WM0824TU Individual Assignment

Wilko Meijer
4224426

November 15, 2018

Abstract

The spread of the Mirai malware is a major security issue in the IoT industry, attacks by subsequent botnets are among the largest ever seen. Lack of security awareness by manufacturers of IoT devices is the main cause of this security issue according to current research. This paper investigates whether certain brands of IoT devices are more prone to infection by the Mirai malware than others with the hypothesis that there is no signficant difference, because the problem is similar industry wide. By correlating the amount of infections of Mirai malware with the amount of IoT devices per country, it is shown that there is significant difference between manufacturers, refuting the hypothesis. Manufacturers, thus influence the spread of the Mirai malware. Sharing security knowledge and the development of new security standards within the IoT industry, thus is vital for mitigating security issues like the Mirai malware.

1 Introduction

For this report data from the Mirai-like Botnet Badpackets [1] dataset was analyzed. The dataset contains IP addresses from which packets were seen that conform to the pattern of packages sent by machines infected by the Mirai malware. An IP address is only added to the dataset the first time it shows behavior suggesting infection. Additional information related to the IP address, like to which Autonomous System (AS) it belongs, Country of origin, and a time stamp is added for each entry as well.

The dataset only reflects when new infections were detected, not the total amount of current infections. The security issue that the dataset describes is thus *the spread of the Mirai malware.* The Mirai malware is used to build botnets of many devices, which are in turn used for cyber attacks. Limiting the spread of the malware, in turn limits the size of the botnet, and the amount and size of attacks. Since the cyber attacks performed by the Mirai botnet have a high impact, since services can sometimes be inaccessible for a day, preventing them is something that is a major benefit to the economy.

This report investigates the security issue further by reviewing current research in section 2 and researching the security issue further in relation to the dataset. The research question is defined in section 3, the methodology is explained in section 4, results of the research are discussed in section 5, limitations are stated in section 6, and finally the conclusion can be found in section 7.

2 Literature Review

The Mirai malware is used to create larger botnets than ever seen before [2], therefore it is a topic of interest for the scientific community. In this section five references that discuss the security issue as defined in section 1, or issues related to it, are reviewed. This gives an overview of the existing research that exists for this security issue.

The Mirai Bonet and the IoT Zombie Armies [2] This paper gives an overview of malware targeting IoT devices focussing on the Mirai malware. It includes an in-depth review of how the Mirai malware works. They distinguish three stages: infiltration, infection, and operation. The infiltration and infection stages relate to the spread of the Mirai malware in order to recruit more bots. The operation stage is where the C&C server controls the bots in order to perform attacks. Infiltration is performed by bots scanning the internet for vulnerable devices and trying to gain shell access through brute-force dictionary-based attacks. A succesful infiltration allows for downloading the malware to the device completing the infection. The paper discusses quite a few mitigation techniques against the spreading of Mirai. Like blocking TCP ports used by Mirai, denying access to the Internet of an IoT device alltogether, and using VPN's, SSH or TLS instead of telnet for remote access. Furthermore the infections can be mitigated by changing passwords, controlling access, and patching the IoT device. The authors attribute the problem mainly to the manufacturers of IoT devices, for shipping IoT devices with (often) undocumented and unnecessary remote admin capabilities. And they conclude that the most effective solution would be firmware updates.

Analysis of Mirai malicious software [3] Sinanović and Mrdovic have performed both a static and dynamic analysis of the Mirai malware to get insight into its operations. From their static analysis they conclude that the Mirai malware has three parts: a C&C server, which instructs the bots and provides a virtual terminal for botnet users, a loader, which loads the malware to an infected device, and a bot, which search for targets and execute attacks. For the dynamic analysis the setup is extensively described so the research can easily be reproduced. The dynamic analysis allowed them to come up with signatures for both the attack traffic and the infection attempts. They conclude that the best and easiest way to mitigate the Mirai malware is through the creation of IDS (Intrusion Detection System) signatures, and subsequently blocking that traffic. Other possible mitigation techniques described are, changing of passwords, and using a similar technique as Mirai for removing other (competing) malware. Furthermore they note that antivirus tools will probably not be effective since the malware leaves no clean signature on the device itself.

IoDDoS — The Internet of Distributed Denial of Service Attacks [4] This paper is a case study of the Mirai Malware and IoT-Based Botnets. An overview of the IoT landscape is given and the many vulnerabilities that come with IoT are shortly dicussed. This includes vulnerabilities like lack of updates, the lack of security by design, insecure interfaces, and insecure network services. Furthermore an overview of possible DDoS attacks is given. The main part of the study is a static analysis of the Mirai malware. Conclusions of this static analysis are similar to the conclusions of the previous two references discussed. The authors make note of a possible SQL injection vulnerability in the C&C server code, which could possibly be used to counterattack the botnet, but no further details or an attack plan are given. For mitigation the authors suggest similar methods as the previous two references. They conclude with the prediction that IoT-based DDoS attacks will become more prevalent as the amount of deployed unsecure IoT-devices is expected to grow exponentially.

Understanding the Mirai Botnet [5] Antonakakis et al. have conducted extensive and thorough research into the Mirai botnet. They have collected a vast amount of data on the botnet by using a large network telescope, honeypots, DNS traces, and logs of attacks. The research is a collaboration of universities and large tech companies, which gives them an excellent overview of the Internet landscape. From their large amount of data they are able to give a good estimate of how the Mirai malware spread over time, linking changes in the data to events like the Deutche Telekom attack. The paper is able to accurately analyse how Mirai behaves in practice, which is a much needed addition to the static analyses that previous research conducted. It is concluded that the Mirai malware disproportionately represented in some parts of the world, suggesting that a local mitigation by a few network operators could be quite effective to mitigate the threat. Furthermore an analysis is given of which devices are targeted and how several variations of the Mirai malware evolve to target other devices and ip ranges. The top manufacturers of infected devices are Dahua, Huawei, ZTE, Cisco, ZyXEL, and MikroTik. Lastly they give an overview of the different kind of attacks Mirai botnets performed and study their targets. Based on their data it is possible to accurately pinpoint which kinds of attacks were performed. The paper concludes with possible mitigation strategies, device manufactured are identified as the main party which needs to change behavior. The authors call for an adoption of security hardening best practices by the IoT industry, in order to mitigate the very vulnerable IoT landscape.

An In-Depth Analysis of the Mirai Botnet [6] This paper provides an overview of how the Mirai malware operates by discussing how botnets are structured, the command API, infection of new devices, and possible attacks performed by the bots. The paper does not state a methodology explicitly, but it is obvious that the main source is static analysis of the published Mirai malware code. The authors do discuss why certain parts of Mirai are designed the way they are. It is focussed on providing raw facts of how Mirai operates, which is a limitation of the research. The authors further propose mitigation techniques, like changing credentials and limiting network access. Furthermore they propose a detailed detection method based on the fact that Mirai disables the watchdog timer in the linux based devices, something which should almost never occur. According to the authors the mitigation techniques can also be used for other strains of malware since they are often similar.

3 Research Question

Manufacurers of IoT hardware are the responsible party according to current research. Antonakakis et al. elaborate on that statement the most by linking the hardcoded credentials in the Mirai malware to specific manufacturers. Furthermore they show that there are only a few manufacturers responsible for the majority of infected devices. [5] This could have a few reasons: 1. they have more sales 2. their security is lacking compared to other manufacturers 3. they are targeted disproportionally by the Mirai malware.

If the entire industry of IoT device manufacturers is not putting in enough effort to get their security right, it will be difficult to fix the lack of security without external pressure by authorities. However, if there is significant difference in security performance between device manufacturers and economic incentive starts to emerge. When consumers have a choice between different levels of security and care about that, manufacturers that do well in security have an extra unique selling point that can be used to convince consumers that their product is the best.

To see if there can be any economic incentive for security improvements in the IoT industry, it is needed to prove that there is significant difference in security performance between manufacturers. Based on the Mirai badpackets [1] dataset and some additional data about the sales/presence of IoT devices of certain manufacturers it is possible to answer the following research question:
Are certain brands of IoT devices that are targeted by Mirai malware more prone to infection than others?
This research question can be answered with help of the following metric:
The correlation between the sales of certain IoT brands and the total amount of infections observed per country.
Current research is agreed on that the best mitigation against Mirai and other malware alike is a better security practice by the device manufacturers. They say that the whole industry has a problem with their security standards. Therefore the hypothesis of this paper is as follows:
There is no significant difference in the infection rate by Mirai malware of dif-

ferent brands of IoT devices.
This would mean that the security problem is the same industry wide and some authority should step in to force the manufacturers to improve security.

4 Methodology

To test the hypothesis that there is no significant difference in infection rate of different brands of IoT devices the metric of correlation between the infection rate of countries and the precense of certain IoT brands in those countries will be evaluated. Correlation can be easily calculated by using Pearsson Correlation [7], for which easy functions are available in Python. Pearson correlation gives a value between -1 and +1, both extremes indicating a total negative or linear postive relation respectively and 0 no relation.

4.1 Badpackets dataset

The Badpackets dataset reflects the spread of the Mirai malware. Every time an IP address is first seen to be showing behavior which relates to the Mirai malware it is added to the dataset. The dataset contains 233 629 entries in total. For each of the entries there are five columns: IP address, Autonomous System (AS), Country, Autonomous System Number (ASN), and date first seen. The AS, country, and ASN entries are the origins of the IP address, the date first seen is the date the IP address is added to the dataset. The dataset contains data from the period of 18 Februari 2017 till 12 September 2018 and says something about how fast the Mirai malware is currently spreading. The data is prone to double entries, since dynamic IP addresses will cause an infected device to be reflective multiple times in the dataset. It is not entirely clear where the data comes from, as this is not clearly stated on the website of badpackets [1]. However, despite these shortcomings, the dataset seems to be consistent with other dataset described in current research, so it gives an indication about what is actually happening in the IoT malware landscape.

4.2 Device sales/presence dataset

It is hard to find reliable information about IoT device sales on a country level. Therefore the data used is based on the presence of certain brands in countries. This data is collected by using the search engine Shodan [2], which is a search engine specific for IoT devices. Using Shodan a dataset was built of how many devices of a certain brand are connected in certain countries. From the paper by Antonakakis et al. a list of brands targeted by the Mirai malware was made. Each of these brand names was searched for in Shodan, which resulted in a list of how many devices with these brand names were online per country. Queries with less than 10 000 results were discarded as they were not reliable enough.

[1] https://mirai.badpackets.net

[2] https://shodan.io

IoT hardware brand	Correlation	P-value
Axis	0.21	0.02
Cisco	0.23	0.00
Dahua	0.60	0.00
Huawei	0.82	0.00
MikroTik	0.63	0.00
Panasonic	0.22	0.03
RealTek	0.60	0.00
Samsung	0.17	0.06
Ubiquiti	0.24	0.00
ZTE	0.32	0.00
ZyXel	0.01	0.94

Table 1: Pearson correlation between the presence of IoT brands and the infection rate per country.

Correlation	P-value
0.55	0.00

Table 2: Pearson correlation between the total amount of infections per country and the sum of the IoT devices considered in this experiment. If the amount of infections is only influenced by the amount of IoT devices in a country a correlation of 1 is to be expected.

The most probable reason for some queries not returning any significant amount of results is that their brand is mentioned nowhere in messages upon connecting with the devices.

This dataset is in no way a reliable indicator of the exact amount of IoT devices currently active in the world, but it is an indication of the differences between manufacturers per country. For calculating the correlation there is no need for exact numbers, as long as the error is about the same for all entries, which is assumed for this assignment.

5 Results

The correlation between the presence of certain IoT brands and the amount of infections per country were calculated. The results of these calculations can be found in Table 1. The P-value of the correlation indicates the probability that an uncorrelated dataset produces an correlation value at least as extreme as this value. From the table it becomes clear that the almost calculations are reliable with the standard evaluation of $p<0.05$. These P-values are not reliable for small datasets [8], but since these datasets are not that small (>100 data points) they will be taken into account.

The first thing that stands out from the results is that there is a big difference in correlations between brands. This suggests that devices used in a country do not influence the infection rate of that country with the same amount. This disproves the hypothesis that *There is no significant difference in the infection rate by Mirai malware of different brands of IoT devices.* If there was a no significant difference in the infection rate, you would expect to get correlation values which are around the correlation value of the total amount of IoT devices and the infection rate per country as stated in Table 2. Therefore the security problems with IoT devices are not the same for the whole industry, some manufacturers are performing better than others.

To evaluate which manufacturers produce IoT devices that are more vulnerable to the Mirai malware the correlations should be compared to the value in Table 2. This correlation value states that the devices under consideration in this research have a correlation of 0.55 with the total amount of infections when compared on a country level. It is hard to quantify what this number exactly means (What does 55% correlation mean?), but we can still use this number to check which brand of devices influence the infection rate more than others. All brands with a correlation above 0.55 can be said to be more vulnerable to the Mirai malware than average. Dahua, Huwei, MikroTik, and RealTek have correlations higher than 0.55 and thus are more responsible than average for infections by the Mirai malware. Especially Huawei, with a correlation of 0.82 can be said to have a significant impact on the total amount of infected devices in a country.

The brands of devices that are infected the most do not align completely with the brands that are more vulnerable than average for infections. In the paper by Antonakakis et al. [5], the brands of the most infected devices are listed as Cisco, Dahua, Huawei, MikroTik, ZTE, and ZyXel. Cisco, ZTE, and ZyXel, however are correlated much less than the 0.55 average. The fact that their devices are responsible for a high number of infections is probably due to the amount of devices deployed more than their security vulnerabilities. The result of ZyXel, is a bit more special, since it indicates that there is no correlation at all. In Germany there is a very high presence of ZyXel devices compared to other countries, around 1 million versus 42 000 in the next country. It could be that certain types of their devices are deployed in only a few countries. When one of those types of devices contains a vulnerability, for example the devices deployed in Germany, this could result in a high amount of total infections of ZyXel devices, while they are only contained to a few countries. Which would explain why there is little correlation, but a high presence of infected devices in general.

6 Limitations

The main problem of this research is collecting reliable and complete data. This research makes use of two datasets, it is not entirely clear how the badpackets dataset is composed and it is also not clear if that causes any bias in the data. Finding a better data source like the one used [5], based on a large network telescope will give more reliable results. Furthermore it would be more useful to have data about the current state of infection instead of the first time a device was infected, as it would be easier to correlate that data with the amount of devices currently online.

The data collected on the amount of IoT devices online per country is also not great. The search engine searches for keywords in things like welcome messages of IoT devices, so a brand can only be found if the brand name is mentioned in those messages or in some other specification of the device collected by the search engine. This way of searching might completely miss certain brands, because they don't mention their brand names anywhere. A more reliable dataset would be the sales of IoT devices per country. This dataset would need to go back quite a few years to account for all the older devices that are still online.

This research assumes that all IoT devices of a manufactur are targeted equally by the Mirai malware. Further research is needed to compile a complete list of which devices are affected by the Mirai malware and to take that into account for the comparison of the security performance of IoT manufacturers.

7 Conclusion

This paper sought to research whether there *are certain brands of IoT devices that are targeted by Mirai malware more prone to infection than others.* The results of this research sugguest that there are brands that are more prone to infection than others: Dahua, MikroTik, RealTek, and especially Huawei. The amount of devices of these brands present in a country have a higher than average correlation with the total amount of infections by the Mirai malware in the same country. There are significant differences in the correlations of brands, meaning that there is a significant difference in performance of mitigation of the Mirai Malware by those brands. This difference in performance is something consumers should take into account when buying devices so there is a financial incentive for the manufacturers to improve their security.

This conclusion supports the general opinion by researchers that the best way to mitigate the security issue of the spread of the Mirai malware is action from the manufacturers of the IoT devices. It does not mean that there is not an industry wide problem with the security problem, which becomes clear from the fact that brands that are less correlated than average are still among the most infected devices in general.

Further research is required to investigate the differences in security policies as performed by the manufacturers of different brands of IoT devices. Sharing the best practices of the better performing manufacturers in the industry and developing new security standards for IoT devices will help the industry in general to produce more secure products and mitigate the spread of malware.

References

[1] A. Rhodes. (2018, Sep) Mirai-like botnet bad packets report. [Online]. Available: https://mirai.badpackets.net/

[2] G. Kambourakis, C. Kolias, and A. Stavrou, “The mirai botnet and the iot zombie armies,” in *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*, Oct 2017, pp. 267–272.

[3] H. Sinanović and S. Mrdovic, “Analysis of mirai malicious software,” in *2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, Sept 2017, pp. 1–5.

[4] R. Hallman, J. Bryan, G. Palavicini, J. Divita, and J. Romero-Mariona, “Ioddos — the internet of distributed denial of service attacks - a case study of the mirai malware and iot-based botnets,” in *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security - Volume 1: IoTBDS,*, INSTICC. SciTePress, 2017, pp. 47–58.

[5] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis *et al.*, “Understanding the mirai botnet,” in *USENIX Security Symposium*, 2017, pp. 1092–1110.

[6] J. Margolis, T. T. Oh, S. Jadhav, Y. H. Kim, and J. N. Kim, “An in-depth analysis of the mirai botnet,” in *2017 International Conference on Software Security and Assurance (ICSSA)*, July 2017, pp. 6–12.

[7] K. Pearson, “Note on regression and inheritance in the case of two parents,” *Proceedings of the Royal Society of London*, vol. 58, pp. 240–242, 1895.

[8] The SciPy community. scipy.stats.pearsonr - scipy v1.1.0 reference guide. https://docs.scipy.org/doc/scipy/reference/generated/scipy.stats.pearsonr.html. Accessed: 2018-11-14.