Group 1

Mirai Botnet: Actors and Security Strategies

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

14-10-2019

1. Introduction

The Mirai malware targets weakly secured IoT devices. When a device if infected with the Mirai malware, it searches for other vulnerable devices to spread the malware. This report focuses on the security issue of the spread of the Mirai malware, creating large IoT botnets. Various metrics and investment strategies have been explored for ISPs in previous assignments. This assignment aims at understanding which factors influence the security issue. First different countermeasures of three important actors are elaborated on. This includes the costs and benefits of these countermeasures and incentives for the actors to act. Next, different factors of influence on the rate of infected devices are explained and analysed.

2. Involved actors

2.1 ISPs

- Extensive research on proactive measures of ISPs shows that in order to fight botnets ISPs include notifying and / or quarantaining users (OECD, 2012). A specific form of this is called the *walled garden* approach (Çetin et al., 2019). The end-user is notified using a landing page and is provided with very limited internet access. Often only access to clean-up tools, updates and communication channels is allowed in the walled garden.
- **Benefits ISPs**: owners with infected devices are pressured to remove malware from their devices themselves, which results in a lower infection rate for the ISP. The landing page with the notification is an efficient communication method for the ISP. Emails may not be read or received and calling customers by phone is expensive.
- **Costs ISPs**: handling end-user reactions in the form of walled garden forms, help desk calls and emails are costly (Çetin, Altena, Gañán & Van Eeten, 2018). The setup and operation of the walled garden, as the abuse handling process in general is expensive (Çetin et al., 2019). The authors mention that some customers threatened to terminate the contract with the ISP, if the quarantine continues. Terminated contracts are costs for the ISP. Also, end-users complain about disrupted services (Çetin et al., 2018). This causes to ISP brand- and reputation damage.
- **Incentive:** Çetin et al. (2019) regard the incentives for ISPs to implement walled garden solutions as being weak. To strengthen these incentives, governments are to assign liabilities to ISPs, according to the authors.

2.2 End-users: IoT device owners

- The IoT device owners also play a role in this security issue. For example, 80% of the current IoT devices do not require a complex enough password to provide adequate protection. This means that the responsibility of changing the default password partly lies with the device owner (Singer, 2018). The IoT device owners can change the

default password of their IoT device to a strong new password (e.g. at least 6 characters, a combination of letters, numbers and symbols, upper and lower case) (Singer, 2018).

- **Benefits**: end-users are not directly impacted by the spread of the IoT malware. However, changing their device password does clear them from being liable when an IoT botnet occurs. Hence, the indirect benefit is that end-users cannot be held accountable by for example the ISP if they properly changed the default password.
- **Costs**: Changing a password takes time and effort for users. The research of Shay et al. (2010) shows that it takes on average 1.77 tries for users to change their password to a password that is acceptable, but can frustrate users.
- **Incentive**: Shay et al. (2010) show that there generally is little support from end-users to change their password to a stronger one. The end-users do not experience disadvantages for their IoT device being used as a bot, so they don't have a direct incentive to change their default password. While the end-users are aware of the fact that changing the default password can provide extra security, one of the main issues is that end-users are afraid that more complex passwords will increase the likelihood to forget them.

2.3 IoT device manufacturers (technology brands)

- The IoT device manufacturers can force end-users to change initial password to a new strong password (e.g. at least 6 characters, a combination of letters, numbers and symbols, upper and lower case). When producing the devices, it can be programmed that the device only works after the default password is changed.
- **Benefits:** IoT device manufacturers do not experience any direct benefit from the implementation of mechanisms that force the change of default password by users.
- **Costs:** Jerkins (2017) states that consumers are interested in ease of deployment, ease of use of the device and low costs. These market forces motivate manufacturers of the IoT devices to omit features that do not provide a competitive advantage or increase cost such as security. Therefore, implementing mechanisms that force the change of default password will affect the device usability, possibly resulting in damages in terms of income and brand reputation to the technology manufacturer.
- **Incentive:** beyond altruism, IoT manufacturers do not have any incentives to implement security mechanisms to change force the change of password (Jerkins, 2017).

3. Role of externalities

Question to teacher: how does point 4 of the first part of the assignment differ to point 1 of the second part of the assignment?: Briefly reflect on the role of externalities around this security issue. vs. Identify different factors explaining (causing) the variance in the metric

ISPs, end-users and IoT device manufactures can apply different strategies to influence the security issue, but there are numerous external factors which must be considered as well.

- Digital savviness (Networked Readiness Index)
  The Networked Readiness Index is often phrased as the Technology Readiness. The index measures the ability of countries to adapt new opportunities in ICT.
- National anti-botnet initiatives (source: https://www.oecd-ilibrary.org/docserver/5k98tq42t18w-en.pdf?expires=1570697351&id=id&accname=guest&checksum=046CF9B92283997EA506B70324EC1DCD OR Cyber Security Measures via Intermediaries by Hadi Ashgari
  Anti-botnet initiatives (ABIs) can be formed on national and regional level. In ABIs, private and public partnerships are formed to collectively combat botnets. Activities of ABIs entail the offer of help to infected ISP users cia call centers, the set-up of code of conducts for ISPs and mitigation schemes in which infection data is collected (Ashgari, 2016). According to Ashgari, depending on whether certain countries have or do not have national ABIs can influence the ISP infection rate.
- Code publishment:
  The source code of Mirai was published on Hack Forums on September 30 2016. As can be seen in figure X, infected IP addresses appeared quickly after this date in early October. After that, many variants of the Mirai code appeared, attacking different ports. As stated by IBM, ports 23 and 2323 were most frequently accessed by the malware in the beginning (IBM, 2017). As reported by Sutherland (2016), an increased use of port 7547 was observed around the 26th of November in 2016 (light blue peak in Figure X).

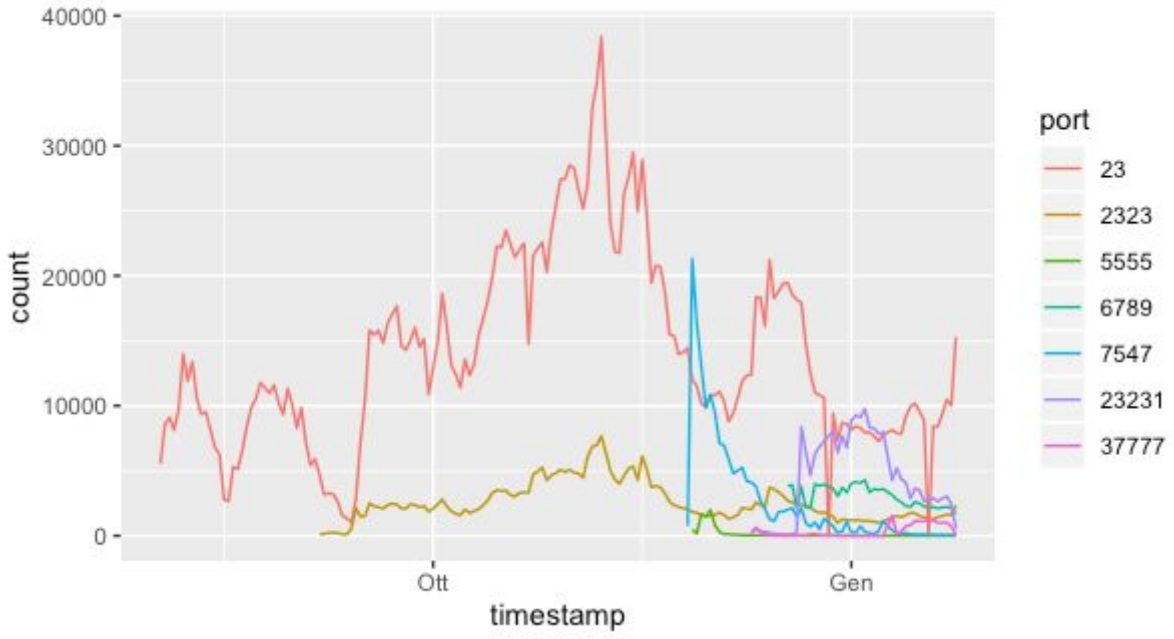


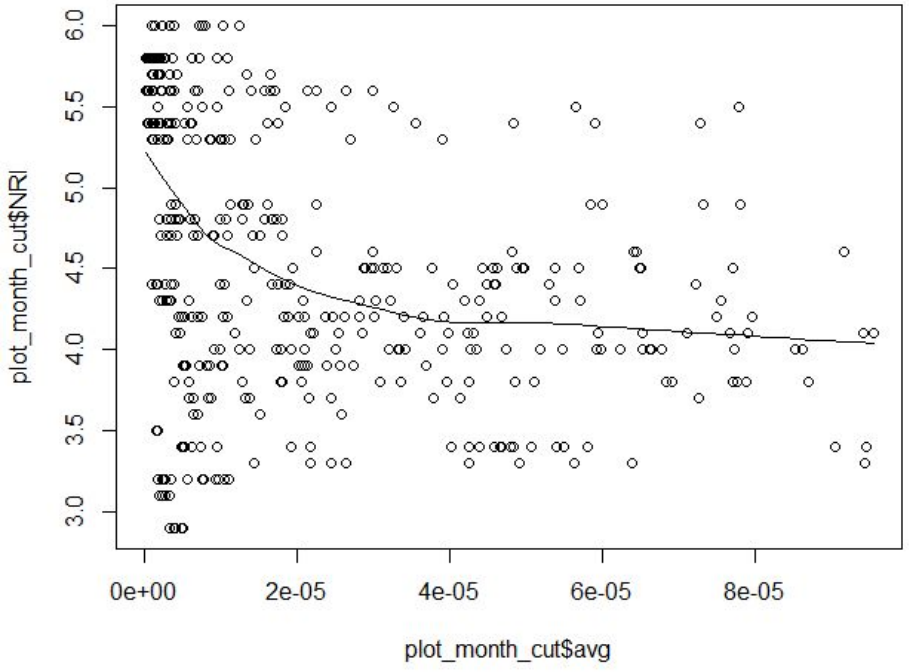
Figure X: Infected IP addresses per accessed port

(7 points) Identify the type of actor whose security performance is visible in the metric(s) you selected (e.g. ISPs, software vendors, countries). Note that this is not necessarily the problem owner, rather is the unit of analysis in your metric.

1. Identify different factors explaining (causing) the variance in the metric,

2. Collect data for one or several of these factors,
    i. Anti Botnet initiatives are present in (source: https://www.oecd-ilibrary.org/docserver/5k98tq42t18w-en.pdf?expires=1570697351&id=id&accname=guest&checksum=046CF9B92283997EA506B70324EC1DCD):
        1. Finland
        2. The Netherlands
        3. Japan
        4. Ireland
        5. Australia
        6. Germany
        7. South Korea
        8. US (not formally)
        9. UK (not formally)
3. Perform a statistical analysis to explore the impact of these factors on the metric.

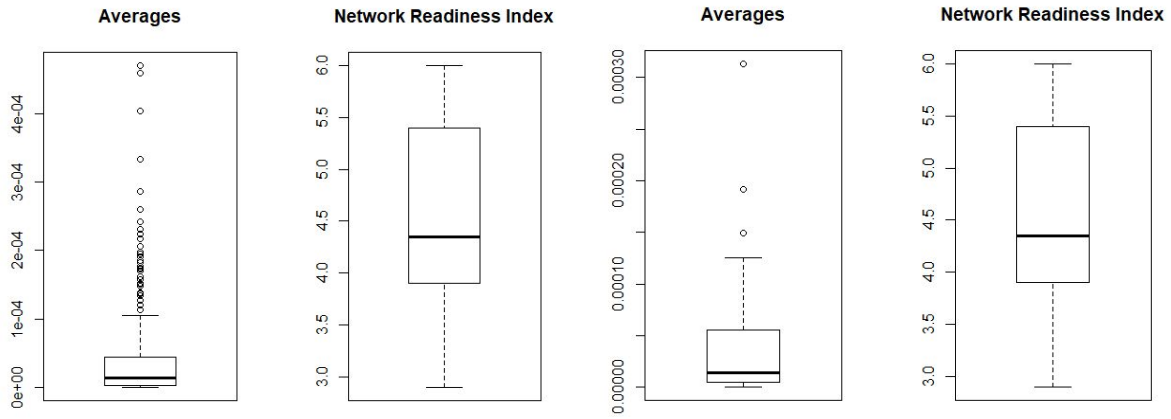
Statistical analysis Network Readiness & Average Infection Rate



- Both Network Readiness & Average Infection Rate are on Ratio scale

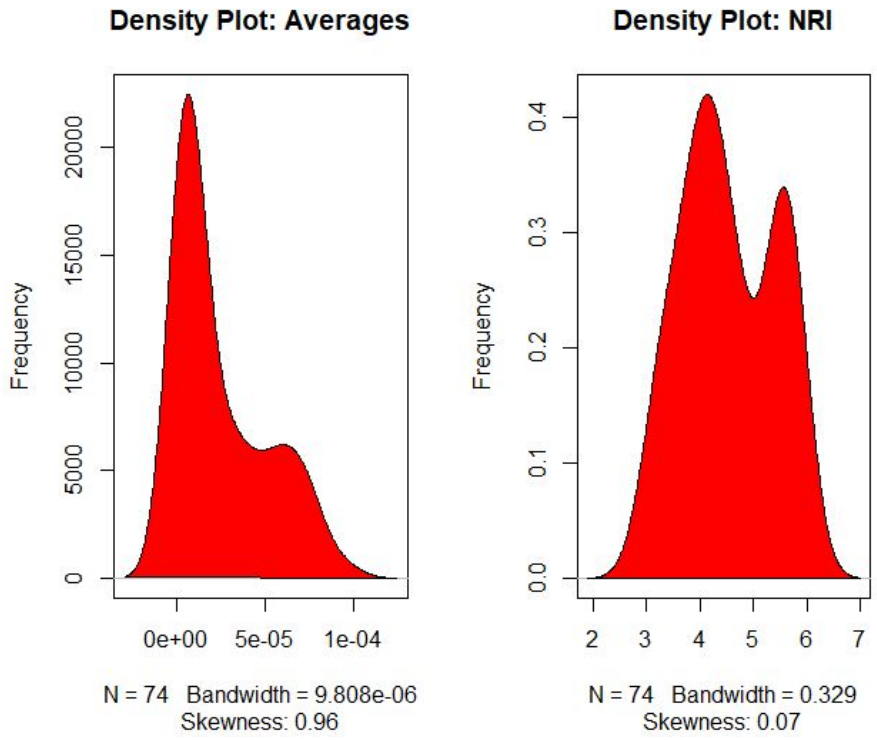
A linear regression analysis is performed to investigate the relationship between network readiness index and average infection rate.

The average infection rate per country per year is obtained.
Yearly averages are taken to reduce outliers and to match the metric with the yearly Network Readiness Index.



Left: monthly average (lot of outliers) Right: yearly average (less outliers)

The three outliers in the yearly average are removed.
Next, it's checked whether the observations in the dataset are normally distributed:



The variables are not normally distributed, so another statistical measure is selected than linear regression.

Suggestion: Spearman correlation (since linear relation is weak, no Pearson)

Assumption List

- Look at infection rate per country, compare to Network Readiness Index.
    - average infection rate calculation: unique IP addresses per day, averaged for the entire dataset
    - Network Readiness Index is yearly rate
- No huge differences between ISPs per country, hence no difference made per ISP but focus on country

References

Asghari, H. (2016). *Cyber Security Via Intermediaries. Analyzing Security Measurements to Understand Intermediary Incentives and Information Public Policy* (Dissertation).

Cetin, O., Ganán, C., Altena, L., & van Eeten, M. (2018). Let me out! evaluating the effectiveness of quarantining compromised users in walled gardens.

Çetin, O., Gañán, C., Altena, L., Kasama, T., Inoue, D., Tamiya, K., ... & van Eeten, M. (2019, February). Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai. In NDSS.

IBM (2017, April). *The weaponization of IoT devices.* Retrieved from: https://www.ibm.com/downloads/cas/6MLEALKV

OECD (2012). "*Proactive Policy Measures by Internet Service Providers against Botnets*", OECD Digital Economy Papers, No. 199, OECD Publishing, Paris.

Shay, R., Komanduri, S., Kelly, P.G., Leon, P.G., Mazurek, M.L., Bauer, L., Christin, N. & Cranor, L.F. (2010). *Encountering Stronger Password Requirements: User Attitudes and Behaviors* (Report from Symposium on Usable Privacy and Security). Retrieved from http://delivery.acm.org/10.1145/1840000/1837113/a2-shay.pdf?ip=145.94.220.112&id=1837113&acc=ACTIVE%20SERVICE&key=0C390721DC3021FF%2E512956D6C5F075DE%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1570699464_24f1fb8042bd4814bbaba6049820a3a4

Sutherland, L. (2016). *Mirai evolving: new attack reveals use port 7547*. Retrieved from: https://securityintelligence.com/mirai-evolving-new-attack-reveals-use-of-port-7547/

Jerkins, James. (2017). Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code. 1-5. 10.1109/CCWC.2017.7868464.