Universiteit of Twente

Economics of Security Course
AY 2018/2019

Internet of Things: Mirai

ASSIGNMENT 2

Authors:
Anna Prudnikova
Giovanni Maria Riva
Federico Casano
Sridhar Bangalore Venugopal

Contents

1 Introduction

IoT Mirai dataset shows the number of IoT devices infected across the different regions over a period of three months. The given dataset was examined with the use of specific tools, such as IBM SPSS, Tableau, and Rstudio. During the previous assignment there were identified:

- security issue;
- the main actor, facing security issue;
- ideal and existing in practice metrics;
- metrics evaluated from given dataset.

The dataset raises a huge security issue - the infection of IoT devices worldwide by Mirai malware. Mirai is a malware, that infects IoT devices and turns them into remotely controlled bots. Attackers scan IPv4 address space of IoT devices, attempt to log-in using a universal default login/password combination or performing a dictionary-based attack of possible IoT credentials and thus gain control of these devices. Furthermore, those infected machines are turned and connected into a so-called botnet, that later on can cause a security issue by performing different types of attacks, such as DDoS attacks, spam sending. At the same time, it can also cause a number of issues not directly related to security, such as losses in computational powers of a device, waste of power, latency and bandwidth issues.

Security issues, raised by dataset, could affect a number of actors, such as companies in different sectors of industry, individuals, governments and internet service providers (ISPs). For our given dataset, we decided to focus on one actor in particular - ISP, as the one, that is most affected by threats of botnets.

2 The problem owner of the security issue

In the previous assignment, we identified the main problem owner of security issues as ISP.

Existing dataset shows around 16200 IP's are listening on port 7547 and around 8000 IP's are on port 5555, (all the others listening on ports 23 and 2323). Mirai is known to attack mostly on port 7547, 5555 (from the point of view of ISP), where ISP links are affected and thus cause significant impact. These two ports are opened on many devices, even though they are supposed to be restricted.

This causes a security issue since the infection of an IoT device by Mirai leads to an attack (spam, DDoS etc) on other actors, which causes ISP potential revenue losses, loss of customer trust and confidence, latency and bandwidth issue, that cause extra costs. At the same time, high network traffic can cause load balancing issues and a high level of discontent from clients.

3 Security performance revealed by the security metric

In the previous assignment we listed the metrics, that could be used by the identified actor to make security decisions.

Among all of them we focused on the distribution of affected IoT devices over time in a particular ISP. It is a stochastic metric, which is computed from the daily distribution of the number of IP addresses within a particular ISP. It is important to notice, that it is a non-deterministic metric, which depends on the attacker's behavior.

Nonetheless, a decision maker is able to understand, if the measures put in place on its system were effective or not. ISPs within the same country might use the metric to compare their performance. As a result, it would be possible to analyze the influence of an attacker behavior.

Figure 1 shows the distribution of affected devices over a period of three months. The number of infected devices is grouped by ISP on a daily basis. It was done to reduce the probability to have a device with dynamically assigned addresses counted more than one time.

Starting from our original dataset, our script queries Team Cymru's IPS-to-ASN mapping service (*http://www.team-cymru.com/IP-ASN-mapping.html*). We retrieved the name of each ISP, to which every IP address belongs to, and computed its total size by summing the sizes of its related autonomous systems' sizes.

To normalize the data, we considered the daily number of infected IPs divided by the size of the relative ISP's size. Figure 2 shows the normalized distribution over three months.

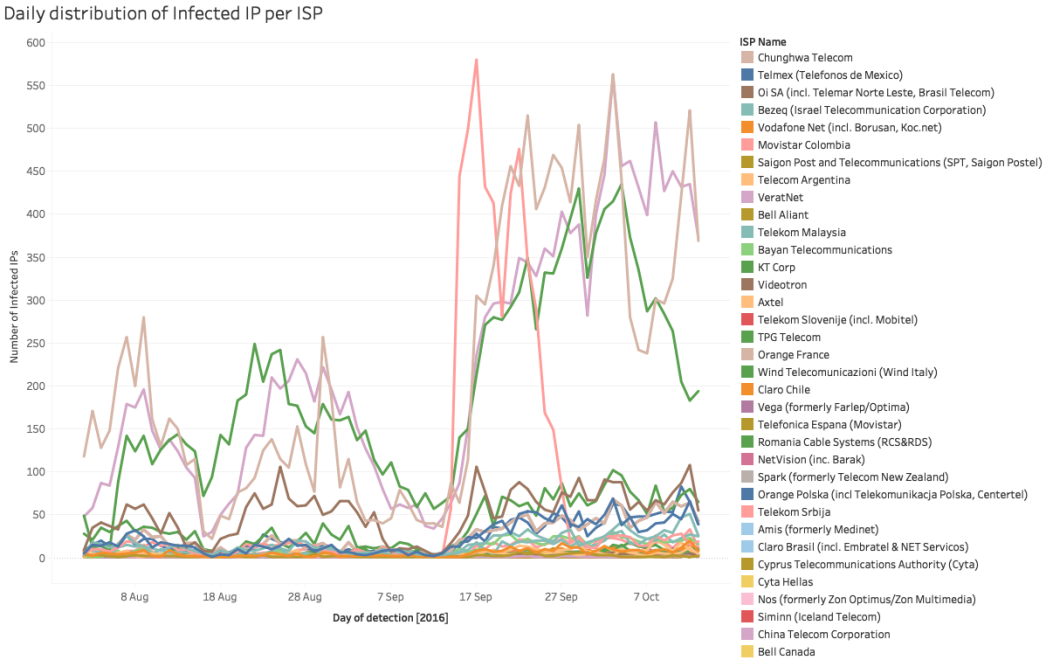

Figure 1: Distribution of infected IoT devices per ISP over days

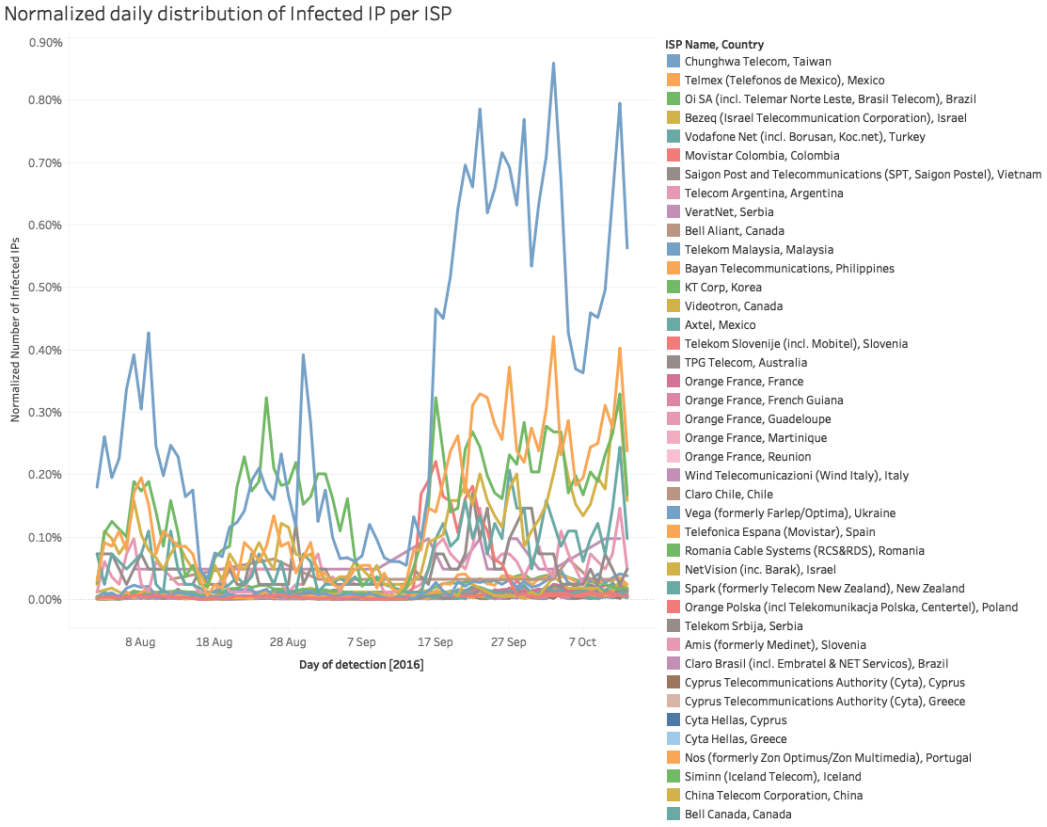

Figure 2: Normalized distribution of infected IoT devices per ISP over days

3.1 Mirai timeline

To evaluate the effectiveness of our metric, we first obtained a retrospective on Mirai malware and analyzed it within our data.

August. In August 2016, the research team MalwareMustDie discovered the Mirai malware [7]. Mirai performed its first attacks on September 19, 2016, which targeted the French host OVH. Subsequently, the source code of the Mirai botnet was uploaded online letting the malware spread all over the world. [10]

October. On October 12, a huge DDoS affected Dyn company, which among all its services also provides DNS services to a lot of big websites. In this period, as the staff at Deep Learning Security observed, Mirai botnets were steadily growing. [7]

December. In December 2016, the author of Mirai was arrested, but the source code was already spread all over the world. [10]

On 12 December 2017, a variant of Mirai was discovered. The malware aimed for a zero-day flaw in Huawei HG532 routers to accelerate Mirai botnets infection. Since early July 2018, at least thirteen versions of Mirai malware has been reported infecting Internet of things devices. [7]

3.2 Security performace evaluation

We can relate these events on the graphs pictured in Figure 2 to analyze the actions taken by the service providers against the malware.

The first peaks can be related to initial spread of original Mirai software and its later variants, once the source code was released. At the time of the biggest Mirai attacks the amount of botnets increased significantly over countries, justifying the huge source of power they originated from.

The increase of attention, caused by the October attacks, probably caused fast decrease of the number of infected devices as a consequence of possible sanitization of every ISP network.

We can see in Figure 3 a positive overall performance of countries such the Netherlands.

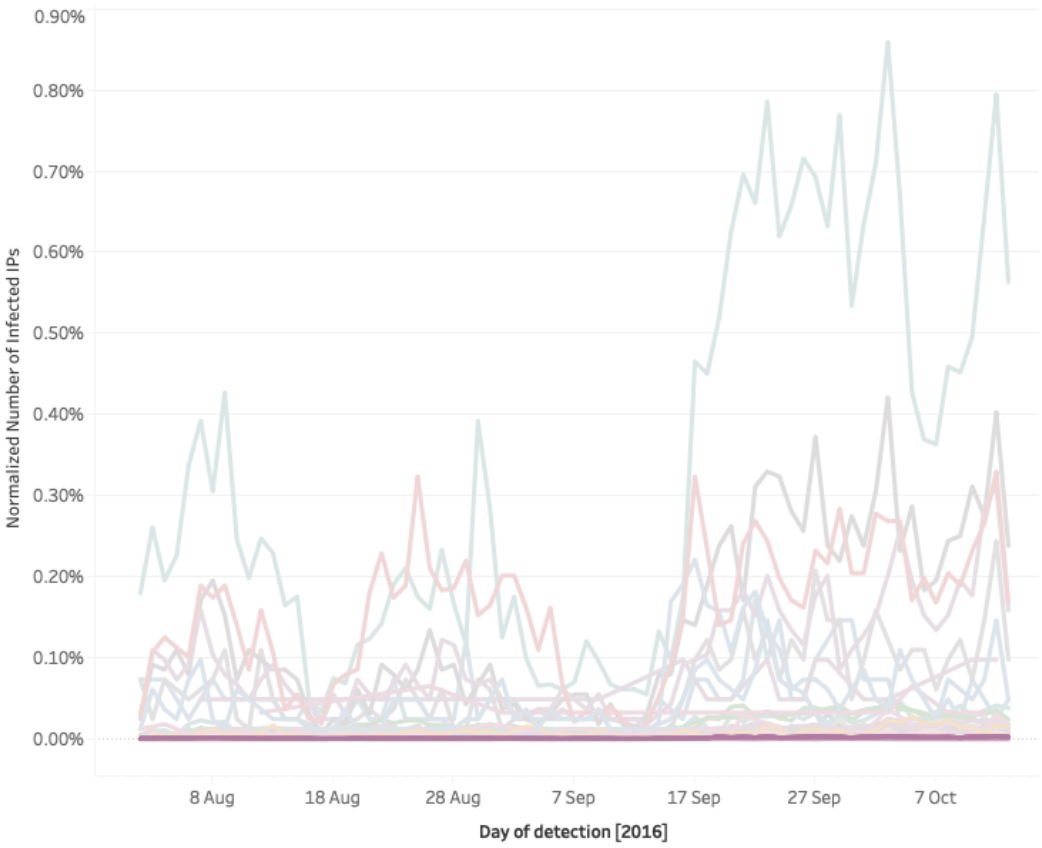

Figure 3: Security performance of Dutch ISPs

On the other hand, countries like Mexico or Taiwan do not have a positive outcome as reported in Figure 4.

The stronger Dutch governmental policies stimulate the service providers to proactively intervene on the issue, while we cannot ensure that the same awareness is risen in the countries with worse performances. However, we also cannot ensure this is happening for the countries which do not show an improvement.

Therefore, our identified security metric could have been the comparator, that might have improved the collaboration between ISPs in order to effectively implement the security measures and result in compliance with policies and regulations.

The combination of efforts of these companies might also effect the possible externalities due to information asymmetries, that are affecting their customers. A new client might not be aware of security when choosing a provider, but base his decision on other factors (es: subscription cost). But with a more homogeneous security level among all ISPs (within the same country) users could feel more secure and less threatened by risks.

On the contrary, we can assume that Mexico or Taiwan, for example, are still facing a higher infection rate due to the information asymmetry, which results from a lower ISP collaboration, that are not using the proposed metric for their security level evaluation.

Given more data (longer period of time, more than 1 year at least) this metric could also be used to understand for a particular ISP, if the security measures, that it implemented, were effective or not (knowing the behaviour of an attacker worldwide). This will require the longer timeline of data due to the fact, that implementing security measures takes time (at least 6 monthes to fully implement the security system) and, thus, cannot be evaluated within a given dataset of 6 months.

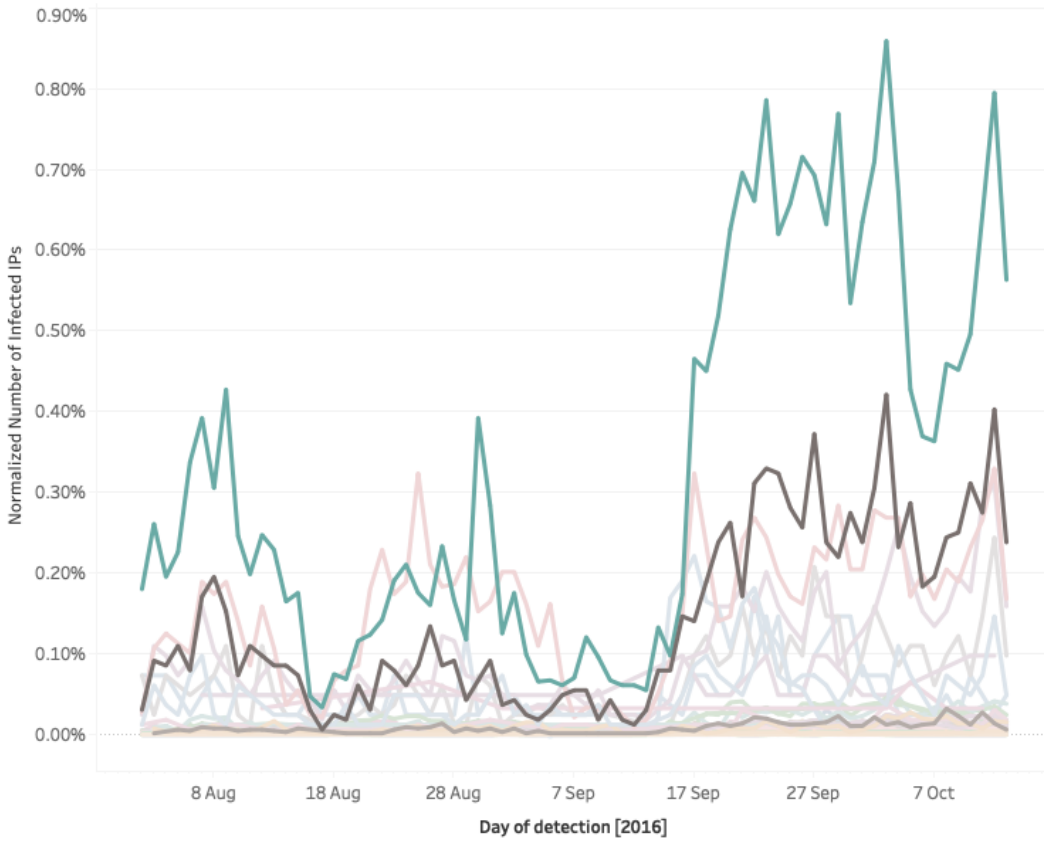

Figure 4: Security performance of Taiwan (blue) and Mexico(brown) ISPs

4 Suggested risk strategies for the identified actor

The risk strategy, that could be implemented by ISP, is risk mitigation (treatment) by means of implementing robust security controls. Risk mitigation decreases the probability of the severity of an unwanted risk, which could potentially damage an organization. Robust security control implementation is an option to reduce the occurrence or severity of the risk. Those controls are based on best-practice anti-botnet and monitoring strategies.

Strategy, which an ISP could use to solve the problem of IoT infections, is to implement a threat intelligence system, which shows potential or current attacks for the resources. Such a system measures a number of incidents (shown from monitoring system) and determines the rate of affected machines by that reducing the risk. Combining multiple strategies can make an effective sustainable long-term plan for ISP.

Below there are listed some more approaches, which ISP can follow to minimize the IoT bot infections. [1]

Network behavior anomaly detection (NBAD) which continuously monitor the network for unusual events or trends. Monitoring system cost lies on implementation, management and support.

Additional controls, that could be implemented:

Call center. ISP can notify internet users about infections which are shown in a monitoring system and thus avoid further damage.

Security information and event management (SIEM) is an approach for security management, which gathers events from network equipment and specialized security equipment like firewalls, antivirus or intrusion prevention systems.

Log management is used to analyze and store log data created within an information system and useful to produce historical event rate per duration.

Network forensics is used to capture, record, and analyze network events for the purpose of discovering the source of security attacks or other problem incidents.

An alternative strategy for ISP could be risk acceptance, that includes documenting the ongoing risks. Risk acceptance could be implemented in case, when a company doesn't have enough resources (financial or personnel) to effectively mitigate the risks or if the mitigation measures cost more than the possible losses could be.

As yet another strategy, ISP can use risk transfer by using insurances for their cyber security risks. This approach is not commonly used nowadays due to a number of factors, explained in the next paragraph.

5 The influence on the security issue by other actors

As was mentioned before, there are a number of actors, that could influence the security issues, raised by the dataset. That includes governments, companies, owning IoT devices (that also could include routers), ISPs, end users of IoT devices. All those actors can influence the security issue in different ways and by implementing different strategies. The most important strategy for all actors is risk mitigation.

The first researches on botnet mitigations suggested that end users are the main actors in fighting against the botnet threat, because it is their devices that being infected by malware. For our particular case of Mirai malware, the way to fight the threat is quite obvious and coming from the nature of Mirai Malware itself.

Firstly, users of IoT devices must never use default passwords.

Secondly, users must avoid a single point of failure, one vulnerable device could allow an attacker to penetrate your home network and pivot to other devices, passwords must be complex and unique to minimize the effect that a single compromise could have.

Finally, users must keep their IoT devices updated with the latest vendor firmware, it is highly recommended to always check for all possible updates when purchasing a new device.[8]

As for the companies (owning IoT devices), the measures they can implement are mostly merged measures of end-users and ISPs.

Even though it is common to think, that the main party to mitigate botnet threat, is an ISP, governments can also play a significant role in a mitigation process. In short, policies that enforce ISPs appear effective, particularly when they take the form of national anti-botnet initiatives. However, the centers' impact shouldn't be overestimated.

The extent, to which ISPs respond to these reduced costs, will differ. In an evaluation of the Dutch initiative we found that, even though large ISPs received the same data feeds, if and when they acted on this data differed among providers, as evidenced by the fact that their relative infection rates continued to differ by a factor of three to five. We see similar variation in other countries with a national initiative. In the end, anti-botnet initiatives seem to nudge provider policies in the right direction but don't dictate them. We also see that policy impact is modest when compared to contextual factors such as the rate of unlicensed software use. Of course, a policy can also try to influence piracy rates—and, in many countries, it does, as part of their intellectual property protections. This raises an interesting policy option for botnet mitigation: focusing on the ICT infrastructure's general health might be the most effective way to reduce the societal burden of botnets. National initiatives change ISP incentives in several ways.

First, a national initiative demonstrates government involvement, which puts more pressure on ISPs to invest in security. Second, a national center reduces mitigation cost for ISPs, enabling them to increase their impact with the same resources. For example, the Netherlands' centralized clearinghouse, called AbuseHUB, is partially government funded. It sets up relationships with suppliers of abuse data, such as the ShadowServer Foundation and Microsoft. It has also automated the parsing of this incoming data and feeds it directly into member ISPs' automated abuse incident response processes. All this reduces ISP costs and scales up mitigation. Anti-botnet centers in other countries, such as Korea and Germany, provide actual customer support via a publicly funded call center. This shifts some of the mitigation cost to the taxpayer, reducing the burden on ISPs.

The problem of botnets isn't located in the networks of shady ISPs in countries with poor governance structures. Well-known and well-established ISPs in relatively well-governed jurisdictions control the bulk of the problem. [11]

6 Alternative risk strategies

All actors mentioned above can use the strategy of **risk mitigation** by implementing security controls.

At the same time companies and ISPs can also accept the risks (**risk acceptance**), in case, if they are not legally bound by policies to implement extra controls (e.g. ISPs in the Netherlands).

To be able to do that, they must document the decisions to accept risks and adjust cyber risks acceptance to a general business risk strategy.

The companies (owning IoT devices) and users can also use the strategy of **risk avoidance** by refusing to use IoT devices at all or disconnecting them from the Internet. In practise, this approach is not feasible, since today we live in a cyber world and depend on techologies in our daily lives.

The latest trend in cyber security is a **risk transfer**. This strategy could be implemented mainly by companies owning IoT devices and ISPs. The main way to do that is cyber risk insurance. In theory, it should help to make financial impact of cyber risk more predictable. In practice, this risk strategy is not really popular, due to the lack of historical data, low demand, and legal uncertainties.

Since the IoT Mirai threat is relatively young, the risk strategies haven't changed significantly over time. The only thing, that changes and evolves over time is the type of controls to mitigate risks, implemented by companies, ISPs and Governments. While Governments tend to implement more organizational security measures to fight botnets by enforcing policies, companies and ISPs tend to implement more technical controls. The reason is not just because they are forced to, but because they start to realize, that investing money into preventing a threat from happening, could bring them more benefits.

7 Return of investment

7.1 Costs estimation

The strategy, that is most common to use between all actors is risk mitigation. We are going to focus on risk mitigation by implementing extra technical measures by ISPs. To calculate the costs involved in following the strategy, we need to calculate the costs of implementing measures, listed in part 2 of the report. The costs include direct costs (sum of expenses for acquisition, deployment, maintenance) and indirect costs (productivity loss, opportunity costs of decisions with incomplete information). In our case, direct costs include:

	The measure	The cost of deployment	The cost of maintenance
1	Network Monitoring system	3000 $ per device, average number of devices 25 for ISP	30k $ per year for an engineer + 18k $ for annual TAC support
2	Call Center	5000 $ for Logistics	20k $ per year for an engineer
3	SIEM	11k $ per on-premises solution	25k $ per year for an engineer
4	Log management	2100 $ per annual support	20k $ per year for an engineer

Indirect costs, which are associated with consumers in security environment using ISP service are shown below.

	The value	Productivity loss	Impact
1	SLA breach	150 $ per hour for every incident	High severity for connection failure
2	Bandwidth reduction	120 $ per hour	Medium severity for latency

For our future calculations we are going to use following measures, as the most suitable ones for price/effectiveness:

- Implementing a network monitoring system: 3 000$ * 25 once, 48 000$ per year for support;
- Organizing a Call-center: 5 000$ once + 20 000$ per year for support;

7.2 Benefits estimation

In order to calculate the benefit of following the strategy we need to understand the prevented losses, if we implement proposed measures. Normally, it might be calculated as a shift between loss distribution with / without implemented measures.

We can simplify, by saying that security benefit minus cost is an expected prevented loss (the bottom line of ROSI formula). The ROSI can be calculated as followed:

$$ROSI = \frac{benefit - cost}{cost}$$

$$ROSI = \frac{expected\ prevented\ loss - cost}{cost}$$

$$ROSI = \frac{(ALEo - ALEs) - cost}{cost}$$

$$ROSI = \frac{Riskexposure * effectiveness - cost}{cost}$$

- **ALEo**: annualized expected loss without security measures;

- **ALEs**: annualized expected loss with security measures,
- **Cost**: cost of proposed security measures;

The challenge here lies in calculation of prevented expected loss. As was said before, the negative effects of botnet threat for the ISP are: lost of customers trust (ISP reputation), network performance issues (ISP infrastructure overload), legal issues, extra outbound peering costs.

We can use a data breach of UK ISP TalkTalk [9]. As reported by TalkTalk, they lost a $£15m$ *"arising from Q3 disruption"* in 2015, as 101,000 customers fled the provider and later £20m disappeared in lost revenue due to having a lower customer base for its fourth quarter. The overall number of clients of TalkTalk was around 3.9 million in 2016, meaning, that around 3 percent were lost to the ISP, because of the cyber security issue.

Also we can estimate the extra outbound peering costs (knowing the number of bots within the ISP, the costs of traffic, how much traffic 1 bot uses). In order to do so, we can take the percentage of overall IP traffic, that was generated by "bad" bots, translate it into gigabytes (knowing the overall world traffic per month) and divide by the number of bots. Since out dataset contains data on 2016 year, we will use statistics from this year later on. The data from those sources:

- Traffic, generated by "bad" bots: 19.9% [2];
- Overall traffic per month: 96 054 petabytes [3];
- The overall number of bots: 98 600 000 bots [4];

Thus, we can estimate, that per month one "bad" bot generates:

$$\frac{96‘054‘000‘000\ GB * 0.19}{98‘600‘000} = \frac{185\ GB}{month * bot}$$

Since bots do not perform 24/7, we can estimate, how much traffic 1 bot generates per day:

$$\frac{185}{30} = 6.1\ GB.$$

According to [5] , the cost for a large incumbent ISP to deliver one gigabyte of data — when you factor in fixed costs like fibre optic cables and networking gear, as well as operating costs such as technicians and electricity — can range anywhere from a few pennies to between 10¢and 15¢per GB.

So, one single bot costs ISP around 1 dollar per day.

To add the uncertainty, needed for ROSI to be meaningful, we are going to calculate the probability of a device to be infected based on our dataset. Since ROSI is normally calculated for a particular company to make security decisions, we are going to calculate it to 1 particular ISP - KT Corp (Korea), which performance in reported in Figure 5

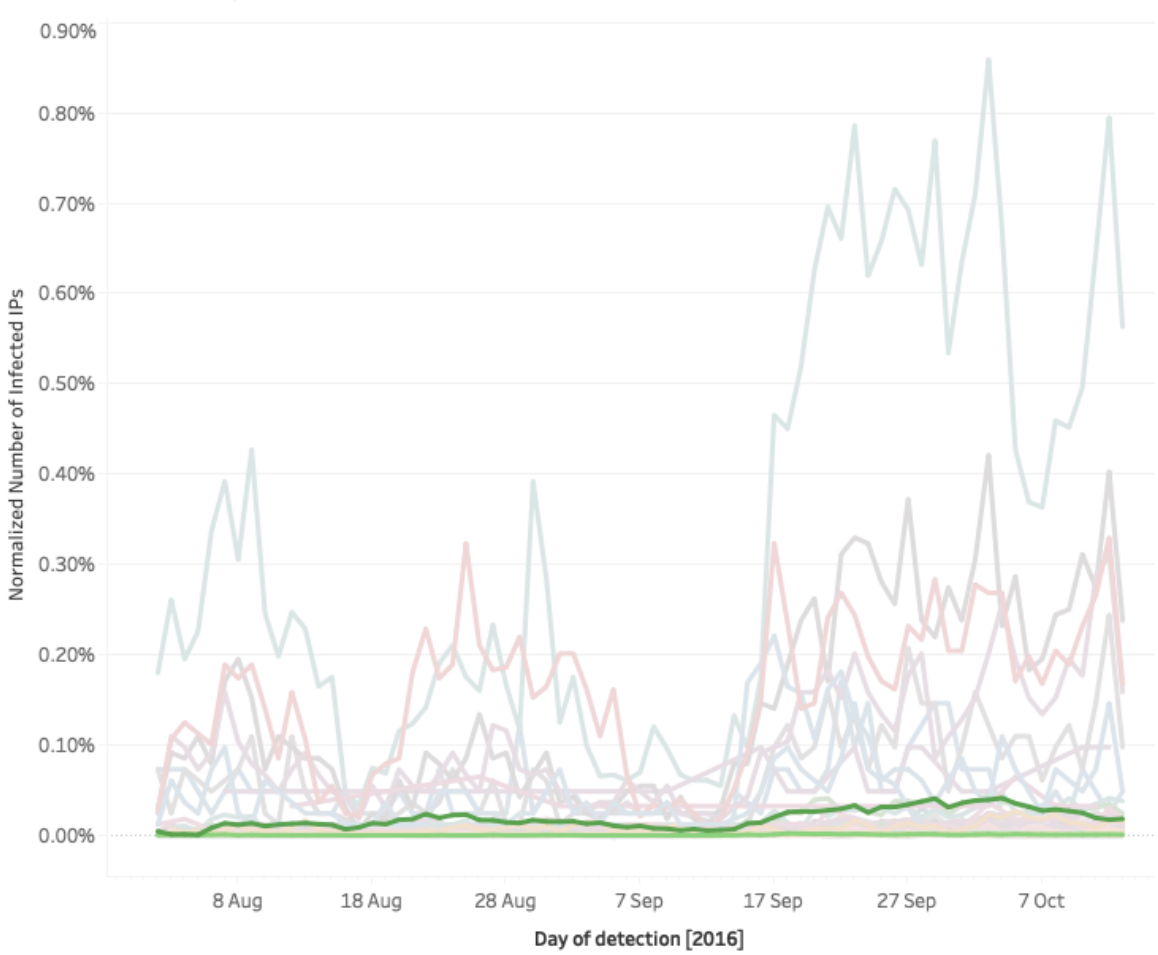

Figure 5: Security performance of KT Corp ISP

Firstly, we are going to calculate the losses due to the bot infections, that is going to be a distribution over time.

Secondly, as was said before, we can estimate, how much money they can lose, due to the loss of reputation and customers' trust. The revenue of KT Corp in 2016 is 17 *trillion* korean wok. If we translate it to dollars (taking the currency exchange rate in 2016) - 14 *billion dollars*. We predict the possible loss of clients as 3 percent, so the overall loss of revenue will be: **425 million dollars over 1 year.**

The calculations for Annualized Expected Losses with added uncertainty are given in Annex.

7.2.1 ROSI calculation

The methodology used to make calculations is as followed.

Step 1. First, we calculated the ALEo without security measures for original scenario.

As was said before, it consists of 2 types of losses: direct losses for payments for extra traffic generated by bots plus the possible losses of clients and revenues due to trust and reputation issues.

1. To calculate the probability of a device to be infected, we took the minimum and maximum number of infected devices per day for KT Corp in a given timeline, than calculated the average number of infected devices per day and later divided it by the overall number of IP addresses used for IoT devices.

   According to [6] around 10 percents of all users of services of ISPs are using it for IoT devices. Our data shows, that there are 14 294 IP addresses within KT Corp, meaning that at least 1 400 belong to IoT devices and can be potentially infected.

$$Pr = \frac{\frac{8+435}{2}}{1400} = 0,31.$$

2. To calculate the losses due to extra payments for traffic we took the minimum and maximum number of infected devices per day and multiplied it by 365 to get an annualized loss.
   - Min loss due to extra traffic per year $= 8 * 1\$ * 365 = 2'920$ \$ per year.
   - Max loss due to extra traffic per year $= 435 * 1\$ * 365 = 158'775$ \$ per year.
3. The losses of revenue due to clients losses are explained above. We assume minimum loss of 1 percent of clients and maximum of 3 percents.
   - Min loss due to loss of clients per year $= 14\$\ billion * 0.1 = 141'666'666\$\ per\ year$
   - Max loss due to loss of clients per year $= 14\$\ billion * 0.3 = 425'000'000\$\ per\ year$

   The final values of ALEo (risk exposure):

$$Min\ ALEo = (2'920 + 141'666'666) * 0.31 = 42'500'876\$\ per\ year.$$

$$Max\ ALEo = (158'775 + 425'000'000) * 0.31 = 127'547'632\$\ per\ year.$$

Step 2. Secondly, we applied Monte Carlo simulation to calculate the average risk exposure.

1. We used the normal gaussian distribution for Monte Carlo simulation of 100 experiments. In order to do so, we calculated the mean and the deviation of ALEo.
2. To calculate the average risk exposure we took the sum of all positive values of simulations and divided it by number of simulations.

The average risk exposure = 94 214 010$ per year.

Step 3. Thirdly, we calculated the cost of proposed measures per year.

$$The\ cost = 3'000 * 25 + 30'000 + 18'000 + 5'000 + 15'000 = 143'000\$\ per\ year.$$

Step 4. Finally, we calculated ROSI for different effectiveness of our proposed measures. Since the proposed measures are relatively cheap comparing to possible losses, even in case of 1% of effectiveness our ROSI stays a positive value.

1. The ROSI for 1 year for different effectivenesses is shown below.

Effectiveness	ROSI
1%	5%
10%	65%
20%	131%
30%	197%
40%	262%
50%	328%
60%	394%
70%	460%
80%	526%
90%	591%
100%	657%

2. To include uncertainty into our calculations, we used Monte Carlo simulation (100 experiments). As minimum effectiveness of proposed measures we used 20%, as maximum 70%.
   - The average effectiveness = 45%.
   - ROSI for 45% effectiveness = 295% for 1 year.

Figure 6 shows the different computed ROSI according to an increasing level of effusiveness of our provisions.

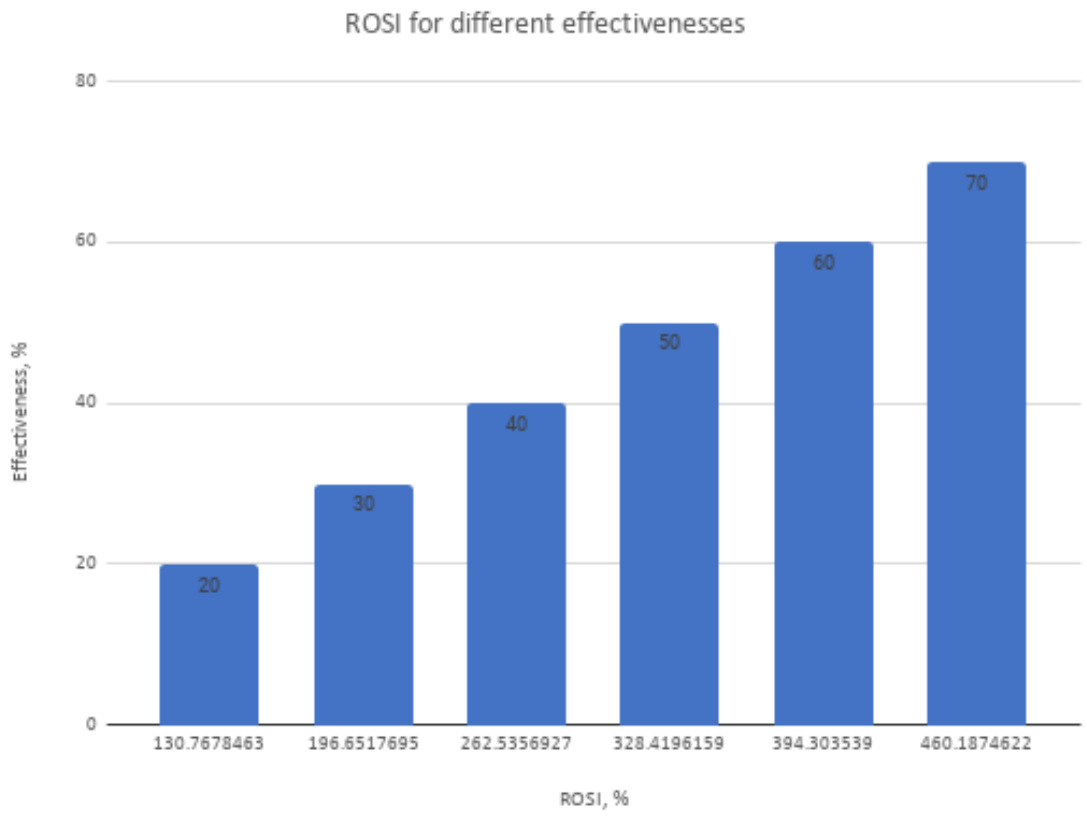

Figure 6: Computed ROSI according to different effectiveness

3. We also estimated ROSI for the period of time of 2 and 3 years, considering that we would lose more every year, but at the same time pay more salaries. The network equipment we don't change, so we don't pay for the second and the third year.

   - ROSI for 2 years = 410%.
   - ROSI for 3 years = 470%.

   Figure 7 contains a three year forecast of the ROSI trend according to the chosen effectiveness.

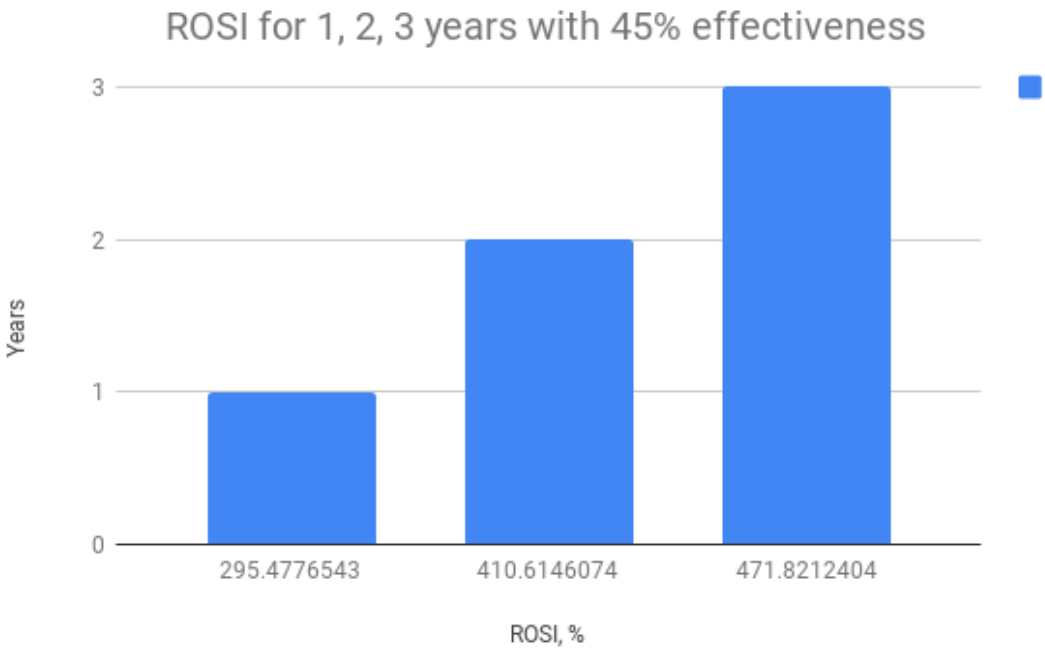

Figure 7: Three ROSI forecast according to the chosen effectiveness

8 Conclusion

During this assignment we identified all actors, involved in a security issue, discussed the strategies, they can implement to fight the threat of botnets, evaluated the metric to compare the performances of chosen actors and estimated the ROSI for one particular actor.

ISP is the main actor in our scenario, as the one most affected by security issue identified in the previous assignment. To compare performances of different ISPs in different countries we chose the metric that shows the normalized distribution of infected IoT devices per ISP over days. This metric was chosen to be able to compare the performances of different ISPs, taking into consideration the knowledge of Mirai timeline, that could explain the behavior of an attacker. As we saw, some ISPs in particular countries (e.g. the Netherlands) implemented security measures to fight the threat of botnets (due to Government's policies enforcement and collaboration among ISPs), that were effective. We came to this conclusion, because, even in case of massive botnet infections in particular times, distribution of a number of infected IoT devices in Dutch ISPs was more or less stable, comparing to other countries (e.g. Mexico), where there might not have been enforced governmental policies or other initiatives to fight botnets. That leads to a further conclusion, that joint efforts of internet providers and Governments could significantly reduce the threat of botnets.

As other actors, involved in the security issue, we identified companies (owning IoT devices), Governments and users. All of them could implement different risk strategies to influence the identified security issue, best one being risk mitigation strategy. Companies and users can avoid risks by refusing to use IoT devices or by disconnecting them from the Internet but in practice is not possible. Companies and service providers can also use the strategy of risk transfer by relying on insurances. Alternatively, when providers are not legally bound to some enforced policies, the best approach would be to accept the risks.

As the last step of our assignment, we calculated ROSI for one particular ISP: KT corp (South Korea). Since our dataset doesn't have enough data to compute precise calculations, we added uncertainty by using Monte Carlo simulation. We calculated the ROSI for different levels of effectivenes for the proposed measures (since we cannot be sure, how succesffull they will be). In our particular scenario, even 1% of effectiveness gives a positive result for ROSI, since the cost of proposed measures is relatively small (thousands of dollars) compared to the amount of losses that KT corp could face from a botnet threat (millions of dollars). Besides, we estimated ROSI for 2 and 3 years, to understand the way ROSI will change over time. As we saw, with every year ROSI will get higher (with fixed effectiveness of the security system).

References

[1] *Security intelligence*, 2018 (accessed February 01, 2015). https://whatis.techtarget.com/definition/security-intelligence-SI.

[2] *2017 Bad bod report)*, 2018 (accessed October 01, 2018). https://resources.distilnetworks.com/i/798906-2017-bad-bot-report/39?

[3] *Global IP data traffic from 2016 to 2021 (in petabytes per month)*, 2018 (accessed October 01, 2018). https://www.statista.com/statistics/499431/global-ip-data-traffic-forecast/.

[4] *Global IP data traffic from 2016 to 2021 (in petabytes per month)*, 2018 (accessed October 01, 2018). https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf.

[5] *How much does bandwidth actually cost?*, 2018 (accessed October 01, 2018). https://business.financialpost.com/technology/how-much-does-bandwidth-actually-cost.

[6] *IoT service subscribers near 6 million in Korea*, 2018 (accessed October 01, 2018). http://www.koreaherald.com/view.php?ud=20170705000680.

[7] *Mirai (malware)*, 2018 (accessed October 01, 2018). https://en.wikipedia.org/wiki/Mirai_(malware).

[8] *Post-Mirai, how to better protect your IoT devices*, 2018 (accessed October 01, 2018). https://www.grahamcluley.com/protect-iot-devices/.

[9] *TalkTalk admits losing £60m and 101,000 customers after THAT hack*, 2018 (accessed October 01, 2018). https://www.theregister.co.uk/2016/02/02/talktalk_hack_cost_60m_lost_100k_customers/.

[10] *The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet*, 2018 (accessed September 29, 2018). https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html.

[11] Hadi Asghari, Michel JG van Eeten, and Johannes M Bauer. Economics of fighting botnets: Lessons from a decade of mitigation. *IEEE Security & Privacy*, 13(5):16–23, 2015.

Appendix.

Excel calculations.

The revenue in 2016 of KT Corp

17,000,000,000,000.00	in korean won	
1 dollar = 1200 $ in 2016		
The revenue in 2016 in $	$14,166,666,666.67	14 billion
The loss of 3% of customers (3% of revenue)	$425,000,000.00	
The loss of 1% of customers (3% of revenue)	$141,666,666.67	Deviation
mean	$283,333,333.33	200346921.3
min number of infected IP adresses	8	
max number of infected IP adresses	435	
mean	221.5	
min number infected IP adresses costs	$8.00	
max number infected IP adresses costs	$435.00	
mean	$221.50	Deviation
mean over year	$80,847.50	150.9672978
mean for both losses	$283,414,180.83	
The probability of a device being comnpromised	(min infected IP + max infected IP)/ overall number of IP used for IoT devices	
0.3164285714		
min losses over year	$42,500,876.00	
max losses over year	$127,547,632.50	
mean	$85,024,254.25	
deviation	$60,137,138.24	
We keep 1 average exposure for further calculations	**$94,214,010.13**	
Average exposure (random)	$97,863,821.18	

Monte Carlo simulation for losses

52496269.58
168867855.6
113304925.3
94122065.93
104114342.5
165851667.8
131278859.2
109866815.9
110544898
172974175.1
77816279.94
176782792.2
32047461.21
130607228.8
156555294.7
120005004.8
123968227.1
36331164.97
33299022.66

97504476.77
179338387.7
47450439.75
203209226.7
4206478.367
93429023.73
112214222.5
16694816.13
50018184.41
152731450.4
122109630.9
84138552.27
-6164273.778
27555218.7
111997826.9
84064055.7
-12722196.7
126781666.1
142817779.6
127666630.7
135843143.8
244666973.3
137150126.1
67089881.87
15928901.07
61309767.75
81649555.55
155734985.2
155564631.8
28898365.78
169127188.8
87597297.31
100385841
77507691.49
34224304.54
152989353.3
83162668.85
-5552287.092
97873259.77
147624567.3
79429999.5
107372665.4
163456780.1
87541751.27
82348705.28
21850711
114349647.9
10250799.59
141935461.7
87132778.25
40446947.08
112538438.8
149803943.4
156256182.1
165893639.1
101076440.6
96473081.11
98806440.6
181505408.2
-21126995.84
69118260.75
62003552.52
40892637.58
-65996581.56
126775556.2
75206800.24

	14121904.69
	94758603.39
	82731598.76
	115304526.9
	123804918.8
	140392308.2
	73270507.52
	88229542.08
	223319144.6
	7483203.473
	75112174.98
	110670648.6
	66349539.13
	138989666.9
	130286278.1

Cost of security measures

cost 1 year	$143,000.00
cost 2 years	$206,000.00
cost 3 years	$269,000.00

143000

ROSI calculation

ROSI for 1 year	((average risk exposure * % risk mitigation effectivness) - cost)/cost	
effectivness 1%	5.588392317	
effectivness 10%	64.88392317	
effectivness 20%	130.7678463	20
effectivness 30%	196.6517695	30
effectivness 40%	262.5356927	40
effectivness 50%	328.4196159	50
effectivness 60%	394.303539	60
effectivness 70%	460.1874622	70
effectivness 80%	526.0713854	
effectivness 90%	591.9553085	
effectivness 100%	657.8392317	
Effectiveness min	20	
Effectiveness max	70	
Mean	45	
Deviation	35.35533906	
Average effectiveness	47.08222251	
The fixed one	45 %	
ROSI for 45% for 1 year	295.4776543	1
ROSI for 2 years	410.6146074	2
ROSI for 3 years	471.8212404	3
Monte carlo simulation for % of effectiveness	82.71308943	
	71.04497735	
	89.95827988	
	68.61047436	
	85.03549834	

37.37959633
58.78586979
70.60897357
46.41792116
78.33452444
-11.33059023
9.084734251
40.78581574
69.71355724
36.63452643
51.04502839
45.49201042
103.7083445
-9.372719765
37.51347461
26.44207886
37.66595198
75.25536479
47.75866904
58.22306663
59.94814323
145.2873855
10.88694281
-3.974911996
65.17984606
25.78567898
48.5911511
34.88868888
72.09564782
-3.485689661
28.79978
58.64880725
-8.966328853
29.24927135
92.77612495
68.04703503
60.81412876
53.6055307
76.50908533
53.73266151
35.835793
41.35732528
17.67734956
69.52090016
112.430067
31.37814224
60.07623198
-10.33235152
54.35659827
1.528571413
64.11543268
13.8416892
54.29359478
25.5001087
64.16617428
-28.95122025
45.77575653
6.801043585
9.09525682
31.173176
39.20921396
86.84301674
36.70780771
63.04975256
23.22525337
51.24928582

35.54452979
18.36359675
100.4170007
27.23662287
56.82949348
75.006128
21.3448032
-7.524597438
74.77388675
34.98855843
56.03912519
65.51888853
27.3357431
66.29376636
65.9722346
-5.670783672
41.42173675
24.37599057
2.52198191
-36.48620544
27.90985572
99.71001438
99.69247656
60.69784035
87.99109318
84.45391854
16.87146854
84.64621823
-11.16759384