Universiteit of Twente

Economics of Security Course
AY 2018/2019

Internet of Things: Mirai

ASSIGNMENT 3, Draft

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 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 previous assignments there were identified and calculated:

- security issue;
- problem owner and other possible actors, involved in security issue;
- ideal, existing in practise and evaluated from given dataset metrics;
- different performances of different problem owners based on 1 metric;
- return on security investment for 1 particular problem owner.

The dataset raises a huge security issues - 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 s pace of IoT devices, attempt to log-in using a universal default login/password combination or performing dictionary based attack of possible IoT credentials and thus gain control of these devices. Furthermore, those infected machines are turned and connected into 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, users, Governments and internet service providers (ISPs). For our particular dataset we identified the problem owner as ISP, as the one, that is most affected by threats of botnets.

2 Study of the three actors facing the addressed issue

2.1 Concrete countermeasures suggestions to be taken

For our assignment we are going to focus on 3 actors, that are the most involved in security issue:

1. ISPs, identified as problem owners;
2. Governments, that could influence the security issue, using their legal power;
3. Users, that are owners of IoT devices.

Each of them could implement different countermeasures to mitigate the threat, they are listed in Table 1 below.

Table 1: The identified main actors and the relative suggested countermeasures for the issue addressed

Actor	Countermeasure
ISP	Network monitoring (network behavior anomaly detection)
Government	Policy enforcement
User	Change of default passwords and-or Update firmware

Network behavior anomaly detection (NBAD) is the continuous monitoring of a proprietary network for unusual events or trends. NBAD is an integral part of network behavior analysis (NBA), which offers an additional layer of security to that provided by traditional anti-threat applications such as firewalls, antivirus software and spyware-detection software.

An NBAD program tracks critical network characteristics in real time and generates an alarm if an anomaly or strange trend is detected that might indicate the presence of a threat. Large-scale examples of such characteristics include increased traffic volume, bandwidth use and protocol use. There exist a number of approaches to detect bots through network traffic analysis This could be done by implementing new security tools, specifically made for fighting botnets or by customizing already existing anomaly detection tools, e.g. intrusion detection systems.

Even though, it is common to think, that internet providers are main actors in fighting against bots, it is not completely true. The problem stands, that there exists the lack of legality and legitimacy. For instance, European Union Law does not require Internet intermediaries, to detect malicious botnets operating in their networks. As a result of this legal void, anti-botnet actions are conducted largely on a voluntary basis and a debate on the legitimacy and eventual legality of these measures in found wanting by legal researchers. The legitimacy of these actions remains unascertained: it is not yet clear to what extent the interested parties and society are willing to give allegiance to Internet industry intervention against botnets. Moreover, their legality within EU law is also unclear, as no thorough analysis investigating whether the launch of such countermeasures is in accordance with the law has been conducted.

To break this legal void, currently there exist a number of initiatives, so-called Anti-Botnet Initiatives, that are started by internet industries with a goal of helping citizens against botnets with the support of Governments. Such initiatives, for example, exist in Germany, The Netherlands, Finland, USA. Those initiatives have a positive effect on a botnet security issue (as was shown also in a previous assignment with our dataset), but while they are not applied in EU law, they cannot be entirely effective.

The main weakness of IoT devices, that allowed to hack those devices in the first places was the usage of default passwords on those devices. That is why, it is crucial for users to change those passwords and update the firmware, as soon as they buy a new device. Normally, it is a simple task to perform and could be done with the help of provided with manual along with the IoT device.

Another measure, that ISPs can also implement is information sharing, since this measure doesn't require any costs, but at the same time can bring benefits for all actors involved in security issue. As was shown by Van Eeten in his studies of botnets infections in Dutch ISPs, when all the ISPs received information about statostics on infection rates, they were able to fight botnets more efficiently. Information disclosure helps in remedying information asymmetries.

2.2 Distribution of costs and benefits for the suggested countermeasures among the different actors

Both costs and benefits could be financial and calculated directly, but also could be, for example, reputational and couldn't be calculated directly. For our assignment we are going to focus on non-financial costs, that could be calculated quantitatively.

ISPs We are going to start with: ISPs. Costs of implementing the suggested countermeasures might include:

- network productivity loss, since implementing network anomaly detection mean extra analysis of every packet;
- hiring third parties to analyze the security level of ISP, to understand, if extra measures are needed, which tools to implement etc;
- extra work for network engineers to monitor the network or hiring a new network engineer.

As was mentioned in previous report, there are mostly no direct benefits for ISPs to implement security measures, we can only estimate the prevented losses, hat include:

- loss of existing clients' trust, that force them to change service provider (when customers are satisfied with quality of service of ISP they tend not to change providers);
- loss of reputation, that leads to less numbers of new clients (better reputation lead to more new clients);
- possible legal issues in case of SLA breaches or major incidents for companies, affected by bots.

Governments For Governments costs may include:

- time spent on developing and implementing policies;
- human resources to develop, implement policies and to regular check if the policies are actually implemented.

Benefits for Governments might include:

- people's content about their security and privacy.
- better standing among other countries (e.g. among EU countries).

Users For user there are no costs involved, it is relatively easy to change password and doesn't take much extra time. At the same time benefits for user are many:

- no extra spending on energy and bandwidth consumption;
- less probability of their credentials to be stolen;
- no productivity loss of a device;
- no need to buy / repair / clean from a malware the IoT device, when it got infected.

2.3 Incentives for the actors

Governments In this report we will focus on countries inside the European Union.

In 2013 the European Commission adopted the EU Cybersecurity Strategy aiming to protect Europeans online, increase the security of networks and improve the information security. EU earmarked more than 600M EUR for a six years project of research and innovation in cybersecurity finishing in 2020. The Commission has further strengthened its approach in the past years by including cybersecurity at the heart of its political priorities: trust and security are at the core of the Digital Single Market Strategy presented in May 2015, while the fight against cybercrime is one of the three pillars of the European Agenda on Security adopted in April 2015. Lastly in 2016, after three years of negotiations, the European Parliament marked the birth of the Directive on security of network and information systems (NIS Directive) to obtain a more secure online environment: including protection against Botnets.

"But how the individual countries are reacting to these sets of regulations?" With regard to the NIS directive the majority of EU member states missed the deadline to transpose the EU directive into national law. The directive was approved by the representatives of the EU's 28 national governments but the same countries that accepted it before seem refuse it now. According to the directive, member states need to identify, before 9 November 2018, the operators of essential services (water, energy, transport, health and banking operations) do everything in their power to manage the risks of being hacked and report to the authorities if there is a cybersecurity breach.

As stated in a commission-run website, last updated on 19 September, the following countries are in still progress or have partially transposed the directive into national law: Latvia, Lithuania, Poland, Belgium, Austria, Hungary, Romania, Bulgaria, Greece, Ireland, France and The Netherlands (12 countries out of 28).

We can clearly affirm that almost half Europe is still working about the NIS Directive. "Does it mean that those countries don't have incentives to apply the regulations?" Let us examine the step of the application of a Directive and the consequences for a country if it does not satisfy it.

The directives are European sources proposed by the Commission and endorsed by the EU Council and the Parliament. They do not produce direct effects on individuals, but instead produce an obligation for member states to adopt a national law that contains the provisions of the directive. It is used instead of the regulation (which is directly applicable and effective even on private individuals, does not require state application), because the states can achieve the goals and apply the directive with a certain discretion, resorting to national regulatory and administrative instruments more suitable. What matters is the purpose and certain minimum standards that must be common to all states. If a member state does not apply the directive with its own national regulatory act, this directive produces direct effects on individuals if "self executing" with repercussions on the state itself. Furthermore, the Commission can open an infringement procedure against that state and sanction it economically. The infringement procedure consists of a first letter of delay that urges the state to apply the directive, if it is not done, the state can be sanctioned.

On 19 July, the commission announced that it has sent warning letters, with two months to respond, to 17 EU member states, telling them to fully transpose the cybersecurity directive.

In conclusion we can infer that countries inside the European Union have economic and reputational incentives to fulfill cyber security requirements leading to a more cyber-secure ecosystem.

ISPs By allowing the growth of botnets inside their network ISPs will be seen as unreliable which will significantly damage their reputation. The growth of botnet infection within ISPs lead to extra bandwidth consumptions, network productivity losses, possible SLA breaches and, in general, lost of customers trust. In their empirical study on spam and botnets, Van Eeten et al. (2010, p. 46) claim "because around 80-90% of all spam is issued by botnets, the origin of a spam message is very likely to indicate the presence of an infected machine". Thus, neglecting the infected computers in their own internal structure, ISPs not only do not eradicate the problem but rather allow it to grow. Ultimately, users of a particular ISP will start receiving constant and regular spam which undermines the professional reputation and reliability of an ISP (Spamhaus, 2014).

To summarize, the incentive for ISPs to implement the countermeasure is to preserve their reputation to be able to keep customers satisfied and attract new clients.

Users End users, owners of IoT devices, have economic incentives and usability reasons to keep them secure and not under control of the botnet. To demonstrate that, we will focus on a report published by the University of California, Berkeley.

An infamous use of Mirai is depicted in the DDoS attack on 20 September 2016 on the Krebs on Security site which reached 620 Gbit/s. The Berkeley School of Information has calculated that, with the extra energy consumption and bandwidth costs, the botnet used in that attack would have cost device owners $323,973.75, or $13.50 for each device. The researchers of the University report that in tests on infected devices, they observed increases in electricity consumption, and "significant increases in bandwidth usage in infected devices when compared with non-infected devices operating normally".

They also found that "infected devices cause a degraded user experience for the device owner, as devices that are involved in attacks can interfere with the owner's use of both the device and the network to which it is connected".

Furthermore in a worst-case scenario, with the Mirai botnet operating at peak power in a UDP DDoS attack, "The projected cost to consumers of this attack would be $68,146,558.13. Increased energy consumption accounts for just $855.00 of that total cost, with the rest accumulated from increased bandwidth consumption. The per-device cost to the consumer for this hypothetical worst-case scenario is $113.58."

2.4 The role of externalities

There are both positive and negative externalities for the already mentioned actors, namely governments, ISP and users.

2.4.1 Negative externalities

Governments Government are boosting subsidies to private ISP with "access to low-cost infrastructure, low-interest loans, loan guarantees, up-front payments, on-going payments, and/or other mechanisms." However, citizens might face a higher taxes.

ISP Every company is now exempted from liability for violations of cybersecurity thus they are not taking against their customers' infection to malware because of their weak incentive to intervene.

Users According to J.A.Chandler: «"Users do not face the full costs of their lack of computer security. This is particularly the case now that bot software is being designed to be minimally disruptive to the computer owner, so that bots may avoid detection and removal. Accordingly, average users fail to invest in security"».

2.4.2 Positive externalities

Governments Governments are enforcing manufacturers to follow standards security. However, customers still base their buying decisions on a price criteria rather then company's compliance. [*note: this is an assumption without references for feedback purpose*]

Governments need to raise awareness of customers in buying products compliant with secure standards of manufacturing. [[*note: this is an assumption without references for feedback purpose*]]

Privacy of people has become central and Governments are aiming to improve this right by imposing also botnet sanitization provisions to providers.

ISP ISPs investing in cyber security is not as effective as for their customers. This market failure is a deterrent for service providers' incentive to invest.

Users According (Kinukawa S.) study, all on-line users create positive externalities for internet service provides.*[source: http://www.jlea.jp/2012zy_ zr/ZR12-05.pdf]*

3 Statistical analysis

3.1 The influencing factors of the defined security metric's variance

The factors, that cause variances in this metric are as followed:

- Attacker behaviour, this is unpredictable factor, attacker can choose some random time to infect the devices and abandon the botnet after that.
- Governmental policies enforcement - ex ante. In some countries the overall infections and variations in number of infected devices is much less, due to the fact, that those countries have policies and initiatives in place, that force and motivate them to implement security measures against bots.
- Information asymmetries (e.g. lack of security awareness), no information sharing between companies. According to video, people buy IoT devices not caring about security, so they just tend to buy cheapest devices, not caring how secure they are.
- Collaboration between ISPs. As with the example of governmental policies
- Producers of IoT devices, that don't care about security and just care about producing the cheap devices and selling more of them. Implementation of security tools to mitigate the threat of botnets.

3.2 Overview of the data collected

First, we are going to implement a new metric for ISPs. This metric will show the percentage of infected IP devices during the "peak" of infection for different ports for different ISPs. As we showed before, infection of some ports (e.g. 7547 - a router port for CPE WAN management protocol) is more severe, than others ports (e.g. 23 - Telnet protocol). This metric can help ISPs understand, how severe was infection for them. For example, infection of IP address associated with port 7547 means that there was infected a router within ISP network, that could cause significant damage, if the router will be overloaded, it could cut the connection for multiple users, instead of cutting 1 user as in an example of port 23.

TCP port 7547 is well-known to be used by ISPs to remotely manage their customers' broadband routers and known as CPE WAN Management Protocol, which is more commonly known as TR-069. This protocol standardizes the wide area network (WAN) management of CWMP devices. TR-069 gives broadband service providers a framework and common language to remotely provision and manage these devices.

Number of Infected IPs		ISP 1	ISP 2	ISP 3	Total
	Port 23				
	Port 2323				
	Port 7547				
	Total				

3.3 Description of the performed statistical analysis

We can test for 1 particular day (“peak” of infection), for each ISP, how severe was the infection. We are going to test, what are the odds of IP address with port 7547 (router) being infected, comparing to other IP addresses (all other IoT devices) using odds ratio.

For the metric, that was used in a previous assignment, we can also perform an analysis. We can compare performances of country with implemented policies and ISP cooperation (e.g. the Netherlands) and the country, that don’t have it (e.g. Mexico) to understand if they depend on attacker’s behaviour or not (based on our timeline).

We can use Pearson’s chi squared test to perform a test of independence of an attacker behaviour. Thus, we are going to test if the performance of the ISP depends on the fact that they implement security measures or not.

By performance we assume the difference between number of infected ip addresses during "peak" of infection wave and the number of ip addresses 3 days after the infection happened. This shows us that for ISPs without implemented measures there is a big variation (e.g. Mexico), while in countries with implemented measures (e.g. nl), the variation is big.

We also make an assumption, that countries, like the Netherlands implement a number of measures (factor 5) to fight the threat of botnets, meanwhile countries like Mexico do not.

- H_0 : performance of ISP doesn’t depend on the fact, that they implement measures.
- H_1: performance of ISP depends on the fact, that they implement measures.

	The difference between “peak” and in 3 days in number of infected devices							
	Peak 1	Peak 2	Peak 3	Peak 4	Peak 5	Peak 6	Peak 7	Peak 8
The ISP in Mexico (Telmex)	100	500	50	358	400	457	389	178
The ISP in the Netherlands	5	8	6	3	7	9	2	2

We calculated value of χ^2 and were able to reject the H0 hypothesis.

By applying the formula of Pearson (presented in the slides) we identified that performance of ISP depend on the fact, that they implement security measures.

4 Conclusion

References