Group 1

Mirai Botnet: Actors and Security Strategies

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

21-10-2019

1. Introduction

The Mirai malware targets weakly secured IoT devices. When a device is infected with the Mirai malware, it searches for other vulnerable devices to spread malware to. 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. Countermeasures

This chapter introduces three actors who are involved in the security issue and explains countermeasures they can take. The suggested countermeasures for ISPs, end-users and device manufacturers are paired with costs and benefits.

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.

Owners with infected devices are pressured to remove malware from their devices themselves, which results in a lower infection rate for the ISP and benefits the ISP. The landing page with the notification is an efficient communication method for the ISP. However, emails may not be read or received and calling customers by phone is expensive. Besides, 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.

Çetin et al. (2019) regard the incentives for ISPs to implement walled garden solutions as being weak. To strengthen these incentives, governments have 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 explicitly require a complex 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).

Generally, end-users are not directly impacted by the spread of the IoT malware. Therefore, end-users do not directly benefit from changing their default password. Only if ISPs block internet access of infected end-users (which is not in every country a usual approach, see 2.1), benefits of changing passwords are present. End-users do face costs when having to change their password. 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. This can frustrate users.

Shay et al. (2010) show that there is generally 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 default 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.

IoT device manufacturers do not experience any direct benefit from the implementation of mechanisms that force the change of default password by users. The costs for device manufacturers therefore outweigh the benefits. 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.

Beyond altruism, IoT manufacturers do not have any incentives to implement security mechanisms to change force the change of password (Jerkins, 2017).

2.4 Externalities Security Issue

In paragraph 2.1, 2.2 and 2.3 the costs and benefits of each actor are explained. In section 2.2 it is highlighted that end-users generally do not bear the consequences of their bad password behavior. They are for example not directly impacted by the spread of Mirai, caused by their bad password practices. Costs of the spread are to be incurred by other actors, such as ISPs having to invest in monitoring practices or walled garden approaches and website owners that are being attacked. Likewise, IoT device manufacturers create externalities regarding botnets. End-users have to invest time and have to acquire knowledge for changing their passwords. If device manufacturers invest in proper instructions or do not ship their devices with default credentials, this externality might not exist. Lastly, an externality can be formulated in the case of bad performing ISPs. ISPs that do not do anything for botnet mitigation do not bear the costs of this neglectance. They do create costs for website owners and ISPs that do have botnet mitigation procedures in place. Botnet mitigation procedures at ISP level are most effective when all ISPs have them. Using this rationale, bad performing ISPs make botnet mitigation procedures of well performing ISPs less effective and thus more costly.

3. Variance in Infection Rate

The infection rate for IoT devices containing the Mirai malware varies per country. This could resemble the security performance of governments or the combined ISPs for a country. As explained in chapter 2.4, there are factors influencing the mirai spread among IoT devices such as IoT device increase per country and specific legislation. In addition to these externalities, there are factors which can be identified which could be of influence on the variance in infection rate per country. This chapter elaborates on two selected external factors. These are cybersecurity savviness of a country and the existence of national anti-botnet initiatives (see figure 1).

Cybersecurity savviness is derived from the Global Cybersecurity Index which measures the commitment to cybersecurity per country. National anti-botnet initiatives (ABIs) are formed on a 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 via call centers, the set-up of code of conducts for ISPs and mitigation schemes in which infection data is collected (Asghari, 2016). According to Asghari, depending on whether certain countries have or do not have national ABIs can influence the ISP infection rate.

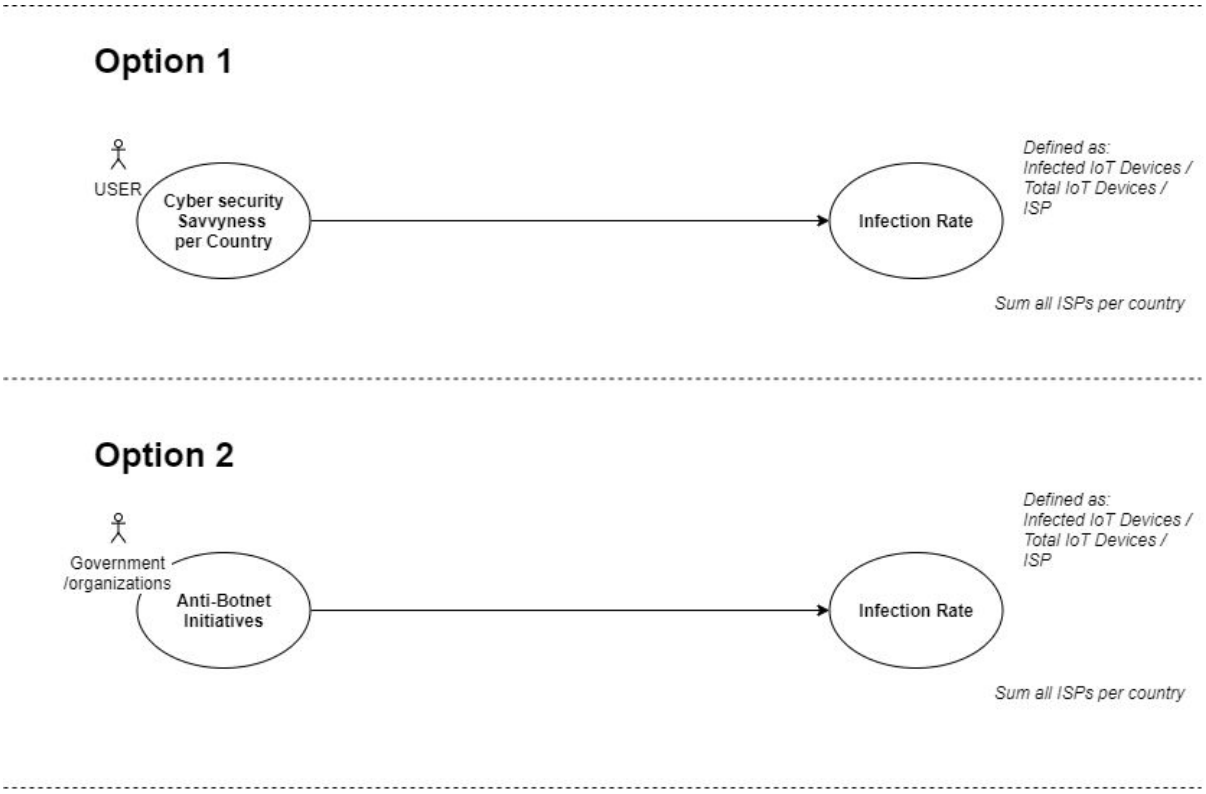

Figure 1: external factors

3.1 Data collection

The Global Cybersecurity Index (ITU, 2018), which represents cybersecurity savviness, shows a global ranking. All countries are scored on their legal, technical, organizational, capacity building and cooperation measures after they completed a questionnaire. Mainly the technical measures and capacity building measures are good indications to show the influence on botnet growth. These measures include standardization bodies, technical mechanism, public awareness campaigns, professional training courses in cyber security and incentive mechanisms. Countries scoring low on these aspects can have higher risk on IoT botnet growth.

The Anti-Botnet Initiatives were identified based on research by Asghari (2016). His research states that ABIs are present in 9 countries. These are Finland, The Netherlands, Japan, Ireland, Australia, Germany, South Korea, the US and the UK. Asghari states that the ABIs help ISPs mitigate botnets through share of data and support in costs.

3.2 Statistical analysis

Statistical analyses are performed to explain the impact of the identified external factors on the variance in the infection rate. Close attention is paid whether the assumptions of the analyses are met. Also, the level of data aggregation is considered to determine the loss of information when working with averaged values.

3.2.1 Variance of Infection Rate explained by Global Cybersecurity Index

To see infection rate is influenced by GCI, the infection rate per country is averaged over months. In this test only European countries have been considered. It's reasoned that averaging over months makes sense, because the short term, erratic courses of daily infection rates are not caused by the constant cyber security index.

When the monthly infection rate per country is set out against the global security index (see figure 2) one point is clearly deviating from the downwards trend. After further investigation of this point, no good reason was found to remove this datapoint: the point shows a huge increase in infection rate in Ukraine in December, which is plausible. The datapoint is kept in the analysis.

Monthly infection rate per GCI score with outlier

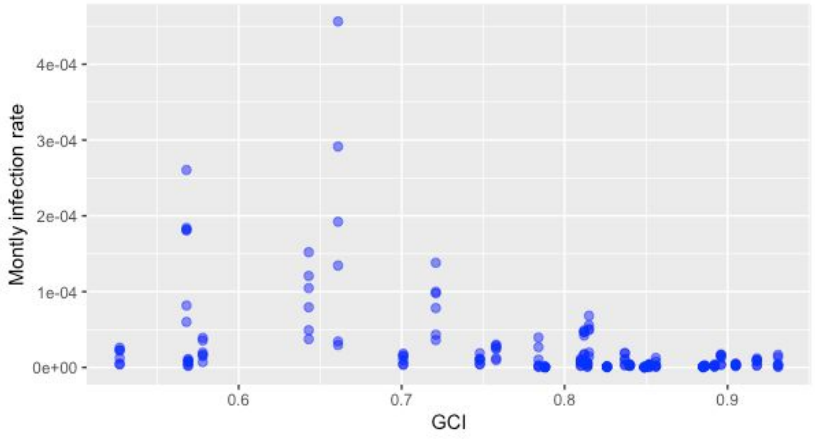

Figure 2: Scatterplot monthly infection rate per GCI score

The linear relationship becomes more clear when plotted on a semi-log scale (see figure 3), in which the logarithm of the dependent variable is calculated. This means the relationship will in the linear regression will be defined as: $log(Infection\ Rate) = \beta_0 + \beta_1 * GCI + C$.

Monthly infection rate (log scale) per GCI score

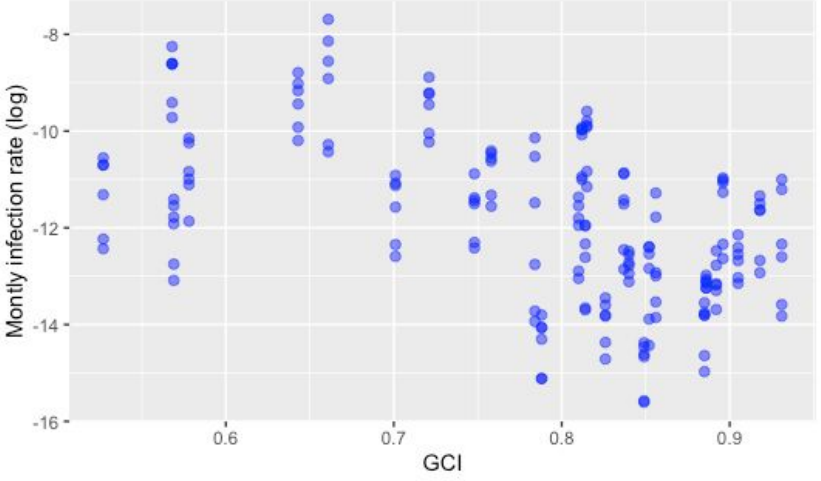

Figure 3: Scatterplot monthly infection rate (log scale) per GCI score

Because a linear regression is performed, several assumptions are tested. First, the normality of the data is regarded. In figure 4a, the distribution of the infection rate is visually inspected for normality. The infection rate distribution can be regarded as normal since Shapiro-Wilk does not test significantly with $p = 0.1989$ and H0 = the data is normally distributed. Figure 4b shows the distribution of GCI, which is not normally distributed (Shapiro-Wilk, $p = 0.009767$). Although not all data is follows the normal distribution, the *residuals* do. In linear regression, this is most important. To check for normality of the residual distribution, a QQ plot is inspected (figure 5). Here it can be seen that the right tail shows some deviation from the ideal line, however the Shapiro-Wilk test states that the residuals are normally distributed with $p = 0.07052$.

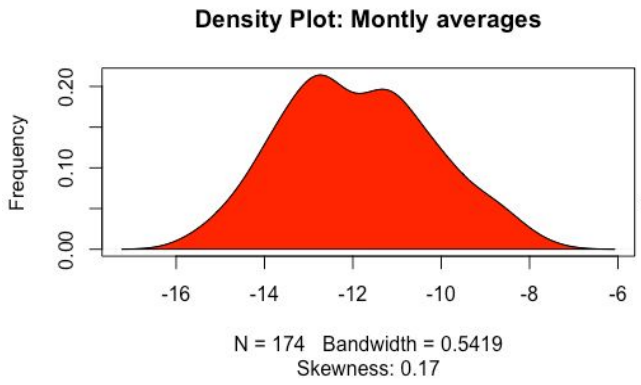

Figure 4a: Density plot infection rate

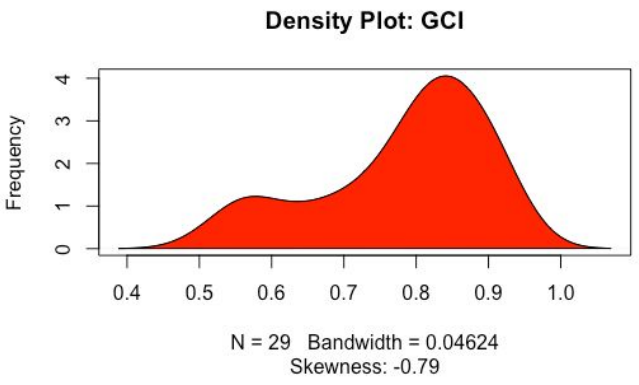

Figure 4b: Density plot GCI

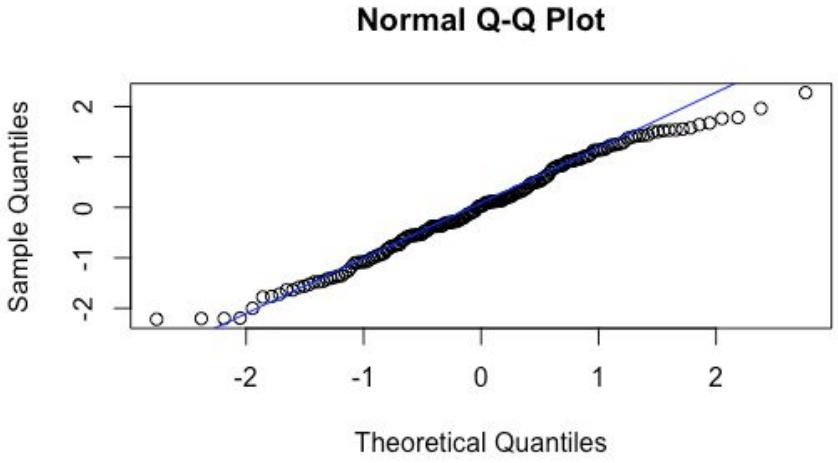

Figure 5: QQ plot residuals

It's concluded that the necessary assumptions of linear regression are met. The linear regression was calculated to predict Monthly Infection Rate per country based the Global Cybersecurity Index (GCI). The equation was significant $F(1, 172) = 65.15, p < .000$ with a R^2 of 0.2747: the GCI can be used to explain 27% of the variance of Monthly Infection Rate.

The coefficients are estimated -5.8096 for the intercept and -7.7840 for the predictor GCI. Thus, $log(Infection\ Rate) = -5.8096 + -7.7840 * GCI + C$. This line is plotted in fig 6.

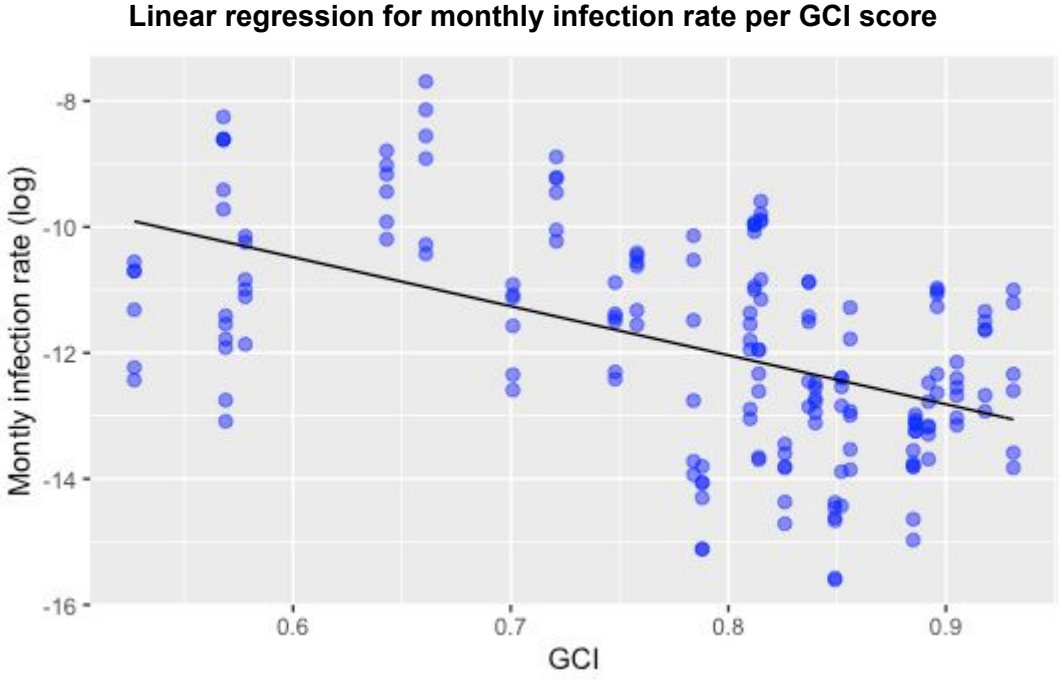

Figure 6: Linear regression

Since one of the axes is in logarithmic scale, interpretation of the results is as follows: $\%\Delta y = 100 \cdot (e^{\beta_1} - 1)$. This yields the following: $100 \cdot (e^{-7.7840} - 1) = -99.95837$. This means that for every unit of increase of GCI, the infection rate decreases about 99.96%. Because GCI is scaled from 0 to 1, this result makes sense but is not insightful. If $\Delta GCI = 0.1$ is taken, it's estimated that $100 \cdot (e^{0.1 \cdot -7.7840} - 1) = -54.0856$. This means that an increase of 0.1 GCI results in a decrease of approximately 54% of infection rate.

3.2.2 Variance of Infection Rate explained by Anti-Botnet Initiatives

To research the impact of ABIs on the infection rate, two groups are created in the dataset. These are countries with ABIs and countries without ABIs. To research this, an independent t-test will be conducted. This test shows the relationship between a binary independent variable, the ABI, and a ratio-dependent variable, the monthly infection rate. The countries without anti-botnet legislation are categorized as a binary variable with value 0, countries with anti-botnet legislation have a value of 1. The results in table 1 show the descriptives of the data: there are 66 countries without anti-botnet legislation and 7 with.

Table 1: descriptives for countries with ABIs

Countries have anti-botnet initiative?	N
No (0)	66
Yes (1)	7

The main hypotheses of this statistical test are:

- *H0*: There is no difference in infection rate between countries with and without anti-botnet legislation
- *H1*: There is a difference in infection rates between countries with and without anti-botnet legislation

Before conducting the actual analysis, two important assumptions must be met. These are the assumptions for normality and equal variances.
First, the normal distribution of the monthly infection rate is tested. The infection rate must be approximately normally distributed for both groups of countries with ABIs and without. The hypotheses state:

- *H0*: The monthly infection rate for both groups are normally distributed
- *H1*: The monthly infection rate for both groups are not normally distributed.

This is tested with the Shapiro-Wilk test. This tests whether the population where the monthly infection rate is drawn from is normally distributed, for both the groups with and without Anti-Botnet legislation.

Figure 7.a and 7.b show the distribution of the average monthly infection rate for the countries that do not have Anti-Botnet legislation and the countries which have it. Both the histograms are looking like a normal distribution.

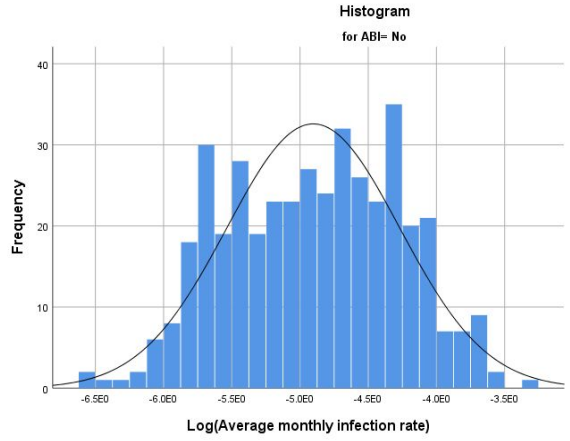

Figure 7.a monthly infection rate countries without ABI

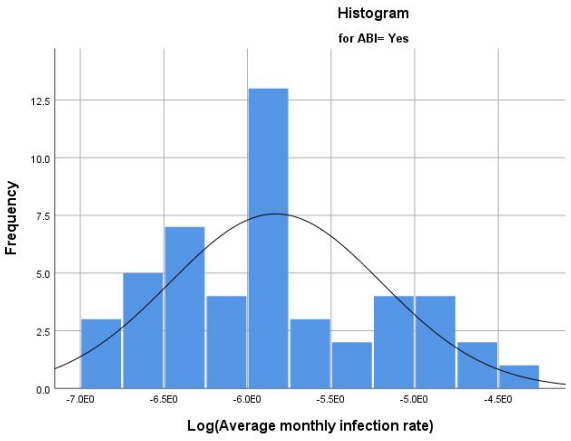

Figure 7.b: monthly infection rate countries with ABI

To statistically test whether the monthly infection rates of both groups are drawn from a normally distributed population, the Shapiro-Wilk test is conducted. The p-value for the group with ABIs is 0.000 and the p-value for the group without ABIs is 0.046. Both values are significant and therefore the null-hypothesis is rejected. The monthly infection rate for both groups are not normally distributed.

This can also be shown with a Normal Q-Q plot, as was done in paragraph 3.2.1. Figure 8.a shows that at the beginning and end of the line there is some deviation from the ideal line. Also in figure 8.b, there is a deviation from the ideal line, now more along the whole line. These graphs support the conclusion that the monthly infection rate is not drawn from a normally distributed population.

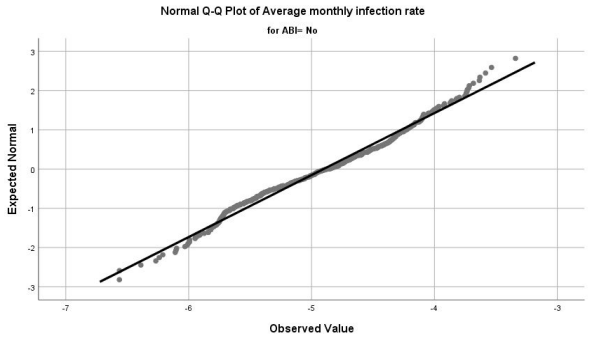

Figure 8.a: Q-Q Plot for countries without ABIs

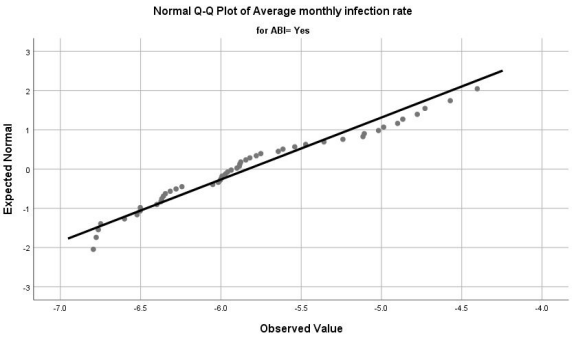

Figure 8.b: Q-Q Plot for countries with ABI

Second, the groups are tested on equal variances to comply to the assumption of an independent t-test. Levene's test is consulted to test for equal variances. The hypotheses state:

- *H0*: the two different groups within the independent variable have equal variances;
- *H1*: the two different groups within the independent variable have unequal variances.

Levene's test for equality of variances shows a significant p-value (p=0.564), which means that the two different groups (countries with and without Anti-Botnet legislation) have equal variances. This assumption is met. The independent t-test shows a significant p-value of 0.000, which means that there is a difference in infection rates between countries with and without anti-botnet legislation.

However, because one of the two assumptions of an independent t-test is not met, the results of the independent t-test cannot be interpreted and there is no conclusive answer to the question of whether there is a difference in infection rates between countries with and without anti-botnet legislation.

4. Conclusion

There are different factors which influence the security issue at hand. The identified actors are ISPs, end-users and IoT device manufacturers. They can take numerous countermeasures to decrease the Mirai spread among IoT devices and mitigate botnet growth. ISPs are in the power to notify the end-users about infected devices, the end-users can change their device password and manufacturers can program devices in such a way that the devices can only be used until the password is appropriately changed. By performing bad security practices, all actors produce externalities. End-users are not economically impacted when maintaining weak passwords. The lack of security measures by the device manufacturers causes end-users to invest more time to change their passwords. ISPs create externalities for parties such as website owners when ISPs don't mitigate botnets. The website owners face the costs to keep their website running in case of an attack.

Apart from these externalities, also other factors influence the security issue. To research the impact of two factors on the infection rate among varying countries, a statistical analysis is performed. First, the influence of the cybersecurity practices (GCI) on infection rate is tested by conducting a linear regression test. A significant model was estimated which explains 27% of the variance in monthly infection rate per country. It was concluded that an

increase of 0.1 GCI results in a *decrease* of approximately 54% of infection rate. Second, an attempt to test the influence of Anti-Botnet Initiatives on the infection rate has been made. However, the results of an independent t-test could not be correctly interpreted since the assumption of a normal distribution is not met. Future research can investigate this issue. Different scales for the infection rate or aggregation levels can be tested to fit the assumptions of a performed test. Also, varying groups can be formed to research differences between countries.

References

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

Cetin, O., Gañán, 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.

ITU (2018). *Global Cybersecurity Index (GCI) 2018.* Retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx#targetText=The%20Global%20Cybersecurity%20Index%20(GCI,different%20dimensions%20of%20the%20issue.

Jerkins, J. A. (2017, January). 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.

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

Russell, G. (2017). Resisting the persistent threat of cyber-attacks. Computer Fraud & Security, 2017(12), 7-11.

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).

Eeten, Michel & Bauer, Johannes. (2009). Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications. Journal of Contingencies and Crisis Management. 17. 10.1111/j.1468-5973.2009.00592.x.