to queries as if they were vulnerable, and therefore are able to incur DDoS attacks and record those events (Krämer et al., 2015).

Fig. 3 shows a comparison of the attack profiles for the top ten hosting providers (expressed in second-level domain names) that incurred the most DDoS attacks from the dataset. Popular cloud and hosting service providers such as Amazon Web Services (AWS), SoftLayer (now IBM Cloud) and OVH are vulnerable to DDoS attacks as they rank top one, five and seven respectively by the total occurrence of attacks. Besides that, most other hosting providers on the top ten list are spam providers such as *your-server.de, poneytelecom.eu, alojandoargentina.net* etc.

Among the three well-known hosting providers identified above, Amazon AWS has a relatively large IP and domain size recorded from the existing database, and suffers from higher attack frequency and longer attack duration. Note that the DDoS attacks against Amazon AWS are also very much *concentrated*, as shown in Fig. 4: for instance, on August 31, 2015 the number of attacks peaked at more than 800 incidents per day. On contrast, the attacks against Softlayer and especially OVH are much less fluctuated. They do, however, sometimes receive more "intense" attacks with higher packet-per-second comparing to Amazon AWS.

3 Risk Strategies

Now that the different actors involved have been defined, it is important to look at the different actions they can actually perform to influence the problem of DDoS attacks. For exploring these possible actions, the framework of risk strategies will be used. This framework includes 4 separate ways to deal with existing risks, in this case around DDoS attacks. For each actor the actions are discussed and also why these actions are performed. The last paragraph will discuss changes that occurred in strategies over time.

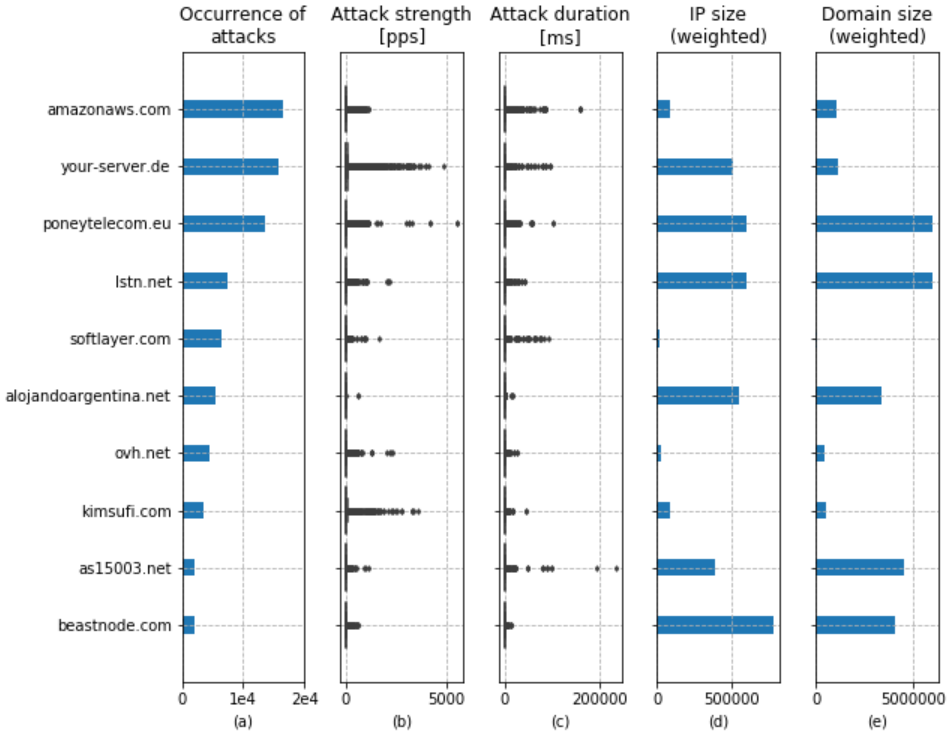

Fig. 3: Top ten hosting providers with most reported incidents and against whom the characteristics of attacks: (a) total number of observed attacks against the host; (b) attack strengths in packet-per-second (pps); (c) duration of attacks; (d) IP size seen and (e) domain size seen. Note that (d) and (e) are weighted from the sub-domains if applicable (created by the authors)

3.1 Possible reactions to risks

Controls The first possible reaction is to reduce or mitigate the risk. This means that the height of the risk is lowered by some sort of mitigation. This can be achieved either by lowering the severity of a loss taking place, or by lowering the likelihood that the loss actually takes place in the first place.

Acceptance The second reaction in to accept the risk, which is actually choosing not to act upon the risk. As it is impossible to get rid of every single risk, every actor in every situation has some risk acceptance to a certain height. Risks cannot be completely excluded because the investment has to be infinite at some point to mitigate a risk marginally further.

Important in the risk acceptance choice is that it is actually a specified choice made beforehand. Explaining an abuse of a risk as expected because the risk was not taken into account afterwards is not classified as risk acceptance. Another feature of risk acceptance is that not all risks can actually be

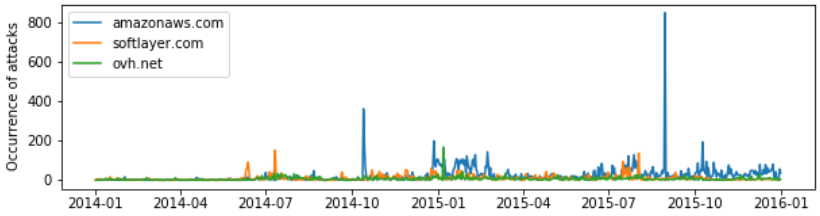

Fig. 4: Number of attacks per day of the three hosting providers (created by the authors)

accepted, for example due to legal reasons in a personal data situation.

Avoidance The third way to deal with risk is risk avoidance, where an actor just ceases the activity that causes the risk to exist.

Transfer A related version of dealing with risk and also the last reaction is to transfer the risks to a third party. In that case some financial compensation is put into place for the third party that now carries the risk. This compensation is based on the expected uncertain costs for the third party that develops because of the risk.

3.2 Actors risk strategies and implications

To get a global sense or overview of involved actors in the system, a formal chart can be created. In this chart, the formal relations between actors are defined by looking at their regulatory exchanges. The formal chart that is displayed in figure (Figure 5), which is based on a formal chart by Su (Su, 2018) for a similar system, shows the overview of the involved actors in the system at hand. The chart shows a number of important actors who are involved such as the problem owner (hosting providers) and attackers, cybersecurity providers and many more actors, but also the formal relations between the actors, which hint at possible actions that each of the actors can perform.
To get more insight into the possible behaviour of these actors, a power interest grid has been created that shows the amount of power and the amount of "interest" (the amount an actor is concerned with the topic) of each of the actors. This plot is shown in Figure 6. Based on these two figures, chapter 4 will discuss the way in which each of the actors deals with the existing risks in the system.

Before assigning the expected actions to the different actors, it is important to emphasize that all actors need to have some risk acceptance in place. Although in theory, a large enough bandwidth can solve the problem of DDoS attacks, in practice this is impossible. This is the case because, independent of the bandwidth, the attacker can always have an army big enough. Another thing to keep in mind is that most of the risk strategies in the case of DDoS should be seen as proactive measures. Because the problem is all about **preventing** availability from suffering, not that much can be done when this availability falls. However, it is also important that a successful DDoS attack is recognized and dealt

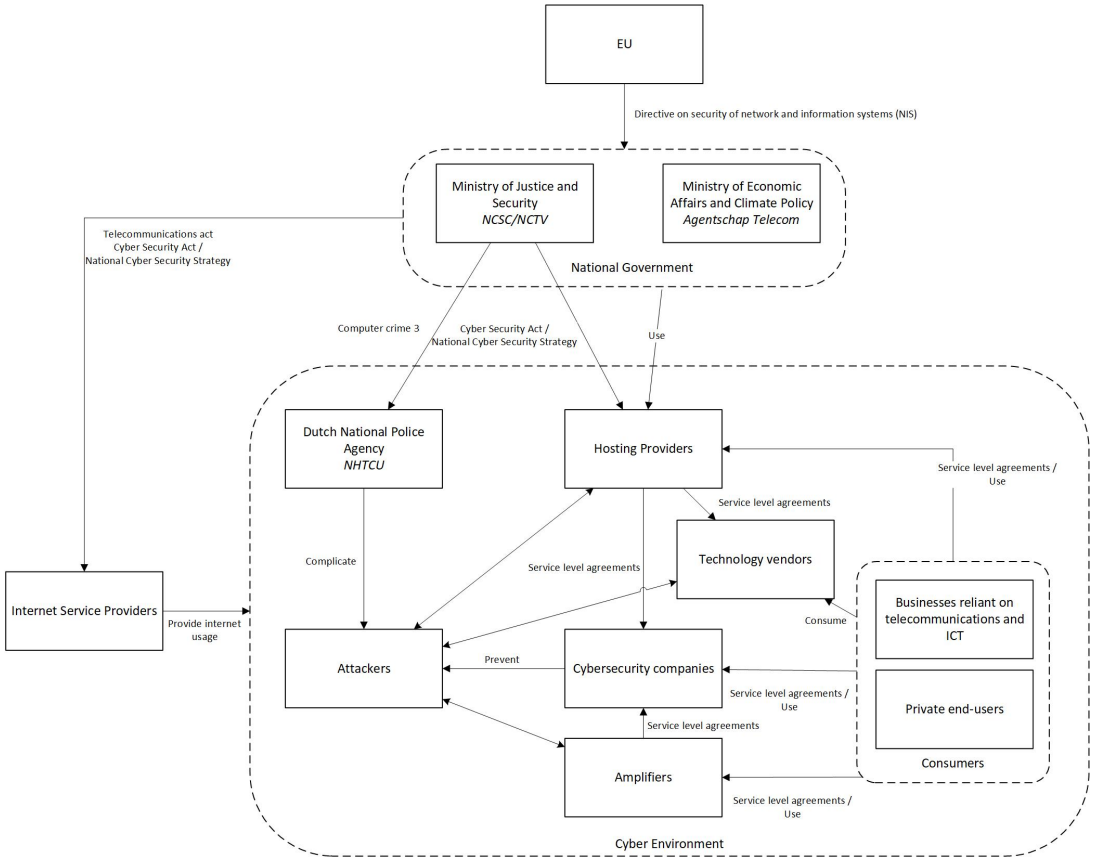

Fig. 5: Chart showing formal relations between actors in the system (Su,2018).

with as soon as possible, which is the only reactive measure that can be taken.

To start with the **hosting providers**, the most interesting strategy is to mitigate risk as much as possible. The DDoS threat keeps increasing with more attacks every year; the consequences hereof will impact the business models of the hosting providers. To determine the risk of DDoS threats, Figure 7 shows the probability with the magnitude and duration of an attack. The classifications A1-4 (Gbps) and B3-5 (seconds) mean the higher the number, the higher the severity of the attack. Any attack that has a loss for the company should be mitigated. That is lowering the risk, for example by investing in investing in capacity, block malicious network traffic or apply dynamic IP addresses, until it is no longer feasible financially. As the business model of these companies is to ensure availability for end users, it is only logical that the hosting providers feel responsible for lowering the risk, in order to keep high customer satisfaction. Hosting providers are the most impacted by the DDoS attacks, meaning the burden falls on them. However, other actors in the system can mitigate the attacks as well.

Another thing the hosting providers can do is to transfer the risk towards **cybersecurity companies**, whose business model is to keep the attackers from performing successful DDoS attacks. These cyberse-

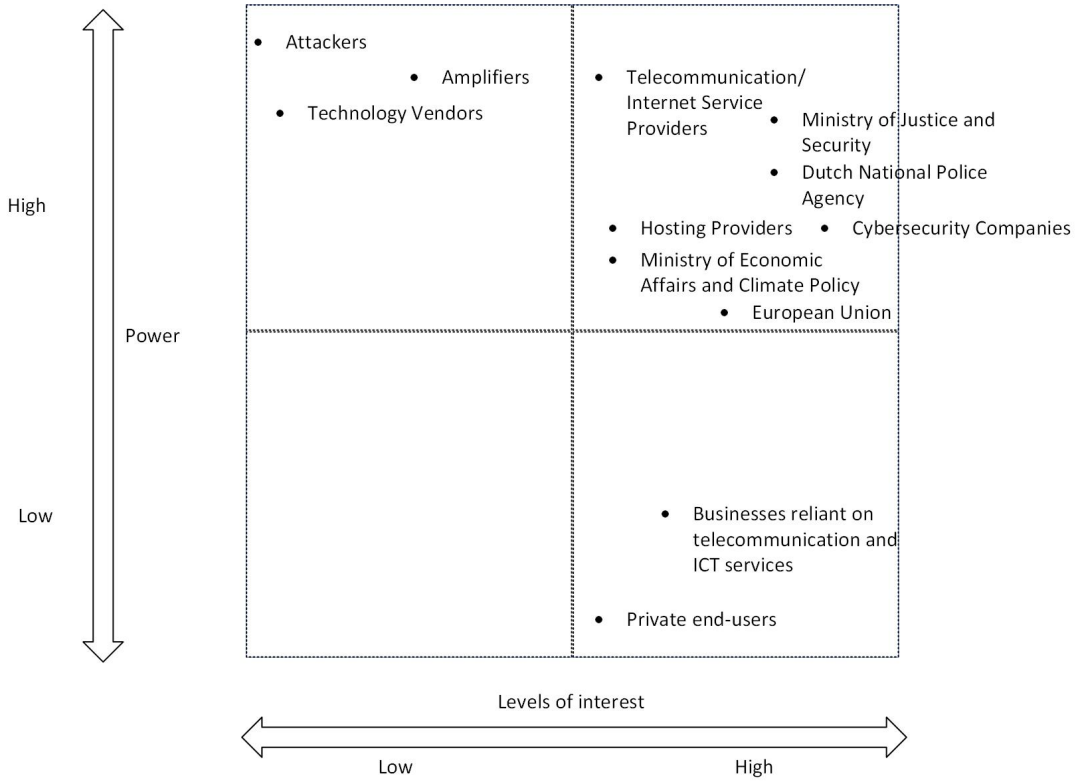

Fig. 6: Power interest grid of actors in the system (Su,2018).

curity companies will then on their turn mitigate the risk that is now their own. Cybersecurity companies can offer scrubbing centers such as *NaWas* (2000), meaning all network traffic will be analyzed to only allow legitimate traffic through to the hosting provider. A benefit of putting the risks on the agenda of the companies that are specialized in cybersecurity, is that it is their only goal to protect the services from failing. This means that their complete focus can go to the security, whereas hosting providers could only focus on this aspect part-time.

Internet service providers has an important role in the facilitation of network traffic. Their network comes under a high load because of these attacks, increasing the costs of the network. These costs can become disastrous if the ISP goes down as everyone on their service is disrupted. It is therefore important for them to mitigate risk as the consequences are unacceptable. Mitigation can be done successfully if for example BCP-38 is implemented worldwide to prevent IP-spoofing (*BCP 38 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*, n.d.). However, this needs to be applied by everyone for it to work but due to the international dimension of the internet this is hard to regulate. There are other measures, such as blackholing, scrubbing, traffic engineering, and local filtering (Vink, 2016). Their strategy would be to apply these for themselves but they do not have any interest in applying these for other victims as it only increases costs but no benefits for them.

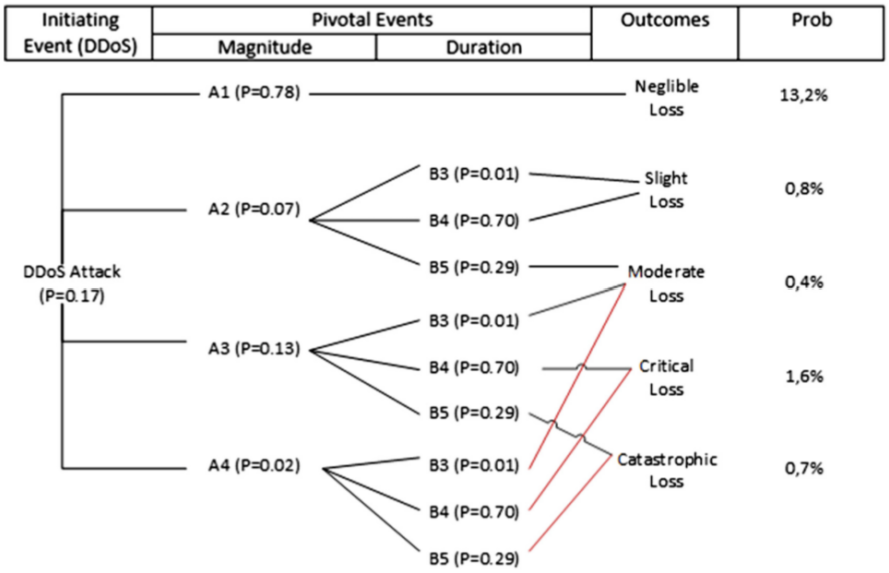

Fig. 7: Event Tree displaying the probability of a monthly DDoS attack including severity (Wangen et al., 2016)

The **consumers** do not have an explicit choice other than to accept the risk they have of losing customers, income and public image. What they could do, is to indirectly mitigate the risk by encouraging other actors to improve their risk mitigation. This process is partly inherent to the market of availability, as hosting providers will perform better in the market if their risks are lower. This is why cybersecurity companies can exist in the first place.

Technology vendors, although less involved with the risks as only their systems are used in the process, can still have influence on these risks. They could for example only provide technologies to hosting providers that are safe and available at most times. This means that the rotten eggs in the basket are eliminated and the risk is lowered indirectly.

Turning towards the governmental institutions, both the **EU** and the **national government** of countries can influence the existing risks, either by creating laws that keep other actors from accepting risks, or by setting standards in risk mitigation, that the other actors need to meet. This could be a law that states at least x percent should be spent on security, or that the probability of losing this availability should be no higher than 4 percent per year. A third thing the governmental organizations can do is place some part of the responsibility on the desk of technology vendors. This way, risk transfer takes place from hosting providers and consumers towards these technology vendors. This could mean that the actor puts more effort into creating stable and safe connections.

The **Dutch National Police Agency (NHTCU)** can perform actions slightly closer to the core of the problem, by eliminating attackers as a way of mitigating the existing risks. By removing the actor that creates the threat in the first place, the risk can be lowered at the start of the problem. This would

mean arresting owners of botnets, or discovering botnets and try to dismantle them.

Last but not least, the **attackers** and **amplifiers** should also be addressed. As they are the cause of the existing risks, they also would like to influence the height of these risks, in the opposing direction. For example by enlarging their botnets, or strengthening the reach of the amplifiers, the risk becomes higher for the victims, making it harder to mitigate it and unethical to accept it.

3.3 Changing strategies over time

As availability of online services have become more and more important over the past decades, due to markets moving towards online business increasingly, the protection of this availability has become more important.

This movement can also be seen in the actions of the actors. Hosting providers invest more in their availability to mitigate the risks further and since some time they can now transfer the risk over towards cybersecurity companies, who have emerged from the problem. However, it can not be stated that these changes have explicitly lowered the risk of DDoS attacks shutting down the availability of the hosting providers' services, because the attackers have increased their power as well. Amplifying techniques have increased in power, as new protocols will be used with a bigger response. As more and more devices can be used for enlarging the botnets, it is also harder to protect from these forces, due to the increase in popularity for IoT devices. It is therefore likely that the threat will continue to grow.

4 ROSI

The strategy of the hosting provider will be further evaluated using a financial cost and benefit analysis. The strategy, based on mitigation of the DDoS risk, is chosen because they have a strong incentive to buy security measures against the threat. Whereas other strategies focus on giving the benefits to other actors, hosting providers have direct benefits for themselves. This does not speak of the efficiency of the investment, but only on the benefits and costs for the actor.

The Return on Security Investment (ROSI) (Sonnenreich, Albanese, & Stout, 2006) will be used to evaluate the strategy of the hosting provider. This metric looks at the exposure and mitigation of the risk to see if the costs are worthwhile. By calculating this metric the benefits and costs of a security investment will become transparent.

Calculating risk exposure, risk mitigated, and solution cost however remain difficult as there is no standardized method for the calculations (Sonnenreich et al., 2006). For the calculation of DDoS strategy of the hosting providers we will apply literature review and the AmpPot dataset to perform the calculations. As there are a lot of differences between different hosting providers, the calculations should ultimately also be specified for the size of an organization.

The risk exposure can be calculated with the following formula (Böhme, 2010):

$$\begin{aligned} \text{ROSI} &= \frac{\text{benefit of security} - \text{cost of security}}{\text{cost of security}} \\ &= \frac{(\text{risk exposure} \cdot \%\ \text{risk mitigated}) - \text{cost of security}}{\text{cost of security}} \end{aligned} \tag{1}$$

...or alternatively (Gordon & Loeb, 2002):

$$\begin{aligned} \text{ROSI} &= \frac{EBIS_S - \text{cost of security}}{\text{cost of security}} \\ &= \frac{(ALE_S - ALE_0) - \text{cost of security}}{\text{cost of security}} \end{aligned} \tag{2}$$

The expected benefits of an investment in information security in the *secured scenario* (denoted $EBIS_S$) can be calculated as the difference in Annualized Loss Exposure (ALE) measured in the original scenario (i.e. without security measures in place, ALE_0) and the secured scenario (i.e. with security measures in place, ALE_S). ALE is further divided into two parts of estimations as shown in Equation (3): it is estimated by multiplying: the annual frequency of occurrence of a certain risk, and the impact that would produce on the affected asset.

$$\text{ALE} = \text{Impact (Unit)} \cdot \text{Probability (Annual)} \tag{3}$$

4.1 Annualized Loss Exposure (ALE)

Original Scenario Without security measures in place - some numbers here

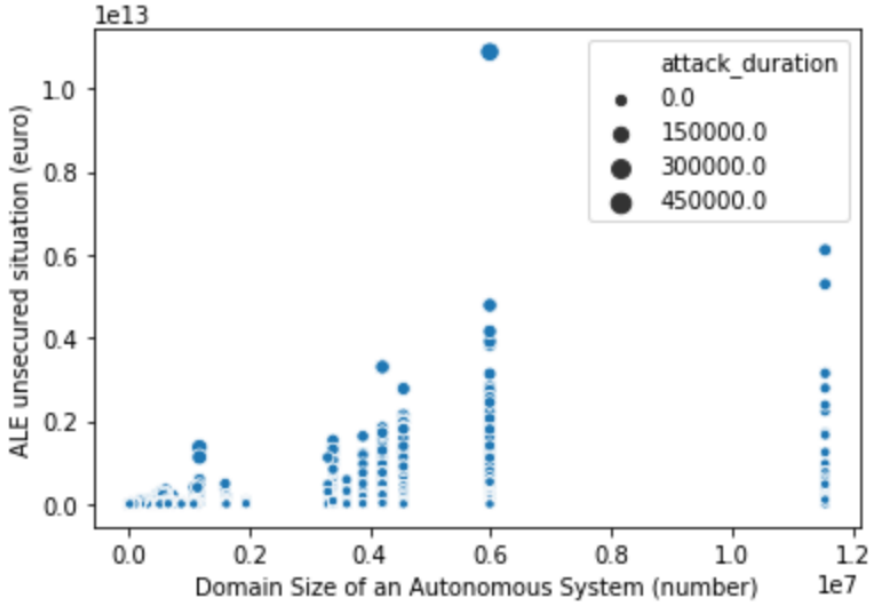

Fig. 8: ALE estimation

Secured Scenario With security measures in place - some numbers here

Return on Security Investment is a metric used to determine how much a firm should invest in security. However, the costs and benefits of an investment are not always clear in computer security investments. As Moore, Dynes, and Chang (2015) mentions, the focus has been much more on the process-side (controls) rather than the outcomes of the investments. Firstly, from a technical view a reason for this could be that the indirect costs are not easily quantifiable, however, a bigger problem with this metric might be that benefits of costs heavily depend on exogenous factors, such as attacker behavior. Secondly, considering the social environment the incentives of actors play a much bigger role. Controls are easier to measure, business model is focused on selling controls and the effort, instead of the risk of failure (Hernandez Gañán, 2015) Nonetheless, ROSI helps to focus efforts on the prevented losses to show how the investment fares in an actual threat environment.

From Figure 5 we can conclude that the probability of a DDoS attack occurring is 0.17 without any type of investment. Although this probability differs for different sizes of impact, we will use the general probability, in order to keep the calculations clear. The impact of a DDoS attack depends on many factors, such as the size of the victimized company, the amount of profit they earn per day of the year, which can be seen as direct impact, but also the indirect loss of lost customers or damage to the brand. The second part of the impact is the time that the severs were down, due to the attack. The longer a company was unusable and the bigger the service that has been unavailable, the bigger the impact. Translating the impact to the formula of ROSI, it can be stated that investing in the security only changes the probability of a successful attack occurring, and has no influence on the height of the impact, as security does not change the size of a company or the strength of attacks.

It is, however, relatively hard to calculate the change in probability of a successful attack taking place, which is why we will focus on calculating the less hard, but still problematic factor of impact.

Using the AmpPot dataset, we can find out the size of the different companies that were victimized, by using the number of IP addresses in their possession. This is not a direct representation of how much money is made by each of the companies, but we have assumed that it is indeed an indicator and that there exists correlation between the 2.

In the paper of Dubendorfer et al., an estimation of damages to a webhost provider from DDoS attacks is made. In this paper, a WPS with 6 employees, 800 customers and 2500 domains would suffer an annual loss of 1 billion CHF, which translates to 920 million euros per year (Dubendorfer, Wagner, & Plattner, 2004). Translating this to a loss per second of downtime, would result in a €29,15 loss per second.

For a better result, each of the organisations in the dataset should be examined in detail, by looking at how successful they are and what type of business they execute.

To find an indication of the time that the services of these organizations were down, we use the time span of the attacks, which is also available in the AmpPot dataset. Again, it cannot be stated that the duration of an attack exactly determines the duration of the system being down, as some of the attacks might not even have been successful. However, due to a lack of better data, we assume that the duration of an attack indeed estimates the duration of the system being down.

With the AmpPot data and the assumption that are stated above, a calculation can be executed that shows the impact of a successful DDoS attack, based on the size of a company and the duration of an attack. Together with the probability of a DDoS attack occurring and being successful, the current risk of DDoS attacks can be calculated per company in the AmpPot dataset.

Now only two variables remain in calculating ROSI, which are the probability of a successful DDoS attack after investing and the size of the investment. As data runs short on calculating these two variables, we have chosen to present a relation between the two. For each of the companies in the dataset, a column is created that shows how much should still be invested for a decrease in probability of 0.01. If the company can achieve this decrease with an investment lower than or equal to the maximum investment stated in the column, they should execute the investment.

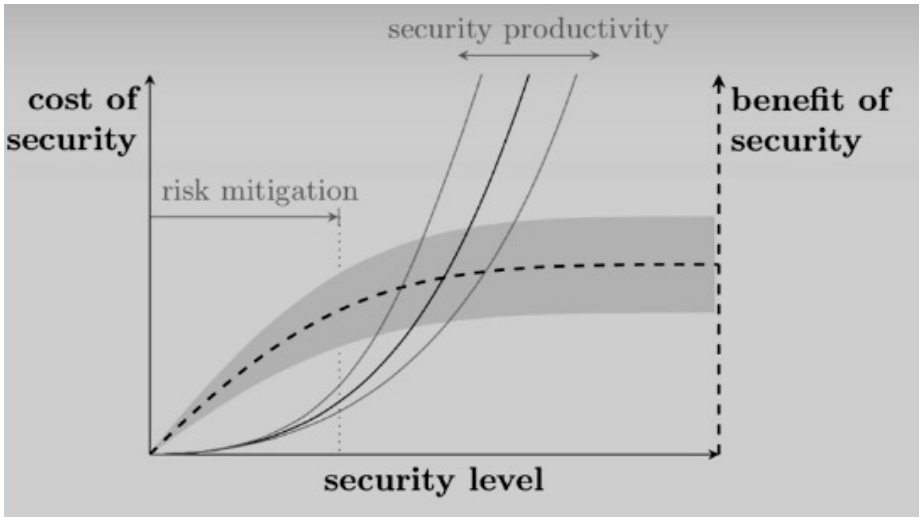

Fig. 9: Non-linear relation between risk mitigation and level of security.

As there is a nonlinear relationship between investment in security and what it actually achieves; increased security (see Figure 9), the calculated column is only true for lowering the probability in one certain case, for example lowering from 0.17 to 0.16. It should be clear that decreasing this probability from 0.16 to 0.15 requires a higher level of investment. Using the created maximum investment, together with the nonlinear relation, the companies in the dataset can now find their optimal height of investment, as at some point, either their budget runs out, or the security does not increase enough to cover the investment made.

Important to note, is the remaining difficulty for the companies to calculate the costs they make to reduce the risk, as they exist of both direct and indirect costs. Once a certain security measure has been implemented (direct costs), other issues might occur that increase the cost after the implementation (indirect costs).

Also, it remains relatively hard to figure out how much any investment can actually decrease the probability of a successful attack. For making a well-founded decision on the height of investment, more and better data is needed.

Cost of security - often deterministic but difficult due to indirect costs:

1. Direct cost
   – Sum of expenses for acquisition, deployment, maintenance
2. Indirect cost
   – Time lost due to forgotten passwords, inconvenience data transfer, etc.

attack_duration	costs_org_domain_per_second	total_costs_attack	maximum_investment	risk_height
1173.511503	1.187035e+08	1.403230e+11	1.403230e+09	2.385491e+10

Fig. 10: Needed investment by Amazon, output generated using Python from AmpPot data.

Figure 10 shows the calculations made for Amazon. It shows the assumed impact, the risk that belongs to this impact assuming the probability of 0.17 and lastly it shows the investment needed to lower this probability with 0.01, which is equal €1.4 billion, which can be plausible considering Amazon is one of the biggest companies in existence. The maximum investment that can be made to lower the probability of a successful DDoS attack from 0.17 to 0.16 for the other companies can be seen in the accessory python file "SecurityInvestments.ipynb".

5 Conclusions

Different organizations will react in different ways to existing risks. As the risk of DDoS attacks continuously increases, both due to an increasing value of online services, as an increasing number of IoT devices in existence, investing in securing the availability of Hosting Providers becomes more important every day as well. Although it can be relatively hard to calculate the optimal height of this investment for different companies that have to deal with this risk, filling in the compartments of ROSI, can be done by indicating factors such as the size of the company, and previous attempted attacks. Literature gives insight in the probability that DDoS attacks occurs, but this is every changing. Hope exists in making better decisions on investing against DDoS attacks, as companies actually have the data needed to calculate their optimal investment, although they do need to be informed about the impacts, probabilities and risks.

References

Asghari, H., van Eeten, M., & Bauer, J. M. (2016). Economics of cybersecurity. In *Handbook on the economics of the internet* (p. 262-287). Edward Elgar Publishing. Retrieved from https://EconPapers.repec.org/RePEc:elg:eechap:14700_13

BCP 38 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. (n.d.). Retrieved 2019-10-02, from https://tools.ietf.org/html/bcp38

Böhme, R. (2010). Security metrics and security investment models. In *International workshop on security* (pp. 10–24).

Bohte, E. (2019). *Evaluation of current state of amplification-based ddos attacks* (bachelor's thesis). Vrije Universiteit Amsterdam, the Netherlands.

Cardoso de Santanna, J. (2017). *Ddos-as-a-service: Investigating booter websites* (Doctoral dissertation, University of Twente, Netherlands). (CTIT Ph.D. thesis Series No. 17-448, ISSN 1381-3617) doi: https://doi.org/10.3990/1.9789036544290

Cardoso de Santanna, J., De Schmidt, R., Tuncer, D., Sperotto, A., Granville, L., & Pras, A. (2017, 7 1). Quiet dogs can bite: Which booters should we go after, and what are our mitigation options? *IEEE communications magazine*, *55*(7), 50–56. doi: https://doi.org/10.1109/MCOM.2017.1600992

Cheung, R. (2017). *Targeting financial organisations with ddos: a multi-sided perspective* (master's thesis). Delft University of Technology, the Netherlands.

Chromik, J., Cardoso de Santanna, J., Sperotto, A., & Pras, A. (2015, 5). Booter websites characterization: Towards a list of threats. In *Proceedings of 33rd brazilian symposium on computer networks and distributed systems, sbrc 2015* (pp. 445–458). Brazilian Computer Society (SBC). (eemcs-eprint-26162)

Dubendorfer, T., Wagner, A., & Plattner, B. (2004). An economic damage model for large-scale internet attacks. In *13th ieee international workshops on enabling technologies: Infrastructure for collaborative enterprises* (pp. 223–228).

Gordon, L. A., & Loeb, M. P. (2002, November). The economics of information security investment. *ACM Trans. Inf. Syst. Secur.*, *5*(4), 438–457. Retrieved from http://doi.acm.org/10.1145/581271.581274 doi: https://doi.org/10.1145/581271.581274

Hernandez Gañán, C. (2015). *Metrics in practice.* Retrieved from https://www.youtube.com/watch?time_continue=4&v=GuyKbRoLmcw

Holl, P. (2015, March). Exploring ddos defense mechanisms. In *Network architectures and services.*

Jonker, M., Sperotto, A., van Rijswijk, R., Sadre, R., & Pras, A. (2016, 11 14). Measuring the adoption of ddos protection services. In *Proceedings of the 2016 acm internet measurement conference, imc 2016* (pp. 279–285). United States: Association for Computing Machinery (ACM). doi: https://doi.org/10.1145/2987443.2987487

Karami, M., Park, Y., & McCoy, D. (2015). Stress testing the booters: Understanding and undermining the business of ddos services. *CoRR*, *abs/1508.03410*. Retrieved from http://arxiv.org/abs/1508.03410

Krämer, L., Krupp, J., Makita, D., Nishizoe, T., Koide, T., Yoshioka, K., & Rossow, C. (2015). Amppot: Monitoring and defending against amplification ddos attacks. In *International symposium on recent advances in intrusion detection* (pp. 615–636).

Moore, T., Dynes, S., & Chang, F. R. (2015). Identifying how firms manage cybersecurity investment. *Available: Southern Methodist University. Available at: http://blog. smu. edu/research/files/2015/10/SMU-IBM. pdf (Accessed 2015-12-14)*, *32*.

NaWas. (2000). Retrieved 2019-10-02, from https://www.nbip.nl/en/nawas/

Noroozian, A., Korczyński, M., Hernandez Gañán, C., Makita, D., Yoshioka, K., & van Eeten, M. (2016). Who gets the boot? analyzing victimization by ddos-as-a-service. In *Proceedings of the international symposium on research in attacks, intrusions, and defenses, raid 2016.* Springer.

Sonnenreich, W., Albanese, J., & Stout, B. (2006, February). Return on security investment (ROSI) - A practical quantitative model. *Journal of Research and Practice in Information Technology*, *38*(1), 45. Retrieved 2019-10-02, from `https://search.informit.com.au/documentSummary;dn=937199632104879;res=IELHSS`

Su, K. (2018). Governance measures to mitigate amplification ddos attacks (bachelor thesis). *Bachelor's Thesis*.

Tajalizadehkhoob, S., Korczyński, M., Noroozian, A., Gañán, C., & van Eeten, M. (2016). Apples, oranges and hosting providers: Heterogeneity and security in the hosting market. *IEEE*. doi: https://doi.org/978-1-5090-0223-8/16

Vink, T. (2016). *How can ISPs handle DDoS attacks?* Retrieved 2019-10-02, from `https://security.stackexchange.com/questions/134767/how-can-isps-handle-ddos-attacks`