Economics of Cybersecurity Block 3
Telnet scans

Calvin Hendriks - c.hendriks@student.utwente.nl
Christiaan van den Bogaard - c.h.m.vandenbogaard@student.utwente.nl
Sander Bakkum - s.bakkum@student.utwente.nl
Riccardo Colombo - r.colombo@student.utwente.nl

October 7, 2019

1 Introduction

In our last assignment [1], we analyzed a set of port scans performed by Shadowserver, specifically on port 23 and 2323. From the data set a security issue came to mind; vulnerable devices can become part of a botnet, like the one created by the Mirai malware, that is in turn used to perform DDoS attacks. After identifying the issue, we defined a set of metrics that could be used to measure the scale of the problem. We advise the reader of this report to read our previous assignment as well.

In this assignment, we identify our problem owner and take a look at the strategies that the problem owner can take to reduce the security risk. Furthermore, we reconsider the actors from last time and see what strategies they can take and how they influence the problem. Finally, a Return on Security Investment (ROSI) will be calculated on one of the proposed strategies.

1.1 Metrics

- What percentage of connection attempts requires authentication? In this case, we found out that 77.2% require authentication. For the other 22.8% it means that no authentication banner is displayed. Conclusively, this means that 77.2% is possibly vulnerable to the Mirai botnet as a dictionary attack can be launched.

- What percentage of connection attempts gets rejected? We found that 6.9% actively refuses the connection which mean that they absolutely can not be attacked.

- What percentage of device publishes sensitive software information? Analyzing this issue we determined that $\sim$ 27% of the scanned IP addresses provide some information on either the running OS or the running service. Such information can be very valuable for an attacker, helping him determine whether the device could be exploited.

- Patch adoption to a severe security vulnerability. This metric discussed the OS patch adoption rate for MikroTik devices.
  - What percentage of devices is vulnerable to CVE-2018-7445? This metric analyzed what is the fraction of IP addresses that have not updated their OS in the 5 months period following the disclosure of the patch.
  - Adoption rate of the patch fixing CVE-2018-7445. The metric analyzes the fraction of IP addresses which updated their OS over the four weeks following the release of the patch.
- What is the adoption rate of the different versions of OpenSSH? In this metric we analyze how recent are the versions of OpenSSH run on the scanned IPs and we give an indication on how many suffer from a serious vulnerability.

1.2 Problem owner

The problem owner is in most cases the party affected by the issue to be solved or the party who would benefit from a solution [2]. From this definition, one might think that the owners of the infected devices are the problem owner. However, since the owners of the hijacked devices often do not experience any problems and would also not really benefit from a solution, they are not our problem owners. The same is true for Internet Service Providers (ISP), since the amount of bandwidth used by a DDoS attack is extremely small compared by the bandwidth that normal users use by services such as streaming. The problem owner that we will focus on in this report are the **victims of DDoS attacks launched from IoT botnets.** These parties are most affected by the issue, since they can suffer serious financial losses if hit by a DDoS attack. Therefore, they will also be the group that would benefit the most from a solution against such botnets and corresponding DDoS attacks.

2 Processed feedback & differences from previous assignment

In this section we discuss how we have modified our metrics to incorporate the feedback that we have received on the previous assignment. A description of the updated metrics can be found in the subsequent section.

2.1 Percentage of devices with authentication

This metric gives insight in the percentage of devices that require authentication when a telnet connection is established. This means, that these devices are *possibly* vulnerable to Mirai, as it used a dictionary attack. In the devices that do not have authentication, we do not know what is the case. In most cases its either a rejected connection or a whitelist. In the precious assignment, we calculated this metric on the whole period thus not keeping in mind that IP change over time. We altered this so it will calculate it on a daily basis and average all the daily percentages. This result in the following updated graph as shown in Figure 1.

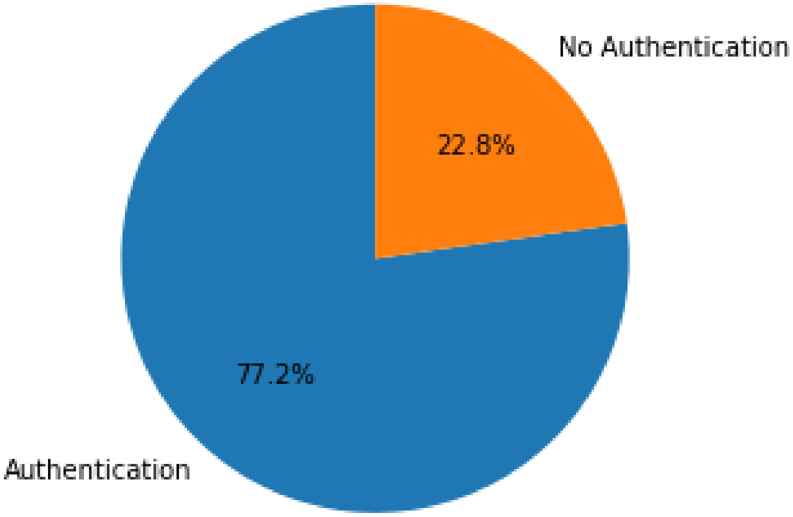


Figure 1: Pie chart of devices which require authentication

2.2 Percentage of devices which reject connection

An import defense mechanism of these devices is whether the connection is rejected. If there is an extra layer of defense in place, such as a firewall, these devices can not be infected to be part of the botnet. Also, this metric was computed over the whole time period thus not including the IP change over time. This is recalculated for every day individually and averaged. This new pie chart can be found in Figure 2

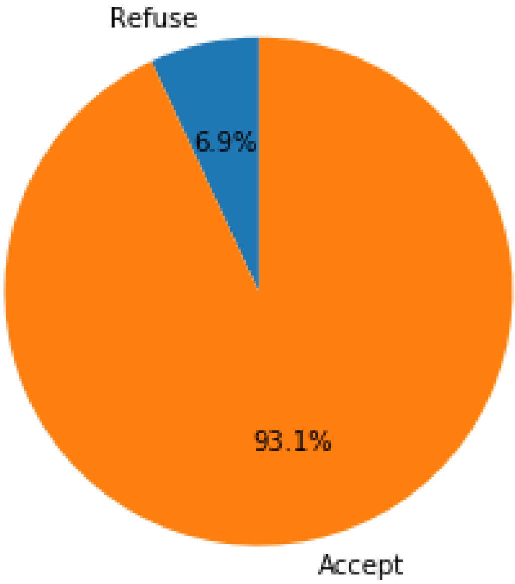


Figure 2: Pie chart of devices which refuse connection

2.3 Machines disclosing information on running software or services

1. The regular expression used in the metric has been adjusted to correct the matching of certain unwanted strings in the response messages of the scanned devices. The wrong matching caused the previous evaluation to erroneously consider a higher number of IPs as disclosing.

2. Further analysis revealed that some IP addresses run two different services/machines on port 23 and 2323. This introduces a certain degree of error in the evaluation of the previous metric as we practically considered two different services/machines as if they were the same. The new metric takes this consideration into account and separately analyses port 23 and port 2323.

3. After implementing point 1 and point 2 the number of total IPs have moved from 125,915 to 127,121 while the number of disclosing IPs have moved from 76,720 to 34,158. It is worthwhile to note that the total number of IPs have slightly increased as we decoupled the two ports, in particular we measured that 123,813 IPs are answering on port 23 and 3,308 IPs are answering on port 2323. The number of disclosing IPs has instead diminished because of the adjustment in the regular expression outlined in point 1.

4. Because of the changes highlighted in the previous point, the percentage of IPs which disclose information on either the running software or services have decreased from 60.9% (fig. 3a) to 26.9% (fig. 3b).

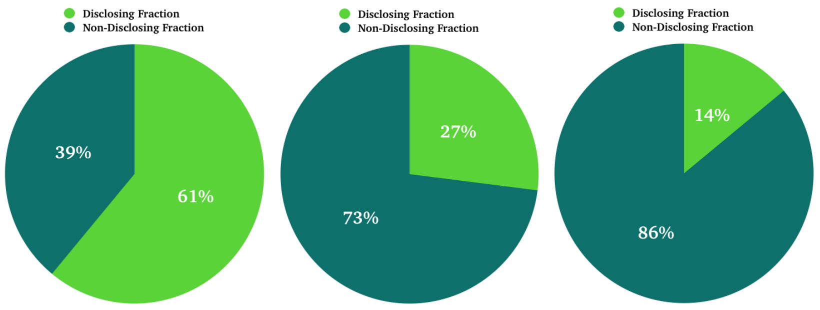
5. One of the concerns highlighted by the feedback is that the IP addresses may be assigned dynamically by the ISP and considering the same IP address over such a long time frame would not capture this information. The suggestion was therefore to consider the the daily percentage of the IPs disclosing information and then compute the average over the total number of days. After computing what we have just outlined we obtained a mean value of 14.2% (fig. 3c), opposed to the 26.9% (fig. 3b) that we computed in point 4.

6. As the previous point shows, computing the fraction over the whole period yields a significantly different result than computing it daily and taking the average. Further analysis showed no sign of IP addresses changing the behaviour of their response to the scan, therefore suggesting that dynamically assigned IPs are not a major factor in such shift. However we identified two main factors that we consider responsible for the result difference:

   (a) A discrete amount of IP addresses have been scanned only in specific time periods, for instance only during a period of few months or, in some cases, few weeks. This lack of uniformity in the IP scans inevitably contributes to a higher percentage when the whole span of the dataset is considered while it contributes to lowering the percentage when a single day is considered. In this last case, in fact, the IPs that are not regularly measured will average out.

   (b) Some IPs, such as 104.206.241.222, consistently do not disclose any information while on really few occurrences (only one in case of 104.206.241.222) respond with a banner featuring the version of the running OS. While this is behaviour is not easily explainable, it is clear how it contributes in boosting the overall percentage while only slightly contributing in the daily one.

7. Having considered all the previous points we consider the measurement of the metric over the whole period to be the most accurate when considering the absolute percentage of the devices disclosing information as the lower percentage in the daily evaluation is principally due to an inconsistency in the measurements.



(a) Original (b) Updated - Global (c) Updated - Daily

Figure 3: Metric evaluation difference

3 Relevant differences in security performance

While this section will discuss differences in security performance, we first need to mention the fact that all of the scanned IP addresses are not behind a firewall. Therefore, all of their open ports are exposed to the internet. This by itself is already a bad security practice.

If we analyze the dataset, we see a great difference in security performance among all IP addresses. The strongest form of security against these botnets is to go from default open to default closed ports [3]. However, if users need to access the device remotely, it is no option to close the port. In this case, device owners can whitelist the IP addresses that need to access the service, and deny any other connection requests. Our metric reveals that only 6.9% of the scanned IP addresses refuse the connection (See Figure 2). This means that most of the devices still accept a connection over port 23 or 2323 from any IP address.

Unfortunately, we could not measure the presence of default passwords on the devices at the scanned IP addresses. Even though Mirai makes uses of default or weak credentials, it is still better to have a form of authentication than none. By checking the banners for words like ”login” or ”password”, be measured the presence of authentication on the scanned devices. However, it is hard to identify differences in security performance, since we do not know if the 22.8 % that did not display any login text do not require authentication or do not present these text values for another reason.

While whitelisting IP addresses that may use the telnet service is better than accepting any connection, it is still far from secure. Telnet does not use any form of encryption, so passwords or any other kind of information is sent in plain text. Therefore, it is recommended to use SSH instead of Telnet. We altered our metric that gave insight in the versions of OpenSSH to measure the amount of devices that run OpenSSH on port 23 and 2323. Here we can see a major difference in security performance among the scanned IP addresses. Although the results (see Figure 4) show a slight increase in the usage of SSH, the average is still only 5%.

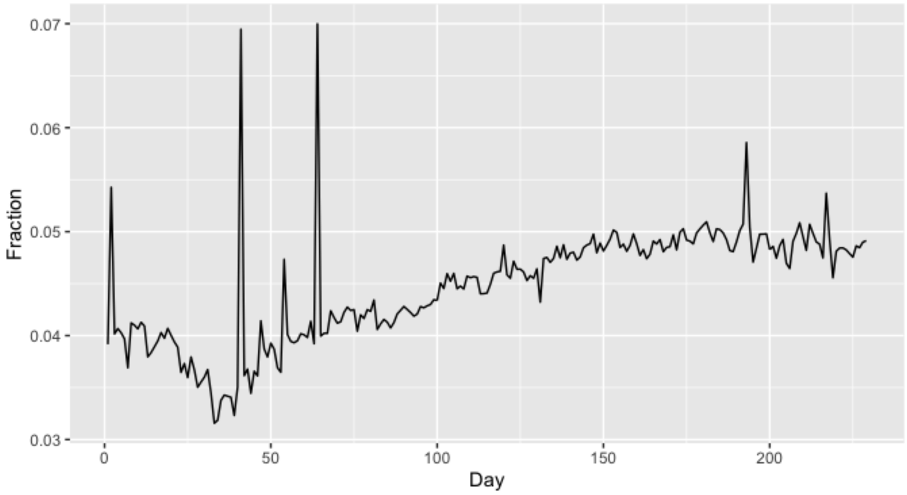


Figure 4: Fraction of devices running SSH on port 23 and 2323

Another difference in security performance can be seen in the amount of information in the telnet banners. In our last assignment, we focused on the IoT malware Mirai, which exploits the usage of default passwords. More recently, botnet malware creators are using software vulnerabilities in order to infect a device, rather than abusing the use of default credentials [4]. The fact that some devices publish sensitive software information in their banner makes it easier for attackers to find the needed vulnerabilities to hijack a device. Using our metric to measure the percentage of IPs that disclose information on running software, we see that over a quarter of them do in fact respond with such information (See Figure 3).

4 Strategies - Problem Owner

In section 1.2 we have defined the problem owner of our research to be a generic company victim of a DDoS attacks. We will further refine the definition of the problem owner in section 7 where we will show how he could benefit from the adoption of a particular risk strategy.

The impact that a DDoS attack can have on a company can greatly affect the availability of its services and it has been consistently increasing in magnitude [5]; this not only generates a direct impact on the productivity of the company but it can also have an impact on its customer retention and public image. Furthermore, as shown in [6], a DDoS attack can negatively influence the stock prices of the company when it disrupts services that are intended for its customers. Being prepared to face a DDoS attack is therefore paramount for digital companies, therefore we will now analyze how the problem owner can approach DDoS related risk management by adopting one or more of the following risk strategies:

- *Risk mitigation* strategies aim at improving the current infrastructure/ processes of the company in order to reduce the likelihood as well as the impact that an attack may have. DDoS attacks can either leverage a vast number of connections to saturate the target infrastructure (*volumetric attacks*) or leverage application layer traffic to exhaust web servers' resources (*application/TCP exhaustion attacks*) [7]. We can identify two main solutions for such issues:

  - *Traffic scrubbing* services and *CDNs* can be used to mitigate volumetric attacks; when anomalous rates of incoming traffic are observed, the incoming traffic is rerouted through the scrubbing infrastructure and then analysed by the scrubbing center where the malicious traffic is dropped and the genuine one is forwarded to the client infrastructure.
  - *On-premises appliances* are instead commonly adopted to efficiently mitigate application attacks; it consists in in-line devices that can both detect and mitigate application attacks.

  Lastly, accordingly structure the company's business continuity plan as well as thoroughly design the disaster recovery plan represent two powerful strategies to reduce the impact of a DDoS attack.

- *Risk acceptance* consists in simply accepting the level of risk that the threat poses as the cost of mitigating it would outvalue the benefit of the mitigation. Therefore depending on the business and on the function of the IT infrastructure accepting the risk of a DDoS attack could be a viable solution. In section 7 we will consider the ROSI of a possible risk strategy; the resulting value would give us an indication on whether it would be more financially effective to accept the risk or to address it.

- *Risk avoidance* plays a role in debating whether the risks of entering a new business would outweigh the possible benefits. Similarly, it is also considered when assessing whether to retire from a business area that is considered too risky. As far as our case is concerned, we consider risk avoidance not to be a viable strategy as it would hinder the core business.

- *Risk transfer* involves transferring the risk to a third party, for instance to a cyber insurance company in exchange of a premium fee. However, as we analysed in class, the cyber insurance market still faces few unsolved challenges and, although the market is growing [8] [9], it is not a popular solution yet.

5 Other Actors Involved

The security issue, as we have analyzed it in this paper, is not only influenced by the problem owner but also by several other actors:

- IoT owners can affect the issue in multiple ways; for instance by buying more devices which could potentially become victims of a botnet increasing its power. Purchase behaviours, however, could also positively impact the issue; customers could in fact tend to sacrifice extra money to buy quality products which will be more secure. Furthermore, adoption of best practices such as network isolation and regular patching will positively impact the issue.

- Manufacturers can also influence the security issue in a positive way; the implementation of OTA updates, the increase of the security level in the design of new products can reduce the number of devices which can fall victims of a botnet. Moreover, groups of manufacturers could cooperate to define minimum security levels for the industry.

- ISPs can directly influence the issue by preventing IP spoofing on their networks but also indirectly by launching awareness campaigns to help IoT owners in making more informed choices.

- Governments have also an impact on the security issue as they could define minimum security levels for the industry, consider device owners also liable for the attacks and design targeted awareness campaigns.

The previous list can give an insight on how vast the number of actors that influence the issue is; the misalignment of incentives for each actor represents one of the biggest challenges in mitigating DDoS attacks.

6 Risk Strategies - Other Actors

6.1 IoT owners

IoT owners can choose to accept the risk. In the case of Mirai, IoT owners could still use their devices as intended. The main problem is when the C&C server orders the devices to DDoS a certain target. The Device will start DDoSsing the target and therefore generate a significant amount of traffic on the IoT owners network. This in this case is risk acceptance. Implementing a security measure will probably not result in positive utility for the end user as most of the time the user will not know whether their device is compromised. The main problem here is that other users beside the IoT owner will have significant losses due to the botnet, therefore when you look at a single IoT owner risk acceptance could be a solution, but will be a horrendous choice when looking at the complete picture.

However, completely throwing away the device would not be a viable solution. It will in some way reduce the consequences of this problem. However, there are multiple issues with this. First end users will need to be notified whether their device has been compromised and many other actors are involved in this case such as ISPs or maybe even government agencies.

6.2 Manufacturers

The IoT devices in use in Mirai are mainly cheap IoT household devices [3] such as IP cameras. Manufacturers want to sell these devices for a low price and consumers are mainly focused on the prices and the specifications of these devices. As the majority of consumers do not have a strong foundation in the knowledge of cyber security, products will not be advertised as ”Completely secure” as they are either oblivious or put their trust fully in the manufacturers of these devices.

We think, however, we should not blame consumers for their ignorance. These cheaply manufactured devices **should** meet some kind of security standard. Manufacturers should put more effort into the development of these devices which is a risk reduction strategy. Furthermore, manufacturers should be obliged to enroll patches when a vulnerability is known.

Risk acceptance is not a viable solution as we see a major problem now and ”ignoring” the solution will not help this unless other actors will reduce the risks of IoT botnets.

6.3 ISPs

There are multiple risk mitigation strategies. Firstly, This security issue can cause losses for ISPs, as an overcrowded network will make their users complain which result in loss of income and a loss of reputation. As mentioned before, ISPs can directly influence the issue by preventing IP spoofing on the network. These are active measures which is a mitigation risk strategy.

Secondly, The ISP can actively monitor their consumers and thus could detect when weakly protected or even hacked devices are present. If this is the case, they can oblige their customers to either fix or completely block the device. This might be not possible due to current regulations, but they can put some form of compliance onto their customers for the use of their network.

Furthermore, as most of the ISPs in the Netherlands provide consumers with a router, they can also implement better security into these routers in the form of Intrusion detection systems or intrusion prevention systems. A very strict solution would be to completely block telnet connections.

6.4 Government

There are multiple ways governments can reduce the risk. The first would be implement security standards for IoT. Nowadays, there are safety standards for (electronic) products. This can also be done for security. Actively enforce the development of secure products or actively refuse to import devices without these devices meeting some kind of security standards.

A completely different reduction strategy would be through education. The consumers should be able to learn more about the security and the potential hazards of weak cyber security. Nowadays, (nearly) everyone knows what and whatnot is a secure password and how they should be used. In the future, consumers could be also taught how to distinguish weakly secured devices with well protected devices. Also, consumers should be taught on the importance of keeping your devices up-to-date.

Furthermore, governments can put more money and effort in security research. Especially collaboration with other countries. For example, the Netherlands and Singapore worked together on the landscape of IoT security [10].

6.5 Have the strategies changed significantly over time in a way that reduces or increases risk?

In terms of consumers there is not much to be found. However, one of the most promising risk mitigation solution is getting more attention. Implementing security standards for IoT is becoming prevalent in multiple countries. For example, The United Kingdom Government's department for Digital, Culture, Media and Sport has published a report where 5 principles are stated for future IoT development. For example, to reduce the burden on consumers to keep their products secure [11].

Also, the same department has proposed a code of practice for the security of IoT products where the main point of importance is that there should be no use of default passwords in IoT [12]. While reducing the burden on consumer knowledge and improving the secure development of IoT devices, a lot of risk is reduced.

Furthermore, within the telecommunications industry improvement is also present. The GSM association, which is the trade body that represents the interest of mobile network operators worldwide, has developed a assessment checklist which enables the suppliers of IoT products, services and components to self-assess the conformance of their products, services and components to their developed guidelines [13].

Finally, there are improvements in the field of DDoS amplification attacks which can be done by ISPs. Steinberger et al conducted a survey where 77% of the ISP said that they implemented BCP 38, which prevents IP address spoofing and therefore mitigate DDoS amplification attacks which is widely used by IoT botnets [14].

7 ROSI

To determine the value of a mitigation strategy to a certain type of loss event, the Return On Security Investment (ROSI) model can be used. The ROSI equation is as follows:

$$ROSI = \frac{ALE_0 - ALE_1 - Costs}{Costs} \tag{1}$$

where

$$ALE = ARO \times SLE \tag{2}$$

In these equations, the included factors are defined as follows:

- $\mathbf{ALE_0}$: Annual Loss Expectancy - Annual expected financial loss resulting from a type of loss events without the security measure in place.
- $\mathbf{ALE_1}$: Annual Loss Expectancy - Annual expected financial loss resulting from a type of loss events **with** the security measure in place.
- **Costs**: The cost to implement the chosen solution per year. Cost can be split into 2 subcategories: direct and indirect costs.
- **ARO**: Annual Rate of Occurrence - The estimated amount of loss events the company will endure over the course of a year.
- **SLE**: Single Loss Expectancy - Total expected amount of money lost in a single loss event.

For all of these factors, sensible estimates need to be made to be made to be able to produce a realistic ROSI value.

7.1 ROSI for DDoS victims

Since our problem owner is a DDoS victim, we need to define one. We define our victim as a company that hosts internet advertisements. It lets other companies place advertisements on websites connected to its network, and charges the placers of advertisements an amount per click. Websites that allow ads to be placed receive an amount of money per click. Advertisements are embedded in other websites and can be hosted statically. The analyzed solution to DDoS attacks is to host the ads in a Content Delivery Network (CDN). To be able to determine a loss per DDoS event, we need to know the size of our company. We define our yearly profit to be €365,000, or €1,000 per day. We chose CloudFlare [15] as our proposed CDN provider.

7.1.1 Annual Rate of Occurrence

According to Nokia, 78% of malicious software detection comes from IoT botnet activity [16]. One of the main reasons that IoT devices are so popular among botnet operators, is the fact that their security is often denied in the rush to be the first on the market [17]. From our dataset, we can see that the security of IoT devices is indeed still a very large issue and that device vurnerabilities often stay unpatched [1]. The easy availability of insecure devices, makes that DDoS as a service (also called booters) are becoming cheaper everyday. This makes DDoS attacks more likely to occur as time passes.

Once a company is struck by a DDoS attack, there is an 82% chance that it happens again [18]. A study among more than 1000 companies from different sectors revealed that 73% of all companies got hit at least once in 2015 [19]. This study also suggests that in 2015, 45% of the surveyed companies were attacked more than 5 times per year, and 82% were at least attacked twice. As our company is relatively small, we expect to be attacked at most 5 times per year, and at least twice.

$$\begin{aligned} ARO_{min} &= 2 \\ ARO_{max} &= 5 \end{aligned} \tag{3}$$

7.1.2 Single Loss Expectancy

To determine the loss of an isolated DDoS attack, we need to determine the length of such an attack. In Q2 of 2018, most attacks took less than 4 hours, and almost all attacks (98.8%) took less than 50 hours [20]. We set our Single Loss Expectancy to be at least the lost profit of a 4-hour attack and at most a 48-hour attack.

$$\begin{aligned} SLE_{min} &= (4h/24h) \times €1000 = €166.67 \\ SLE_{max} &= (48h/24h) \times €1000 = €2000 \end{aligned} \tag{4}$$

7.1.3 Annual Loss Expectancy

The loss expectancy with the security measures in place should be €0. By hosting all ads on a sufficiently large CDN like CloudFlare, all DDoS attacks can be mitigated. CloudFlare guarantees 100% uptime in their SLA, so (part of) the montly investment is returned in the rare case CloudFlare is down.

$$\begin{aligned} ALE_{0min} &= ARO_{min} \times SLE_{min} = €333.34 \\ ALE_{0max} &= ARO_{min} \times SLE_{max} = €10000 \\ ALE_1 &= €0 \end{aligned} \tag{5}$$

7.1.4 Solution cost

In order to have guaranteed 24/7 DDoS protection from CloudFlare, a business plan would be needed [21]. The costs for such a plan are €200 per month, or €2400 per year. These are direct costs.

In order to transfer to CloudFlare and to perform maintenance. We expect to spend €600 on employee wages per year. These are indirect costs.

$$Costs = €3000 \tag{6}$$

7.1.5 ROSI calculation

With all parameters determined, we can calculate a best-case and worst-case ROSI value.

$$\begin{aligned}ROSI_{min} &= \frac{ALE_{0min} - ALE_1 - Costs}{Costs} = -88\% \\ ROSI_{max} &= \frac{ALE_{0max} - ALE_1 - Costs}{Costs} = 233\%\end{aligned} \tag{7}$$

We can conclude from this that when we receive few and short attacks, setting up a CDN is not cost effective for this size of the company. However, when DDoS attacks take significantly longer it becomes viable to set up a CDN with CloudFlare. Also, when the company's daily revenue grows it would be worth it to invest in a CDN. Perhaps a good strategy to further decide on what the company should do, is to wait for the first attack and measure its duration. It might lose some money in this attack but at least it will not have to spend money unneeded.

Since the given company only loses a €1000 each day, the break-even point of purchasing a CloudFlare subscription is met when the business is hit with a total amount of DDoS attacks that make up for 3 days, or 72 hours. This requirement is met if $ARO = 19$ and $SLE = SLE_{min} = 166$, meaning the company is hit with 19 DDoS attacks of roughly 4 hours each per year. The requirement is also met if $ARO = 2$ and $SLE = SLE_{max} = 2000$, meaning only two large DDoS attacks would be needed to break even.

8 Conclusion

In this report we identified the problem owner to be the victims of DDoS attacks launched from IoT botnets. We compared differences in security performance and see that while some IP addresses have implemented some form of protection, a lot of IP addresses are very vulnerable to IoT botnet malware because they accept connection attempts from any IP address, disclose sensitive software information or use the unencrypted telnet protocol instead of SSH. Different strategies that encompass risk mitigation, avoidance, transfer and acceptance have been evaluated from the point of view of the problem owner. Furthermore, there are many different actors who can mitigate this risk by adopting a wide spectrum of strategies. We see that there are improvements in both the compliance part and the technical part. Governments and standardisation organisations are adopting safe-practice strategies for IoT development. Furthermore, we see that ISPs are adopting ways to mitigate DDoS attacks by preventing IP spoofing. Finally, we calculate the ROSI for the risk mitigation strategy of our problem owner. The result from our ROSI calculation shows that the expected return is heavily dependent on the amount and length of DDoS attacks.

References

[1] C. Hendriks, C. van den Bogaard, S. Bakkum, and R. Colombo, "Economics of security block 2 telnet scans." [Online]. Available: https://github.com/thechib12/EOS_telnet/blob/master/reports/block_2/eos_assignment1_final.pdf

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

[3] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the mirai botnet," in *26th USENIX Security Symposium (USENIX Security 17).* Vancouver, BC: USENIX Association, Aug. 2017, pp. 1093–1110. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[4] ATLAS Security Engineering & Response Team, "Fast & furious iot botnets: Regifting exploits," December 12 2018, accessed on 06.10.2019. [Online]. Available: https://www.netscout.com/blog/asert/fast-furious-iot-botnets-regifting-exploits

[5] K. Whalen, "The consequences of ddos attacks are rising," accessed on 06.10.2019. [Online]. Available: https://www.netscout.com/blog/consequences-ddos-attacks-are-rising

[6] R. Joosten, L. J. Nieuwenhuis *et al.*, "Analysing the impact of a ddos attack announcement on victim stock prices," in *2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP).* IEEE, 2017, pp. 354–362.

[7] Netscout, "How to analyze and reduce the risk of ddos attacks," accessed on 06.10.2019. [Online]. Available: https://www.netscout.com/sites/default/files/2018-07/SECWP_005_EN-1802-How-to-Analyze-and-Reduce-the-Risk-of-DDoS-Attacks_0.pdf

[8] Insurance Journal, "State of the cyber insurance market— top trends, insurers and challenges: A.m. best." [Online]. Available: https://www.insurancejournal.com/news/national/2019/06/18/529747.htm

[9] M. van Wieren, "Cyber insurance: What you need to know, and how to seize the opportunities." [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-cyber-insurance.pdf

[10] Cyber Security Agency of Singapore Ministry of Economic Affairs and Climate Policy of the Netherlands, "The iot security landscape," September 2019, accessed on 06.10.2019. [Online]. Available: https://www.rijksoverheid.nl/documenten/rapporten/2019/09/30/the-iot-security-landscape

[11] U.K. Department for Digital, Culture, Media and Sport, "Secure by design," September 2019, accessed on 06.10.2019. [Online]. Available: https://www.gov.uk/government/collections/secure-by-design

[12] ——, "Code of practice for consumer iot security," October 2018, accessed on 06.10.2019. [Online]. Available: https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

[13] Global System for Mobile Communications, "Iot security assessment," October 2018, accessed on 06.10.2019. [Online]. Available: https://www.gsma.com/iot/iot-security-assessment/

[14] J. Steinberger, A. Sperotto, H. Baier, and A. Pras, "Collaborative attack mitigation and response: a survey," in *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM).* IEEE, 2015, pp. 910–913.

[15] CloudFlare, "Cloudflare - the web performance & security company." [Online]. Available: https://www.cloudflare.com/

[16] Verdict, "Rise of the iot botnet: The problem in securing hundreds of connected devices." [Online]. Available: https://www.verdict.co.uk/rise-of-the-iot-botnet/

[17] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[18] Networkworld, "Hit by ddos? you will likely be struck again." [Online]. Available: https://www.networkworld.com/article/3064677/hit-by-ddos-you-will-likely-be-struck-again.html

[19] neustar, "April 2016 neustar ddos attacks & protection report." [Online]. Available: https://ns-cdn.neustar.biz/creative_services/biz/neustar/www/resources/whitepapers/it-security/ddos/2016-apr-ddos-report.pdf

[20] Kasperky, "Ddos attacks in q2 2018." [Online]. Available: https://securelist.com/ddos-report-in-q2-2018/86537/

[21] CloudFlare, "Cloudflare plans and pricing." [Online]. Available: https://www.cloudflare.com/plans/