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 device infected across the different region over a period of six 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. They 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 the 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 particular 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), which causes potential revenue losses, loss of customer trust and confidence, latency and bandwidth issue. At the same time, high network traffic can cause load balancing issues.

DDoS only could have a huge impact on ISPs. IT professionals ranked the loss of customer trust and confidence as the worst effect of a DDoS attack (42%), followed by data theft (26%), potential revenue losses (13%) and intellectual property theft (10%).

3 Security performance revealed by the security metric

In the previous assignment, we listed the ideal metrics that could be adopted by the identified actor. Among all of them, we focused on the distribution of affected IoT devices over time in a particular ISP. It is a stochastic value based which is computed from the distribution of the number of IP addresses within a particular country over a time window of about six months. It is important to notice that, being a non-deterministic value which depends on the attacker behavior.

Nonetheless, a decision maker is able to understand if the measures put in place on its system were effective or not. In order to come up to this conclusion, internet service providers within the same country to understand should be compared on the same performance which would if it was influenced by attacker behavior.

Figure 1 shows the distribution of affected devices over a period of six months. The number of infected devices is grouped by ISP on a daily basis. When a system relies on a dynamically assigned IP address, it can be counted more than one time in a bigger time unit. Therefore, considering the total amount of infected systems per day would significantly lower the probability to have duplicates.

We queried *Whois* service to retrieve the name of ISP for every address in our dataset. However, we want to point out that we could only retrieve ISP located in Brazil. Therefore, Figure 2 provides an overview of the distribution considering the countries in order to have a also a more comprehensive point of view.

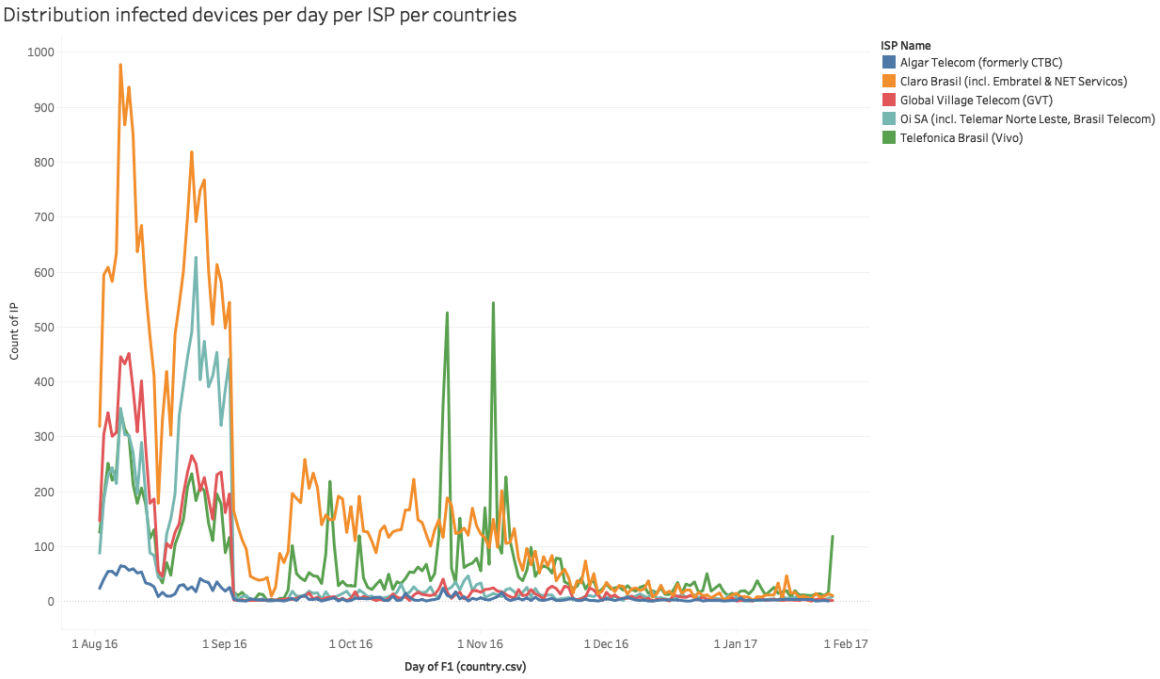

Figure 1: Distribution of infected IoT devices per country over days

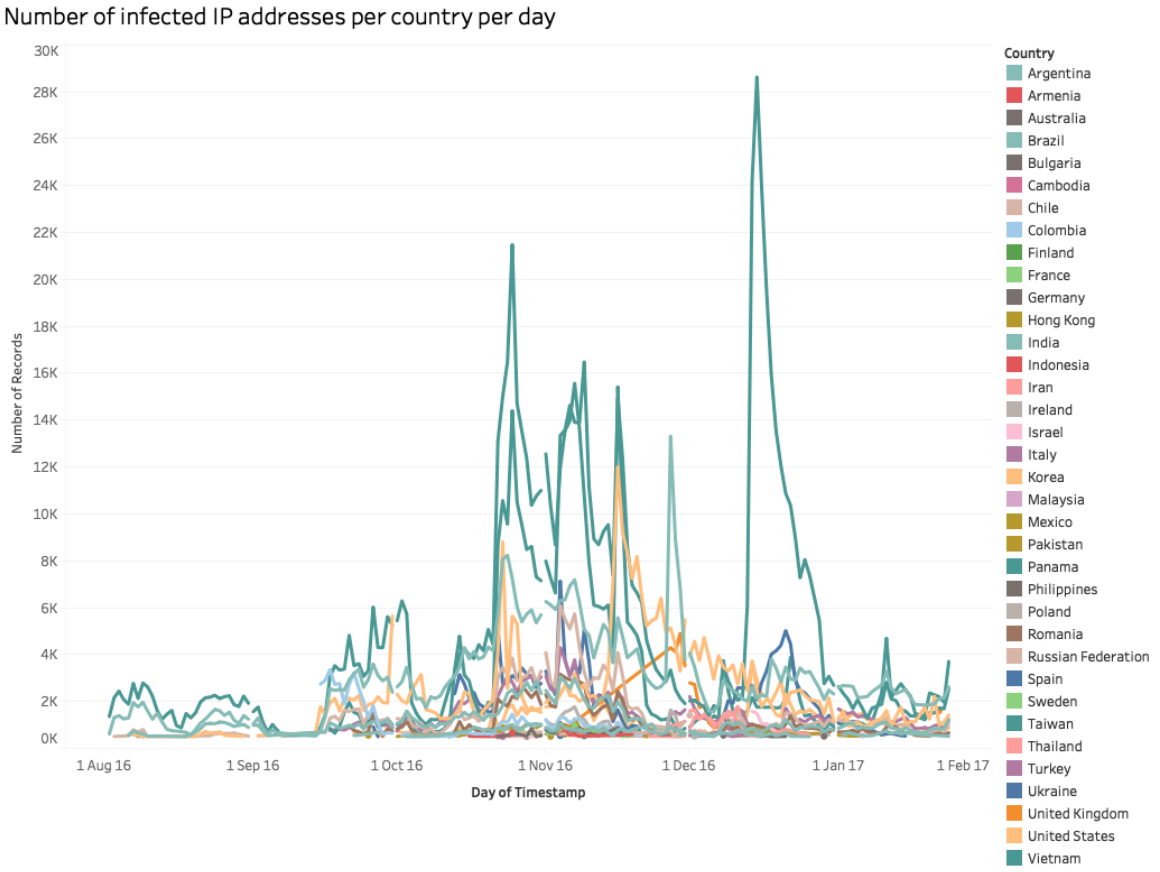

Figure 2: Distribution of infected IoT devices per country over days

To evaluate the effectiveness of our metric we first obtained a retrospective on Mirai malware and

analyzed within our data.

August In August 2016, the research team MalwareMustDie discovered the Mirai malware [wikip]. 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.

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

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

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. [wikip]

We can relate these events on the graphs pictured in figures 1 and 2 to understand the actions taken by the service providers against the malware. Different peaks can be related to initial spread of original Mirai software and its later variants, once the source code was released.

4 Suggested risk strategies for the identified actor

The strategy that ISP could follow for reducing the security issue is by implementing robust security controls. The rxisting controls from ISP end to mitigate attacks such as DDoS or malicious traffic are as listed below [reference]:

- Blackholing Traffic: Blackhole filtering is a mechanism were ISP defense against malicious traffic and can block packets from a domain or IP address. The benefit here is that it will not saturate the ISP's uplinks.
- Scrubbing: A scrubbing center is a centralized data cleansing station. This scrubbing center has the equipment to filter unwanted traffic, leaving a stream of (mostly) clean traffic which gets routed back to the ISP.
- Sinkholing: Sinkholing is a method that diverts malicious traffic away from its target as specified by the sinkhole owners. [Source: https://www.incapsula.com/ddos/ddos-mitigation-services.html]
- Arbor Implementation: Tier 1 service providers are deploying Arbor device as a most comprehensive suite for DDoS protection. They can have automated recognition of attack patterns and filtering traffic for known attack patterns.

	STAGE	ACTIONS
1	Preparation	• Contacts and Procedures; ISP and specialized support; • Network and Infrastructure setups
2	Identification	• Detection and Alerting • Attack analysis • Motivation identification • Mitigation acquirement / refinement • Traceback
3	Containment	• Network modifications • Content delivery control • Traffic control
4	Remediation	• Bandwidth prioritization and blocking
5	Recovery	• Normal state verification • Rollback
6	Aftermath	• Incident review and information disclosure • Law enforcement

5 The influence on the security issue by other actors

As was mentioned before, there is 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. 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, keep your IoT devices updated with the latest vendor firmware, it is highly recommended to always check for all possible updates when purchasing a new device. [source: https://www.grahamcluley.com/protect-iot-devices/] 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, that could mitigate botnet threat is ISP, governments can also play a significant role in a mitigation process. n short, policies that incentivize 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.

6 Risk strategies identified for the actor(s)

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, in case if they are not legally bounded 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 latest trend in cybersecurity is risk strategies is risk acceptance. 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 didn't change 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); Indirect costs (productivity loss, opportunity costs of decisions with incomplete information). In our case, direct costs include:

	The measure	The cost of acquisition + deployment	The cost of maintenance
1	AntiDDoS system		
2	Arbor Implementation	300k per TMS device	
3	Scrubbing	100k for a monthly subscription with Corero	
4	Remediation		

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). Based on data from dataset for 1 particular ISP we can only calculate the number of bots within it is network. We will choose 1 ISP in Brazil, since we were able to map our dataset to it.

ROSI = (benefit - cost) / cost ROSI = (expected prevented loss - cost) / cost

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. With existing in the open data, we can try to estimate the possible losses for the ISP, in case if a company, that uses its services, will come with a legal complaint. We have the data on different botnet incidents:

- company 1: loss in euro, number of bots;
- company 2: loss in euro, number of bots.

At the same time 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).

We can also try to estimate, how much money will the ISP loss due to losses of clients (knowing the yearly net revenue).

Thus, the expected prevented loss will be a sum of all variables mentioned above.

8 Conclusion

References