Mirai security metrics

Economics of cybersecurity assignment
Rômy Bergman 4369408
Saskia Kooijman 4473795
Giulio Pellizzari 5143160
Jochem van de Laarschot 4227530

September 16, 2019

1 Introduction

In august 2016, white-hat security researchers discovered the Mirai malware [4]. The malware infects devices connected to the internet. In particular IoT devices that are weakly configured are targeted. The malware tries to access to vulnerable devices through a dictionary attack that exploits a set of the most common default credentials. Once access has been gained, malware notifies the command and control server and the malware is installed on the vulnerable machine. The newly infected device then searches for other vulnerable devices and repeats the previously mentioned operations on these devices. [3].

This way, a large botnet was created, which consisted of IoT devices such as IP cameras, routers and printers [1]. This botnet was used to carry out one of the most powerful DDoS attacks [3]. After the discovery of Mirai, the source code was published on hackforums.net , resulting in fast propagation of the Mirai virus and the instantiation of look-alikes [1].

In this paper, the security issue at hand is clarified using three different levels of analysis as depicted in Figure 1.

On macro level, Mirai showed that 'the internet' and internet services used throughout the whole world should be secured. DDoS attacks proved to be able to take down DNS servers and therefore a multitude of internet services were not available for significant parts of the world population [3].

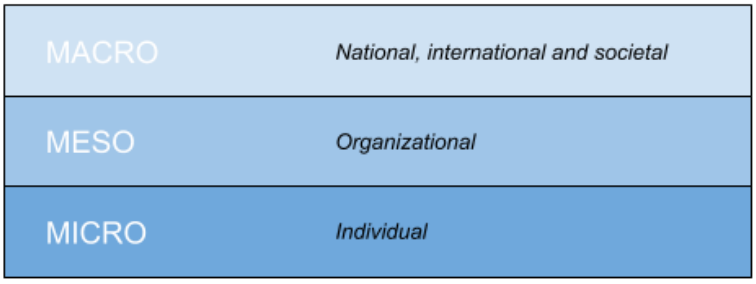

Figure 1: Analysis level classification

On meso level can be viewed from two perspectives. (1) organizations providing (vital) internet services should secure themselves against DDoS attacks. (2) organizations manufacturing IoT devices should work more securely by following common security practices. [3] speak of a "chronic neglect in applying even basic security practices" as one of the major reasons for the Mirai success.

On micro level, consumers should secure their IoT devices by changing the default password of their devices. This way, the devices are not vulnerable to the dictionary attacks of Mirai.

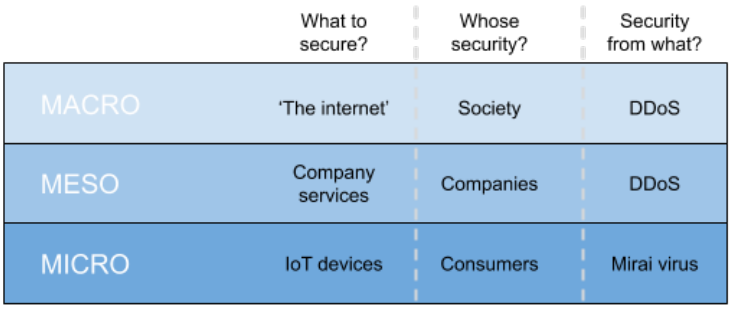

Figure 2: Levels specification

Given this scenario, we initially focus our analysis on two levels of details: individual level, where we considered the IoT devices, and organizational level where we considered companies and internet services (such as DNS).

IoT devices have to be protected against Mirai malware while companies and internet services have to be protected against DDoS attacks. In the former case, the responsibility of prevention lies on private citizens while in the latter companies and ISPs have to take care of their systems. However, companies and ISPs need metrics to understand how much money they should invest to prevent this kind of threat. For this reason, in the following sections, we will discuss our considerations about metrics that may help companies and ISPs in taking these decisions.

2 Ideal metrics

First of all some ideal metrics will be defined that in our perspective will help companies and ISPs to better identify how much money they have to invest in protection of their services against DDoS.
The core issue leading the way to Mirai malware infection is the use of default credentials. Device manufacturers sell devices configured with known pattern of username and password and customers, once bought, do not change this configuration allowing Mirai to easily infect them.

Starting from this point, the number of devices having default password would be the first useful ideal metrics for companies and ISPs. Knowing this number could be really useful for companies and ISPs, because it would allow them to approximately estimate the number of bots that can carry out a DDoS attack and, from that information, identify whether their infrastructures have the capabilities to resist against an attack of that capacity. Therefore this metric would indicate in a straightforward way if the company/ISP has to invest on security against DDoS or not.

Secondly, metrics about the infected devices: information about the type and the location of infected IoT devices and demographics information about their owners can be analyzed and correlated to get insights about customer behavior. These insights could be very useful because they can help ISPs to identify in which segments of the population they have to take action to tackle this kind of threat.

The metrics we have just described can be classified into two categories: the first one goes under the category of control metrics. These metrics check whether a control is in place or not. In this case, the metric checks how many device owners have not changed the default credentials of their devices. The second set of metrics is classified under the category of incidents, since they

exploit information gathered from previously successful infections and attacks to extract useful insights for ISPs.

3 Metrics in practice

The metrics in practice suitable for this issue will be discussed in this chapter. Based on various literature sources, there are different metrics identified which are used in practice for this kind of issue. These identified metrics can be of help when analyzing the data.

[3] highlight the importance of device owners to change the default password and mention the danger of IoT devices that operate using the default password.

[5] stress the importance of access control as a countermeasure for DDoS attacks from IoT devices. A combination of identity authentication and code access to the device shall establish a more security picture of the device owner and provide higher security. Many consumers can opt for their preferred access control mechanisms. Hence, the diversity of access controls installed on a device is a metric used.

[6] direct on several measures organizations need to track in order to monitor attack traffic. Their research mentions the resource IP addresses, the increasing degree of traffic and similarity of the traffic as important parameters.

[2] have tracked the infections in darknets, honeypots and abuse reports under the domain of an ISP. Their gathered data has been used to study the effectiveness of different notification systems in the process of telling the customers they have been infected by Mirai malware and to help them along the remediation process. The metrics they used to analyze the behavior of the malware across the time (infection, remediation, reinfection) have been the type and the location of infected devices, the number of devices performing scans with a specific protocol and they also mapped each device to the network type it belongs to in order to identify which are the network type more prone to be infected.

4 Data description

In this dataset three different kinds of columns are shown. One column shows the IP-addresses from the infected IoT devices, which can help analyzing where in the world the IoT devices are located. The ideal metric defined in chapter 2 can help with this. Secondly, the amount of port variables and their frequency in which these are used to gain access to the IoT device are counted.

5 Data analysis

To gain a better understanding of the spread of the virus, in terms of newly infected devices over time, the data set was filtered down to only unique IP addresses. In this chapter, the analysis of the data will be performed. First of all, exploratory analysis are conducted.

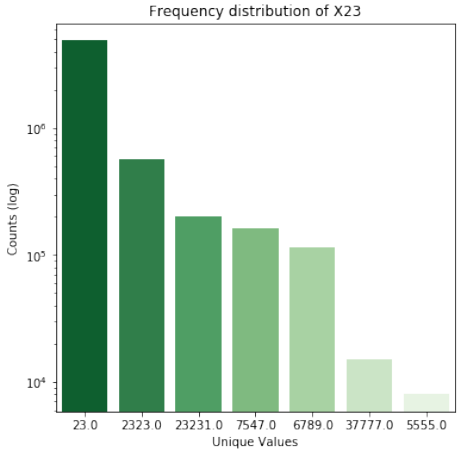

Figure 3: Frequency distribution of ports

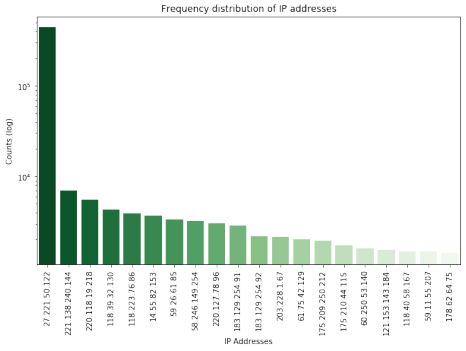

Figure 4: Frequency distribution of IP addresses (top 20)

When the frequency distribution of the third column is plotted (Figure 3) it becomes clear that this column shows the port used for access. From Figure 4 it becomes clear that one IP address evidently occurs most frequently in the data set.

6 Conclusion

References

[1] Manos Antonakakis, Tim April, Michael Bailey, Matthew Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou. Understanding the mirai botnet. In *Proceedings of the 26th USENIX Conference on Security Symposium*, SEC'17, pages 1093–1110, Berkeley, CA, USA, 2017. USENIX Association.

[2] Orcun Cetin, Carlos Hernandez Ganan, Lisette Altena, Takahiro Kasama, Daisuke Inoue, Kazuki Tamiya, Ying Tie, Katsunari Yoshioka, and Michel van Eeten. Cleaning up the internet of evil things: Real-world evidence on isp and consumer efforts to remove mirai. In *Network and Distributed System Security Symposium (NDSS) 2019*, 2019.

[3] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. Ddos in the iot: Mirai and other botnets. *Computer*, 50:80–84, 01 2017.

[4] Pierluigi Paganini. Linux/mirai elf, when malware is recycled could be still dangerous. https://securityaffairs.co/wordpress/50929/malware/linux-mirai-elf.html, September 2016. Last access on September 16, 2019.

[5] Tasneem Yousuf, Rwan Mahmoud, Fadi Aloul, and Imran Zualkernan. Internet of things (iot) security: Current status, challenges and countermeasures. *International Journal for Information Security Research*, 5:608–616, 12 2015.

[6] Congyingzi Zhang and Robert Green. Communication security in internet of thing: Preventive measure and avoid ddos attack over iot network. In *Proceedings of the 18th Symposium on Communications & Networking*, CNS '15, pages 8–15, San Diego, CA, USA, 2015. Society for Computer Simulation International.