Group 1

Mirai Botnet: Security Investments

Rômy Bergman 4369408, Saskia Kooijman 4473795
Jochem van de Laarschot 4227530, Giulio Pellizzari 5143160

07-10-2019

TU Delft
Delft University of Technology

1. Security issue and problem owner

The identified security issue is the growth of a Mirai botnet through IoT-devices. The problem owners of the issue are the ISPs. ISPs are responsible to maintain the network infrastructure and provide end-users access to the Internet. Thereby, ISPs possess data about devices accessing the network, such as the source IP address and ports used to route the internet traffic. Therefore, ISPs have a good position in the network to mitigate the growth of such a botnet. Incentives for ISPs to mitigate the growth of a botnet are heavily debated (Van Eeten et al., 2010; Lone, Moura & Van Eeten, 2014). In the past, DDoS attacks have been performed on ISPs as a consequence of large Mirai botnet formation (Antonakakis et al., 2017; Cimpanu, 2019). In this paper, it's assessed what the impact of such a DDoS attack is on an ISP. It is assumed that if ISPs mitigate Mirai spreading in their infrastructure, botnets size decreases. Therefore, powerful DDoS attacks targeting ISPs and causing them damages such as service unavailability are less likely. It should be noted that this assumption only holds when the majority of ISPs implement mitigation measures to reduce botnet size.

2. Metric security performance

Based on this security issue, two metrics have been defined to give an indication of how IoT botnets can be mitigated. These are:

- Infection rate: percentage of infected devices relative to the total number of devices for each ISP per month. An infected device is defined as an IoT-device which has the Mirai malware installed, thereby turning into a remotely controlled bot.
- The behavior of Mirai botnets: port exploited for the infection over time

Both metrics provide some information about the security performance of ISPs. In the process of deriving at the conclusions, some assumptions were made, which should be noted:

1. A device has been considered infected when its IP was detected by the honeypot. Therefore, each IP present in the dataset has been mapped to an IoT device.
2. To compensate for measurement issues caused by DHCP churning and NAT, the unique IP addresses per day per ASN are analyzed.
3. The ISPs have been mapped to IP using the *Cymru-services* package. The IP addresses are linked to ASNs, which are retrieved in R. Each ASN is assumed to represent an ISP.

2.1 Infection rate: percentage of infected devices per ISP

The line graphs for the first metric show the 3 worst performing ISPs (figure 1a) and the 3 best-performing ISPs (figure 1b) in relation to the percentage of infected IoT devices with respect to the estimated total number of IoT devices. The considered observation period is the month of October 2016 when Mirai DDoS attacks targeted the DNS provider Dyn and Lonaster Cell, a Liberian telecom provider (Antonakakis et al., 2017).

As can be seen from the comparison of the two graphs, the infection rate is different among ISPs. While some ISPs have a concerning percentage of infected devices in their network (e.g. SL-NET-ASN in Poland, Figure 1a), others, such as the three American ISPs of Figure 1b, do not have to worry about that. This comparison shows the relevance of this metric in

support of investment decisions. ISPs can, for example, define a policy that sets an acceptance threshold below which the percentage of bots in their network can be accepted while above it the ISPs have to invest in security to stop the spreading of the malware.

Percentage of infected devices of 3 worst performing ISPs over time

Figure 1a: line graph size of infected devices 3 worst performing ISPs

Percentage of infected devices of 3 best performing ISPs over time

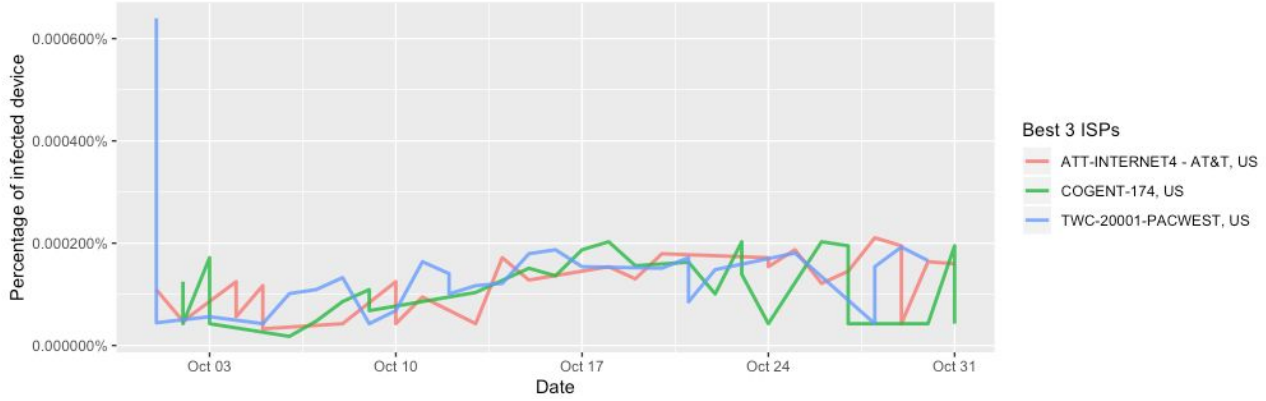

Figure 1b: line graph size of infected devices 3 best-performing ISPs

2.2 Port distribution: ports scanned by Mirai

Secondly, the behavior of Mirai botnets shows which ports are scanned by the malware. The port distribution can also be composed of separate ISPs. Consequently, the scanned ports represent different protocols and traffic. Hence, ISPs in different countries can be advised about which ports should be better protected. For example, port 23 could be primarily scanned in Vietnam and port 5555 in Germany. Besides, the port distribution indicates what devices are the focus of attack because different types of ports can be used to infect different types of IoT-devices. This offers ISPs the knowledge of which IoT devices might be more vulnerable. Therefore, ISPs can implement mitigation strategies more directed to protecting a specific category of IoT devices.

3. Risk strategies

With the performance of different ISPs on the metrics known, ISPs now can apply four categories of risk strategies to reduce the growth of a Mirai botnet. These are **avoiding**, **mitigating**, **accepting** and **transferring** the risk. The possible strategies for the IPSs will be explained in this section.

First of all, the ISPs can **avoid** the risk of a growing botnet by blocking specific ports (Kambourakis et al., 2017). Even though this is a possible strategy, it is not desirable to block a port. Even if Mirai infections can be prevented when ports are blocked, also the other services provided by those ports cannot be used. Therefore, this strategy will reduce customer devices operability. But for the purpose of specifically mitigating the growth of a Mirai botnet, blocking ports is a possible strategy.

Secondly, the security issue can be **mitigated**. An example of a mitigation strategy is awareness campaigns. ISPs can inform end-users about the risk of not changing the default password. This creates awareness about the importance to change default passwords as soon as possible. Besides, clear instructions can be provided to IoT device users about how to clear their IoT device from the Mirai virus. This way, users can clean their own device as quickly as possible from the Mirai virus.
Another mitigation strategy can be to use intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) to respectively detect and block the attempts of infection. These systems scan the traffic over the network and find out what traffic does not comply with their policy. IDSs can only detect what traffic does not match their policy and notify the system administrator about the detected suspicious behavior. IPSs are not only able to detect a suspicious behaviour but they are also able to block it. Therefore they can block Mirai malware spread and mitigate our security issue.

Third, the risk can be **accepted**. Using the security metric discussed in section 2 that provides the percentage of IoT devices infected by Mirai malware in each ASN, if the rate is below a certain threshold, the existence of the botnet could be accepted by ISPs. Only when this percentage is higher than the threshold, the risk of impacts due to a botnet is increasing, therefore, the risk can no longer be accepted. This threshold will be determined by the ISPs.

Fourth, the risk can be **transferred**. This is often done using cyber insurances. Angrishi (2017) discusses cyber insurances for different actors in the chain of events when IoT devices are infected by malware. He states that an IoT device consumer and the target of a DDoS attack can insure themselves against instances such as theft of data, privacy breaches, and network security. Angrishi recommends making cyber insurance compulsory for IoT device users to cover the 1st and 3rd party liability. In the case of ISPs, this gets complicated. The end-user can be held responsible when performing bad security practices, leading to an infected device potentially spreading the malware. Nevertheless, ISPs can be held responsible for mitigating malicious traffic in their network. The asymmetry of the information just described make insurers not aware of the different levels of risk and for this reason, determining risk-based premiums is really difficult and insurers usually adopt fixed premium. However, this choice does not offer ISPs a completely safe way of transferring risk since too bad attacks may not be entirely covered by the insurance.

Another way of transferring risk for ISPs can be to outsource the security to a company specialized in that sector. By signing an agreement with the security company, ISPs transfer the liability to that company. Doing this, in case of an attack, the security company has to pay for the losses that occurred to the ISP. However, as might happen with insurance, too bad attacks may not be entirely covered by the collaborating company.

4. Influence of Other Actors

The ISPs are not the only actors who can have an influence on the spread of the Mirai malware. In this chapter, the different actors who can influence this security issue will be mentioned, together with their possible risk strategies, which may vary over time.

IoT device manufacturers (OEM)
First in the supply chain, are the original equipment manufacturers (OEM). Original equipment manufacturers are producing (parts of) the IoT device, but are not bringing it to the market. As Kolias, Kambourakis, Stavrou & Voas (2017) argue, IoT manufacturers have been producing IoT devices with poor security practices. For example, according to SecurityLedger (2016), hardware combined with software from Chinese manufacturer XiongMai was present in infected IoT devices from multiple brands of IoT devices. When technology brands aren't shipped components with default passwords, botnets such as Mirai will not be able to spread using a dictionary attack. Not shipping with default credentials *mitigates* the risk.

IoT device manufacturers (Technology brands)
When technology brands such as Asus and Digicom (SecurityLedger, 2016) rebrand OEM components and bring the devices under their own name to the market, they also play a part in creating the risk. It seems that these companies accepted the risk of the default credentials. For these tech companies, the risk would be brand damage for being known as not a secure manufacturer. If credentials are changed, clear instructions are provided to end-users or OEM manufacturers are pressured, these would be mitigation strategies.

Retailers
The retailers are the parties who sell the devices to the end-users, online as well as in a retail store. The retailers could play a role in informing the end-users of the need to change their passwords. This is also a mitigation strategy.

End-users
End-users may not know how to harden the security of their devices. (Silva, Silva, Pinto & Salles, 2013). Especially regarding IoT devices, refined permission control is often not feasible due to limited interactions with the device (Bertino & Islam, 2017). The authors note that prevention is the best form of defense and that user awareness is critical since botnet malware mostly spreads through users' mistakes. In terms of risk strategies, end-users should inform themselves and change passwords frequently as a mitigation strategy.

Script kiddies or 'crackers'

As per de Bruijn, Ganan & Van Eeten (2017) crackers, or script kiddies, particularly use botnets to issue DDoS attacks because of their accessibility and easiness in use and their potentially destructive nature. Regarding the security issue, the spread of the Mirai, this group is very influential because the data shows how different versions of the malware developed after the release of the source code. These crackers increase the risk of Mirai becoming more advanced. Since risk strategies for adversaries are deemed out of scope in this paper, it's not further elaborated on how attackers should deal with the risk of being blocked, tracked or obstructed in any other way.

Governments

Governments are in a position to issue specific laws to prosecute cyber-crime. This is most effective when it's consistent and coordinated between countries (Silva, Silva, Pinto, Salles 2013). When a comprehensive legal framework is in place, this could be a risk mitigation strategy in the following ways:

1. By assigning liabilities, security externalities can be internalized (van Eeten & Bauer, 2009). When actors are held accountable for their poor security, rational actors would invest more in their security practices, reducing the spread of Mirai.
2. People would refrain from becoming a botnet *master* when it's more likely that they get tracked down or they would put more effort into the process of securing their devices to prevent infections. This avoids Mirai spreading.

Not only through thorough prosecution governments can push other actors towards more security. Also through other measures, governments can pressurize or incentivize other actors (including ISPs, end-users, and IoT vendors) to fix their insecure practices (Jerkins, 2017). By incentivizing these actors, the problem is tackled at its source. IoT manufacturers are pressured not to use default credentials, end-users are made more aware and ISPs secure their network: this also mitigates the risk due to the spread of Mirai.

Depending on the *infection rate* metric*,* which denotes the amount of infected IoT generated traffic relative to the total number of IoT traffic per ISP, governments may have a certain acceptance strategy as well. When the infection rate is low, government intervention is not deemed necessary and disproportionately expensive. When the issue becomes more pressing and excesses the acceptance threshold, the different mitigation strategies as outlined above can be deployed.

Overall, it can be seen that actors have strategies mainly focussing on changing the default password settings. In the manufacturing phase of the IoT device, the possible strategies are mainly focused on no longer manufacturing IoT devices with default passwords. When these strategies are not used, retailers can advise their buyers to change this as soon as possible, and end-users can be educated and incentivized to do so. Governments have a more coordinating role. These can vary between changing their regulations and laws, to incentivizing the actors in the supply chain to use their own strategies, in order to mitigate the risk of the spread of Mirai.

5. Return on Security Investment Infection Rate

After having identified different actors involved in the security issue and strategies parties can pursue when combating the spread of the IoT malware, this chapter will analyze the investment of one strategy for an ISP. Related to the infection rate of devices as stated in chapter 2 and the goal to mitigate the spread of the Mirai malware, the mitigation strategy of the implementation of an Intrusion Prevention System will be analyzed. IPSs aid ISPs in detecting traffic from infected devices and in blocking this traffic.

Justification for investment will be reasoned using the Return on Security Investment (ROSI). The calculation includes the Annual Loss Expectancy (ALE). First, the monetary loss reduction is calculated by the ALE without a security measure installed (ALE0) and the ALE with a security measure in place (ALE1). Finally, the cost of the solution is subtracted and the amount is divided by the cost of the solution. This results in the following formula:

$$ROSI = \frac{ALE_0 - ALE_1 - c}{c}$$

5.1 The Annual Loss Expectancy without IPS installed

The security issue is reducing the spread of Mirai through ISP-level countermeasures. The consequences of the spread of the malware are DDoS-attacks. Therefore, to calculate the annual loss expectancy, the frequency and impact of DDoS attacks are estimated.

5.1.1 Frequency

NSFocus (2017) concludes that 4.5 DDoS attacks occur per year per company. This is based on a survey with more than 370 security members from different industries.

5.1.2 Impact

The Mirai malware targeted large hosting providers (Antonakakis et al. 2017). As reported by ZDNet, ISPs in Cambodia and Liberia have been attacked through DDoS attempts as well (Cimpanu, 2019). The impact of DDoS attacks on ISPs is calculated using estimations on the length of an attack and the costs of an attack per hour. The costs are split into two categories: direct costs and indirect costs.

Length of an attack

Since large attacks on ISPs are scarce, it's difficult to estimate the length of a DDoS attack on an ISP. ISPs have encountered days-long attacks, but also short attacks on peak hours have been measured (Cimpanu, 2019). It is assumed that the length of a DDoS attack on an ISP follows the same distribution as DDoS attacks in general as shown in table 1 (Kaspersky, 2015).

Table 1: Length DDoS attack

Duration (worst case scenario)	*% DoS causing unavailability*
< 10 minutes	10%
10 min to 1h	21%
Several hours	35%
1 day	14%
2 days to 1 week	9%
Several weeks	7%

Kaspersky (2015) states that 50% of DDoS attacks (in general) cause noticeable disruption and **24%** of attacks result in service unavailability. While these numbers seem high, a recent source discussing an attack on a South African ISP states that attacks on ISPs are *"not that hard to pull off"* (Cimpanu, 2019).

> *Assumption: the only costs incurred by ISPs regarding botnet attacks are when their service becomes unavailable (24%). Occurrences of e.g. noticeable disruption such as reduced up- and download speed are deemed out of scope in this paper.*

Costs of an attack

Next, the costs of an attack *per hour* are estimated. According to an economic analysis of DDoS attacks by NSFocus (2017) direct and indirect costs of service unavailability include:

Direct

- Revenue missed.
- Loss of productivity
- Personel: IT operation / security
- Personel: Helpdesk
- Specialized Consultants
- Customer credits / SLA
- Legal/compliance
- Public relations

Indirect

Damage to brand
Customer Loss
Theft of vital data
Opportunity costs

Tables 2.1 and 2.2 show the specified direct and indirect costs in $/hour. NSFocus (2017) specified direct and indirect costs for three different scenarios. The scenario of a DDoS attack targeting an online retail shop was selected. In this scenario, the DDoS attack caused a complete outage of the online store, leading to the specified costs of revenue missed, personnel IT and personnel helpdesk. An ISP will face similar costs regarding these cost items. However, costs items for legal/SLA, loss of productivity, brand damage and customer loss are retrieved from other sources since they're reasoned to differ compared to an online retail shop. ISPs use Service Level Agreements to assure their (corporate) clients proper availability. To calculate the costs of SLAs breached it's assumed that they have to credit

users their downtime and/or compensate for losses. It's assumed that these legal costs and costs of breaching the SLA equals to the turnover of an ISP. In the example by NSFocus (2017), the company has a turnover of $35 million. This equals approximately $4000/hour. The loss of productivity is based on research by Dubendorfer, Wagner & Plattner (2004). This results in a loss of productivity of $1167/hour and a customer loss of $1997/hour. According to Sinanaj & Muntermann (2013), a data breach costs $20/hour for reputational damage control.

Table 2.1 direct costs

Direct	**$/hour**
Revenue missed	7200
Loss of productivity	1167
Personnel IT	215
Personnel helpdesk	20
Customer credits	11
Legal / SLA	4000

Table 2.2 indirect costs

Indirect	**$/hour**
Brand damage	20
Customer loss	1997

5.1.3 ALE0 calculation

Using the frequencies and impacts (Table 1, 2.1, 2.2) and the introduced uncertainties, the ALE0 can be calculated. To compute the cost distribution with respect to the probabilities described in Table 1, the total costs per hour are first computed as the sum of direct and indirect costs.

$$Cost\ per\ hour\ (C_H) = Direct\ costs + Indirect\ costs = \$14630$$

The result is then multiplied for the different durations reported in table 1 to obtain the corresponding impacts (see table 3).

Table 3 Impact

Duration worst case scenario (D)	*Impact ($I = C_H$ * Duration)*
< 10 minutes (considered 10 min)	$2438
10 min to 1h (considered 1h)	$14630
Several hours (considered 6h)	$87780
1 day	$351120
2 days to 1 week (considered 1 week)	$2457840
Several weeks (considered 2 week)	$4915680

Consequently, for each duration the probability is computed as shown in the formula below. This formula results in the impact distribution as shown in table 4 and plotted in figure 2.

$$P(D = X \wedge ServiceUnavailable) = P(D = X) * 0,24$$

Table 4 Impact distribution ALE0

Duration worst case scenario (D)	*Impact (I = C_H * D)*	$P(D = X \wedge ServiceUnavailable)$
< 10 minutes (considered 10 min)	$2438	2,4%
10 min to 1h (considered 1h)	$14630	5,04%
Several hours (considered 6h)	$87780	8,4%
1 day	$351120	3,36%
2 days to 1 week (considered 1 week)	$2457840	2,16%
Several weeks (considered 2 week)	$4915680	1,68%

Probability of impact without security measure

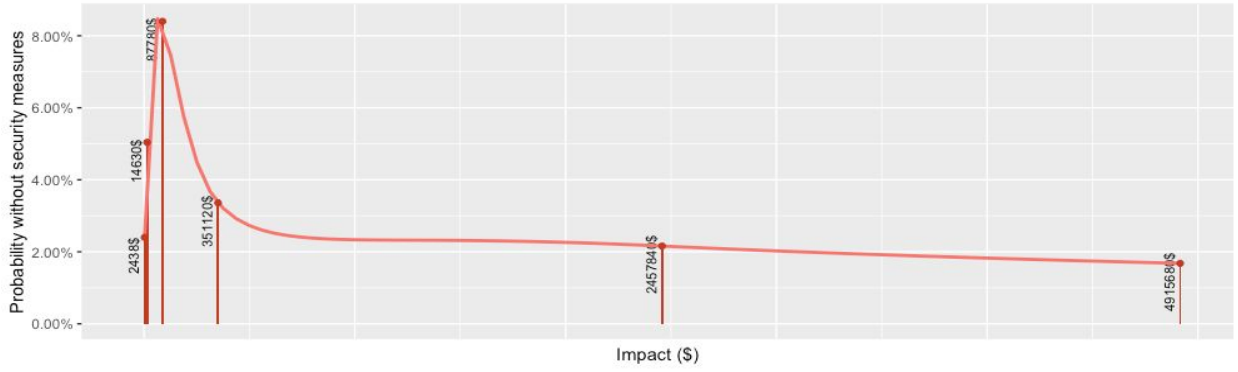

Figure 2 Barchart impact distribution ALE0

From the distribution the expected value for the cost of an attack without security measures implemented can be computed. The expected value of impact for a DoS attack is $155640. Given that NSFocus (2017) stated that 4.5 DDoS attacks occur per year per company, the resulting ALE0 is $700379.

5.2 The Annual Loss Expectancy with IPS installed

The ALE1 costs are the annual costs *with* the chosen security measure. It is assumed that the security measure will decrease the number of infected devices and decrease the likelihood of a DDoS attack on an ISP.

To estimate the effectiveness of the IPS security measure, the works of Al-Jarrah et al. (2016), Meidan et al. (2018) and Kumar & Lim (2019) are analyzed. These authors report techniques to detect infected IoT devices. Al-Jarrah et al. (2016) stated their technique provides a detection accuracy of 99.984%. Theoretically, this means that the implementation

of an IPS would detect almost all infected devices. If every ISP has this system implemented, the spread of the malware will almost completely stop, resulting in no service unavailability caused by IoT botnets. However, (a) since the infections would only decrease if all ISPs in the world would implement measures to prevent the spreading of Mirai and (b) while IoT botnets represent the biggest source of DDoS attacks, they can be performed also from non-IoT botnet. There is still a chance for a DoS attack coming from other kinds of botnets.

Taking the results of Al-Jarrah et al. (2016) and the two reasons illustrated above into account, it's estimated that an IPS solutions brings the successful attack percentage down from 24% to 3%. Therefore, likewise to ALE0, each duration leads to a new probability distribution (see table 5 and figure 3):

Table 5 impact distribution ALE1

Duration worst case scenario (D)	*Impact ($I = C_H * D$)*	$P(D = X \wedge ServiceUnavailable)$
< 10 minutes (considered 10 min)	$2438	0,3%
10 min to 1h (considered 1h)	$14630	0,63%
Several hours (considered 6h)	$87780	1,05%
1 day	$351120	0,42%
2 days to 1 week (considered 1 week)	$2.457840	0,27%
Several weeks (considered 2 week)	$4915680	0,21%

Probability of impact with security measure

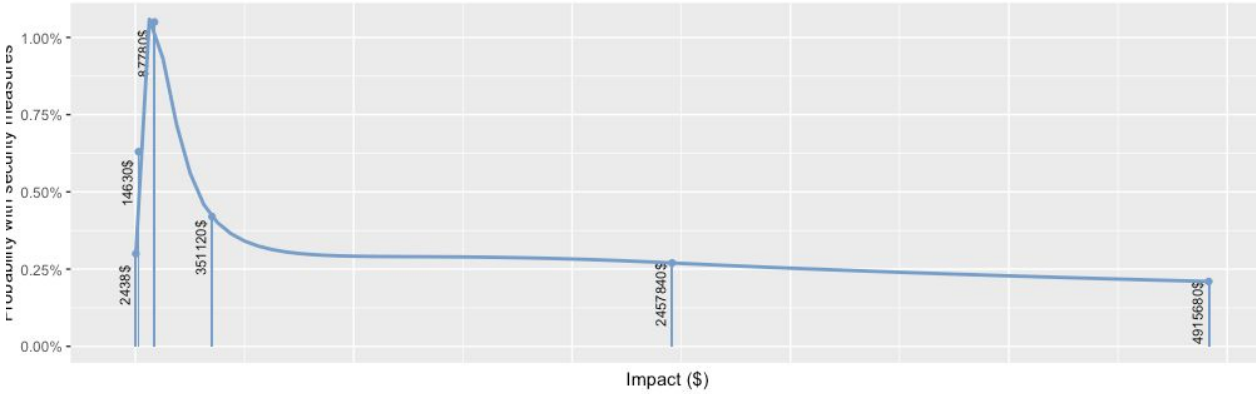

Figure 3 Barchart impact distribution ALE1

Now the distribution with and without security measure can be compared (figure 4). From this figure it becomes clear that the impact and the uncertainty of the magnitude of the impact is greatly reduced.

Comparison probability impact with and without IPS

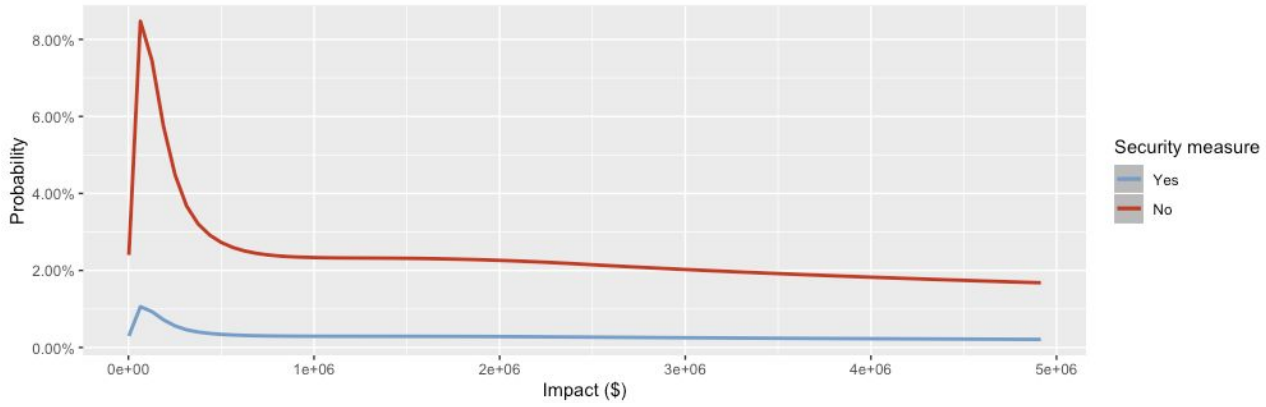

Figure 4: Comparison impact distribution

Finally, the expected loss can be computed after implementing the security measure which results in an expected value of $19455. Considering the 4.5 DDoS attacks per year as shown in the ALE0 calculation, ALE1 equals to $87547.

5.3 ROSI calculation

To calculate the ROSI, not only ALE0 and ALE1 have to be defined, also the costs of the security measure have to be estimated. As reported by NetworkWorld (2016) the cost for a Cisco IPS is $128330. However, this is not the only cost involved. IPS needs to be tuned and maintained, as reported by the SANS Institute (2016). Using this rationale, a total cost of $39720 is estimated.

The ROSI for the first year is calculated according to the formula below:

$$ROSI = \frac{ALE_0 - ALE_1 - c}{c} = \frac{700379 - 87547 - (128330 + 39720)}{(128330 + 39720)} = 265\%$$

However not all costs are recurring yearly. IPS acquisition costs is a constant cost item. Therefore, when considering a projection over 2 years the ROSI increases. In this scenario ALE0 and ALE1 are multiplied by 2, just as the IPS maintenance costs ($39720*2). The costs of the solution over 2 years are then estimated at $207770.

$$ROSI = \frac{ALE_0 - ALE_1 - c}{c} = \frac{700379 * 2 - 87547 * 2 - 207770}{207770} = 490\%$$

6. Conclusion & Discussion

To conclude, the security issue of the growth of a Mirai botnet through IoT devices has been considered. The discussed risk strategies focus on the infection rate metric, the percentage of devices infected by Mirai malware. This metric is the first step in botnet detection and aids ISPs in taking appropriate next steps. Not only ISPs are in the position to take steps in

botnet mitigation. There are also other actors influencing the security issue: OEM IoT device manufacturers, technology brands, retailers, script kiddies and governments. It was concluded that their mitigation strategies revolve around password change practices. Regarding ISPs, the mitigation strategy of implementing an Intrusion Prevention System has been further researched in this paper. This strategy functions to detect and block Mirai malware, directly impacting the infection rate and ideally improving the security issue. In this paper it's reasoned that if most ISPs implement such measures, botnet size decreases. Therefore powerful DDoS attacks targeting ISPs and causing them damages become less likely.

For this mitigation strategy of implementing an IPS, the Return On Security Investment (ROSI) was calculated. When taking a time span of 1 year, the ROSI has been estimated at 265% and over a two year time period a value of 490% is calculated. But does this mean that this investment is worth it? Based on these calculations, the investment gives a positive and increasing ROSI. But given the fact that there is a lot of uncertainty given the numbers used for this calculations, some caution has to be taken into account.

To investigate this uncertainty further, it's necessary to reflect on the numerous assumptions made and the probability distributions as shown in figure 2, 3 and 4. The assumptions fuel uncertainty of the results. First, the direct and indirect costs of a DDoS attack are derived from different sources. Many values are based on a scenario of an online retail shop with a revenue of $35 million. ISPs differ in terms of business model and yearly turnover. For example AT&T is the ISP with the highest worldwide revenue of $170.8 billion (Forbes, 2019). Liberty Broadband has the lowest revenue which is $22 million (Forbes 2019). Having this huge heterogeneity among ISPs influences the estimated impact to great extent. Second, based on research by Kaspersky (2015), the assumption is made that DDoS attacks targeting ISPs cause complete outage in 24% of the cases. When this number is lower, the estimated impact without security measure is overestimated. Third, a probability distribution for time duration of DDoS attacks is assumed based on Kaspersky (2015). When numbers in reality are different from this estimation, the whole shape of the impact curve, both for ALE0 and ALE1 would differ. Fourth, the calculation of the annual loss expectancy with IPS installed is based on the assumption that the likelihood of a DDos attack resulting in full unavailability of the ISP service decreases from 24% to 3%. As set out in this paper, this number will be only a realistic estimation if all ISPs implement security measures. If not, the 3% may be an underestimation and ALE1 will be more like the distribution of ALE0. All of these assumptions incorporate high uncertainty in the ROSI calculation, because these values can easily differ. To provide more clarity for this matter, multiple ROSI calculations should be made based using reliable data regarding different scenarios.

References

Al-Jarrah, O. Y., Alhussein, O., Yoo, P. D., Muhaidat, S., Taha, K., & Kim, K. (2015). Data randomization and cluster-based partitioning for botnet intrusion detection. IEEE transactions on cybernetics, 46(8), 1796-1806.

Angrishi, K. (2017). Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets.

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., ... & Kumar, D. (2017). Understanding the mirai botnet. In 26th {USENIX} Security Symposium (pp. 1093-1110).

Bertino, E., & Islam, N. (2017). Botnets and internet of things security. Computer, (2), 76-79.

de Bruijne, M., van Eeten, M., Ganan, C., & Pieters, W. (2017). Towards a New Cyber Threat actor Topology: A Hybrid Method for the NCSC Cyber Security Assessment. Delft University of Technology.

Bauer, J. M., & Van Eeten, M. J. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. Telecommunications Policy, 33(10-11), 706-719.

Cimpanu, C. (2019, september 24). 'Carpet-Bombing' DDoS attack takes down South African ISP for an entire day. Retrieved from https://www.zdnet.com/article/carpet-bombing-ddos-attack-takes-down-south-african-isp-for-an-entire-day/

Dubendorfer, T., Wagner, A. & Plattner, B. (2004). *An economic damage model for large-scale internet attacks* (Report). Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1376837

Van Eeten, M. J. G., Bauer, J. M., Asghari, H., Tabatabaie, S., & Rand, D. (2010). The role of internet service providers in botnet mitigation an empirical analysis based on spam data. TPRC.

Forbes (2019). *The World's Largest Public Companies*. Retrieved from https://www.forbes.com/global2000/list/#header:revenue_industry:Telecommunications%20services

Jerkins, J. A. (2017). Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code. In 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 1-5). IEEE.

Kambourakis, G., Kolias, C., & Stavrou, A. (2017, October). The mirai botnet and the iot zombie armies. In MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM) (pp. 267-272). IEEE.

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80-84.

Kumar A., Lim T.J. (2019) Early Detection of Mirai-Like IoT Bots in Large-Scale Networks through Sub-sampled Packet Traffic Analysis. In: Arai K., Bhatia R. (eds) Advances in Information and Communication. FICC 2019. Lecture Notes in Networks and Systems, vol 70. Springer, Cham

Lone, Q., Moura, G. C., & Van Eeten, M. (2014, June). Towards incentivizing ISPs to mitigate botnets. In IFIP International Conference on Autonomous Infrastructure, Management and Security (pp. 57-62). Springer, Berlin, Heidelberg.

Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Computing, 17(3), 12-22.

NetworkWorld (2016). *How intrusion prevention costs compare*. Retrieved from https://www.networkworld.com/article/2268117/how-intrusion-prevention-costs-compare.html

NSFocus (2017). *Distributed denial-of-service (DDoS) attacks: an economic perspective.* Whitepaper.

SANS(2016). *Calculating Total Cost of Ownership on Intrusion Prevention Technology*. Retrived from https://media.zones.com/images/pdf/calculating-total-cost-ownership-intrusion-prevention-technology-34745.pdf

Silva, S. S., Silva, R. M., Pinto, R. C., & Salles, R. M. (2013). Botnets: A survey. Computer Networks, 57(2), 378-403.

Sinanaj, G. & Muntermann, J. (2013). *Assessing Corporate Reputational Damage of Data Breaches: An Empirical Analysis* (Conference Report). Retrieved from https://pdfs.semanticscholar.org/122c/19a0a7a7ca8f3f9e532fbff8f45c2468ca9b.pdf